A STUDY OF THE IMPACT OF THE BLURRING OF THE LINES BETWEEN PERSONAL AND WORK LIFE CONTEXTS ON CYBERSECURITY HUMAN BEHAVIOUR

Paul Hayes

A thesis submitted to

Auckland University of Technology

in partial fulfilment of the requirements for the degree of

Master of Information Security and Digital Forensics

2023

School of Engineering, Computer and

Mathematical Sciences

Abstract

Human behaviour is a factor in a significant number of cybersecurity breaches. The increased use of smartphones, laptop computers and tablets mean that more people are carrying out personal and work online activities from different locations. The Covid-19 pandemic has forced more businesses online and more employees to work from home, which has increased the blurring of lines between the use of technology for both personal and business use.

Whilst there has been some research carried out in the field of human behaviour and cybersecurity, this has predominantly been focused on an organisational work context and on aspects such as assurance and compliance. There has been relatively little research carried out about how the blurring of lines between personal and work contexts affects cybersecurity human behaviour. This study considers cybersecurity human behaviour across both personal and work life contexts, to understand the impact of this blurring of the lines between them.

This research adopted a qualitative approach and interviewed several participants to gain insights into their human behaviour relating to cybersecurity in both a personal and a work life context. Data gathered included what devices they used, the networks over which those devices communicated, and the type of activity or applications being used on those devices and over those networks. The research also looked at other aspects such as identity authentication, training and smart devices on the home network.

Based on an analysis of the gathered data, the impacts relating to cybersecurity human behaviour in personal and work life contexts were identified, which in turn informed the barriers to improved cybersecurity and proposed mitigations for these. Firstly, human behaviour regarding use of company provided devices over their networks is typically influenced by company policies. This is a key difference from personal devices and home networks where there are no policies or guidelines to comply with.

Secondly, more organisations are providing cybersecurity training to their employees. This is mostly targeted at protecting the organisation, but the absence of any training or guidelines in a

personal context means this work-related training predominantly informs their cybersecurity knowledge and awareness, missing specifics that may be relevant in a personal context.

Specific barriers to improved cybersecurity resulting from these findings are firstly a lack of knowledge and guidelines specifically focused on cybersecurity protection when carrying out personal activities. Secondly, the lack of consideration of the potential risks of the home network environment given it is shared by multiple parties whose behaviour may have an impact, and that this home network environment may include multiple connected smart devices with their associated security risks. A proposed mitigation for these barriers is the provision of training and guidelines focused on behaviour relating to personal cybersecurity, including set-up of the home network.

Table of Contents

ABSTRACT ..... **II**

TABLE OF CONTENTS ..... **IV**

LIST OF FIGURES ..... **VII**

LIST OF TABLES ..... **VIII**

ATTESTATION OF AUTHORSHIP ..... **IX**

ACKNOWLEDGEMENTS ..... **X**

ABBREVIATIONS AND ACRONYMS ..... **XI**

1 INTRODUCTION **1**

1.1 Cybersecurity and Human Behaviour 1

1.2 Research Aims and Objectives 2

1.3 Research Approach 2

1.4 Contribution 3

1.5 Thesis Structure 3

2 LITERATURE REVIEW **5**

2.1 Cybersecurity and Human Behaviour 5

2.2 Working From Home and Covid-19 8

2.3 Research Question 11

3 RESEARCH DESIGN AND METHODOLOGY **12**

3.1 Research Approach 12

3.2 Research Design Steps 12

3.3 Research Methodology 14

3.4 Behaviour and Cybersecurity Models 14

3.5 Data Collection Method 17

3.5.1 Research Sample *19*

3.5.2 Interview Process *20*

3.5.3 Questionnaire Development *21*

3.6 Research Aim and Selected Methods 24

3.7 Data Analysis 24

3.7.1 Coding *25*

3.7.2 Codebook *25*

4 FINDINGS 29

4.1 DEVICES 29

4.1.1 Smartphones 29

4.1.2 Computers, Laptops and Tablets 31

4.2 NETWORKS 32

4.2.1 Mobile Networks 32

4.2.2 Work Networks 33

4.2.3 Home Networks 33

4.2.4 Public Wi-Fi 34

4.3 APPLICATIONS AND TYPE OF USAGE 35

4.4 IDENTITY AUTHENTICATION AND PASSWORD MANAGEMENT 37

4.5 IDENTITY THEFT AND PRIVACY 40

4.6 SMART DEVICES ON THE HOME NETWORK 41

4.7 CYBERATTACKS 42

4.8 TRAINING 43

4.9 AWARENESS, INTENTIONS AND ACTIONS 43

4.10 WORKING FROM HOME (WFH) AND COVID-19 45

4.11 CATEGORIES AND THEMES 45

5 FURTHER ANALYSIS AND DISCUSSION 49

5.1 INFRASTRUCTURE IMPACTS 50

5.1.1 Smartphones 50

5.1.2 Laptops and Tablets 52

5.1.3 Smart Devices on the Home Network 53

5.1.4 Public Wi-Fi 54

5.1.5 Summary of Infrastructure Impacts 55

5.2 IDENTITY AUTHENTICATION 56

5.3 ONLINE ACTIVITY AND USAGE 57

5.3.1 Work Tasks and Activities 58

5.3.2 Online banking 58

5.3.3 Online Shopping & Payments 59

5.3.4 Social Media, Identity Theft and Privacy 60

5.3.5 Other Usage/Applications 61

5.4 AWARENESS, INTENTIONS AND ACTIONS 62

5.4.1 Training & Guidelines *62*

5.4.2 Awareness, Intentions and Actions *63*

5.5 Human Behaviours and Cyberattacks 63

5.6 Barriers and Mitigation to Improved Cybersecurity 64

5.6.1 Barriers *64*

5.6.2 Mitigations *66*

5.7 Comparison with Other Research 67

6 CONCLUSION, LIMITATIONS AND FUTURE WORK 69

6.1 Summary of Research Approach 69

6.2 Insights, Barriers and Mitigations 70

6.2.1 Insights *70*

6.2.2 Barriers to Improved Cybersecurity *70*

6.2.3 Mitigations *71*

6.3 Research Contributions 71

6.4 Implications and Opportunities 72

6.5 Limitations 72

6.6 Future Research Opportunities 73

7 REFERENCES 74

APPENDIX A. ETHICAL APPROVAL 76

APPENDIX B. PARTICIPANT INFORMATION SHEET AND CONSENT FORM 77

APPENDIX C. INTERVIEW TRANSCRIPTS 81

List of Figures

Figure 1. Research Design Steps 13
Figure 2. Cybersecurity Culture Model – Individual Level (Georgiadou et al., 2022) 15
Figure 3. Revised Individual Level Cybersecurity Culture Model 16
Figure 4. Cybersecurity Dimensions Model 17
Figure 5. Codes and Categories 46
Figure 6. Cybersecurity Behaviour Model / Framework 47

List of Tables

Table 1. Sample List of Questions 18
Table 2. Updated Sample Questions 23
Table 3. Nvivo Codebook 26
Table 4. Participant's Smartphones and Usage 30
Table 5. Participant's Laptops and Tablets 31
Table 6. Use of Public Wi-Fi 34
Table 7. Types of Online Usage 36
Table 8. Identity Authentication 38
Table 9. Password Changes and Complexity 39
Table 10. Identity Theft and Privacy 40
Table 11. Smart Devices in Participants Homes 41
Table 12. Cyberattacks 42
Table 13. Intentions and Actions 44

Attestation of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

Signed by: Paul Hayes

Date: 20th July 2023

Acknowledgements

Firstly, I'd like to acknowledge the support that I received from my supervisor Dr Krassie Petrova. The help and guidance that she provided me to help me navigate through my research study was invaluable and I have learned much from her, especially regarding the research process.

Secondly, I'd like to thank the research participants who agreed to participate in this research, the time they devoted to it, and the openness with which they shared their information and views.

And last, but not least, I'd like to thank my wife Chrissie for her support, understanding and encouragement whilst I spent many evenings writing up my research.

Abbreviations and Acronyms

Abbreviation / Acronym	**Definition**
BYOD	Bring Your Own Device
IoT	Internet of Things
IT	Information Technology
MDM	Mobile Device Management
PC	Personal Computer
USB	Universal Serial Bus
VDI	Virtual Desktop Infrastructure
VPN	Virtual Private Network
Wi-Fi	Wi-Fi is a family of wireless network protocols based on the IEEE 802.11 family of standards

1 Introduction

The Verizon 2023 Data Breach Investigations Report (DBIR) found that "74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering" (Verizon, 2023). This thesis presents the research carried out on the subject of cybersecurity and human behaviour, and the impact of the blurring of the boundary between personal and work life contexts. The study evaluates the behaviours relating to personal and work activities and the infrastructure that these are carried out over, given the context of many more people working from home because of the Covid-19 pandemic. The study findings are analysed, and the impact of these findings are discussed, including the barriers to improved cybersecurity. Limitations of the research are identified along with possible future research opportunities.

Background relating to human behaviour and cybersecurity in a personal and work context is introduced in this chapter, along with the motivation for and aim of this research. The main research question is identified, informing the aims and objectives of the research. The contribution from the research is highlighted. The structure of the thesis is outlined along with a summary of its content.

1.1 Cybersecurity and Human Behaviour

Cybersecurity is often considered as the responsibility of the IT department of an organisation, where the main attention has been on technical solutions to improve cybersecurity infrastructure (Hadlington, 2018). However, it has long been understood that a significant number of cybersecurity breaches are a result of human error or human behaviour (Bhaharin et al., 2019). The increased availability and use of smartphones, laptops and tablets for both personal and work usage, including Bring Your Own Device (BYOD) concepts (Veljkovic & Budree, 2019), combined with increased capacity and performance of broadband and wireless networks has enabled us to carry out many more activities from locations that we could not in the past. With the arrival of Covid-19 in early 2020 and the resulting lockdowns implemented in several countries, businesses were forced to establish the capability for their employees to work from home, which forced many individuals to carry out work activities that they had traditionally done at the office but were now

required to be done from their homes to limit the spread of the virus (Borkovich & Skovira, 2020). Whilst the capability has existed for some time for professionals to work remotely, the Covid-19 pandemic resulted in many more people doing this, as well as much more time spent working remotely for those that already had the capability. This has resulted in a blurring of the boundary between an individual's personal life and their work life, with work activities now being carried out at home on a regular basis and company policies being updated to allow this. Whilst many of us previously had a clear demarcation between work activities carried out on the work computer in the office and personal activities typically carried out on the shared home computer, these activities have become mobilised, with smartphones, laptops and tablets being able to be operated from anywhere, including personally owned devices as well as devices provided by the organisations that we work for (Veljkovic & Budree, 2019).

1.2 Research Aims and Objectives

Whilst there has been some research carried out in the field of cybersecurity and human behaviour, this has predominantly been focused from an organisational context. There has been some research on this from a personal and home context, but research carried out that looks across both the personal context and work context is limited. Given the increased blurring of the lines between these two contexts and the known fact that human behaviour is a factor in a number of cybersecurity breaches, the motivation for this research is to understand more about human behaviour relating to cybersecurity in both contexts, the impacts of these behaviours and whether there are learnings that can be applied to the corresponding context. The aim of the research is to investigate how the blurring of the lines between personal and work contexts impacts cybersecurity human behaviour. The main research question of the study can be formulated as: What is the impact of the blurring of the lines between personal and work contexts on human behaviour with respect to cybersecurity?

1.3 Research Approach

The research carried out followed a phased approach. Firstly, the proposed research question was formulated based on the author's understanding and experience. Following this a literature review was carried out to confirm the validity of the research question, by identifying and reviewing

existing research carried out in the field of the research question. The insights gained from the literature review were then used to inform the research design and methodology to be used to answer the research question posed. A qualitative approach was adopted, using semi-structured interviews to gather data. The data gathered was then analysed using coding to identify useful themes. The findings are then further analysed and linked back to the research question and sub-questions.

1.4 Contribution

The outputs of the research carried out contributes to the body of knowledge on human behaviour relating to cybersecurity by: (i) highlighting a significant gap in the knowledge, training and guidelines available to individuals to inform their behaviour relating to cybersecurity in their personal life; and (ii) identifying the additional risks posed by home networks both for personal data and work data, due to the lack of appropriate security controls combined with the use of the home network by multiple parties, and the possible additional risks posed by the increasing number of smart devices on those networks.

1.5 Thesis Structure

The organisation of the thesis follows the phases of the research carried out. This chapter (Chapter 1) introduces the research including background and motivation for carrying out this research, the aims of the research in terms of the research question and the contribution that this research makes. Chapter 2 provides a literature review of research already carried out in the field of the research question and validates the original research question, making minor adjustments based on insights gained from the literature review. Chapter 3 outlines the research design and methodology and the approach used to carry out the research, including the data analysis carried out and the software used to code the gathered data. The findings are presented in Chapter 4. Chapter 5 discusses the findings made and brings these findings back to the aim of the research and the research question and sub-questions posed. Finally, Chapter 6 summarises the work carried out, highlights the contribution that the research has made, captures the limitations of the

research and identifies opportunities for further research in the field of human behaviour relating to cybersecurity both in a work and personal context.

2 Literature Review

2.1 Cybersecurity and Human Behaviour

The literature review for this topic started by looking at the broad aspect of human behaviour related to cybersecurity. There have been number of studies focused on this topic, including research into cybersecurity assurance processes and the role of human behaviour in this (Evans et al., 2016). That paper primarily focuses of cybersecurity assurance in relation to organisations and proposes an assurance framework to help to address the issue that a significant number of security breaches are the result of human behaviour. It notes that whilst security awareness training provided by organisations is important, the volume of cybersecurity incidents that are related to human factors suggests that this alone is not effective in addressing these threats and this needs to be supplemented by some form of cybersecurity human reliability assessment. The conclusions of this paper highlighted that it had been proven that half of cybersecurity breaches have human error at their core, and that developing and applying an assurance framework would benefit in an area that relies on independent knowledge and expertise.

Cybersecurity policy compliance is a topic closely related to assurance and research into this area also highlights that human behaviour is “the main security threat to information security” (Bhaharin et al., 2019) . As with the paper focused on cybersecurity assurance, the subject of information leakage and cybersecurity compliance is focused on organisations and their use of information security policies to address cybersecurity threats against organisations. The article concludes that whilst information security compliance behaviour is affected by employee’s attitudes, other aspects such as technology and organisational factors also play a role. Whilst the paper notes that the “the need for employees to understand the issue of compliance with information security policies is also vital” and suggests that this can be understood by integrating aspects of human behaviour, technology and process, it looks at this only in an organisational context and does not consider how their understanding of individual/personal threats could also have an impact.

A survey carried out in the UK researched employees attitudes towards cybersecurity and risky online behaviours (Hadlington, 2018). This research concluded that the activity of the majority of employees surveyed increased the likelihood of a cybersecurity breach.

There has also been research carried out into specific aspects such as the role that gender differences play in an employee's cybersecurity behaviours (Anwar et al., 2017), concluding that there are statistically significant gender-wise differences in a number of aspects relating to cybersecurity.

The research carried out to date in the field of human behaviours and cybersecurity has largely been focused on the behaviours of individuals as employees and the associated potential business and organisational impacts. This has included a focus on aspects such as security policy compliance (Bhaharin et al., 2019), education and awareness (Maria & Jason, 2019) and risk management (Sebescen & Vitak, 2017). Whilst some of these aspects are also important when considered in an individual personal context, there appears to have been less focus on this from a research perspective, although some research has been carried out focused on cybersecurity and behaviours relating to the individual/home computer users (Addae et al., 2019) and the need to make cybersecurity mechanisms accessible to the average user.

There have been few studies that have researched the aspects of human behaviour from both a personal and organisational context. This is becoming an increasingly important consideration as more companies adopt Bring-Your-Own-Device (BYOD) policies and more personal devices are being used in the workplace connected to company networks. The BYOD concept that has been adopted by a number of organisations is a good example of devices that are intended to be used for both personal and business use. Whilst it is predominantly applied to smartphones, there are also examples of this type of approach being used for laptop devices as well. Whilst there has been some research carried out into the risks associated with BYOD policies (Veljkovic & Budree, 2019), and that research identified that security and privacy risks are two key concern areas for BYOD implementations, the human aspects risks of this are identified as being "lack of control over data and devices", "stolen or lost devices" and "identity theft". The article highlights that ENISA, the European Union Agency for Network and Information Security, "has published a valuable set of controls and best practices for managing the risks in a BYOD programme, classifying them into three groups, these being "Governance; Legal, Regulatory and HR; and Technological (device, application, user and data)". It should be noted that human behaviour is not specifically stated in these groups. In the BYOD risk management model proposed by the authors of that paper (Veljkovic & Budree, 2019), employee education and training are identified as well as the need for an organisational security culture, which would include support for

creating employee's habits, which can be considered as one aspect of human behaviour. As with the research that was focused on assurance and compliance, the primary focus of the BYOD research report (Veljkovic & Budree, 2019) is on addressing the cybersecurity risks of BYOD approaches for the organisation and it doesn't consider the risks to the individual. An example of this is the inclusion of Mobile Device Management (MDM) as a solution suitable for managing BYOD risks for the organisation but does not discuss the implications for the individual of this approach.

Correspondingly, with the recent coronavirus pandemic there has been an increase in the number of organisations allowing and enabling employees to work from home using company provided devices on their home networks.

With these two dynamics, there is the increased potential for human behaviours in a personal use context to have cybersecurity impacts on organisations and vice versa. Further research is needed to understand more about the behaviours in both a personal and work context, their similarities and differences, and potential implications, so as to understand whether there are opportunities in one context that may be leveraged to provide improvements in the other context.

A conceptual taxonomy for cybersecurity behaviour was explored in (Mashiane & Kritzinger, 2019). This paper highlighted that cybercriminals have changed from targeting security systems to targeting the users of the systems. The two key contributions that the paper aims to address are "a unified terminology for cybersecurity behaviour" as well as "the identification and categorisation of home user security behaviour". The paper highlights that in an organisational context, cybersecurity is governed by policies and regulations, and hence is typically evaluated in terms of the level of compliance against these regulations. It presents the taxonomy looking at two dimensions, the expertise of the user (e.g. novice to expert) and the intentions of the user (malicious to benevolent). The paper goes on to break down the work cybersecurity intentions into intentional and unintentional bad and intentional and unintentional good. When it comes to the taxonomy for home users, the paper highlights that the user is typically responsible for managing their own cybersecurity behaviour and that whilst their knowledge may be gained from work environments, the home behaviour is different. Two different cybersecurity behaviour taxonomies are presented, one for behaviour in a work environment and one for behaviour in a home environment. Whilst the same dimensions are used to plot the different

categories, they are different between a work and a home. This raises the question if they are really different or just named differently. In the work-related taxonomy, how is information security carelessness in the unintentional bad, low expertise domain different from cognitive laziness in the home related taxonomy? These differences are not explained by the paper. The two intended contributions from the paper are somewhat conflicting in that whilst presenting a unified terminology for behaviour in organisations, different terminology is defined for the home user, and the paper does not address that in a number of cases these users can be the same person, potentially carrying out work in a home environment. It should be noted that malicious behaviour is not in scope for the research carried out for this study.

With the exception of the paper on a conceptual taxonomy for cybersecurity behaviour (Mashiane & Kritzinger, 2019) and the study of user behavioural data relating to home computer users (Addae et al., 2019), the literature reviewed above predominantly focuses on the cybersecurity and human behaviour challenges associated with protecting organisations, with little focus on protecting individuals. Where individuals are referred to, it is in the context of them as employees.

Whilst the literature reviewed has focused on human factors and human behaviour, be it from different perspectives such as compliance, small and medium enterprises and BYOD, a common theme that has emerged is the need to improve employee's awareness and knowledge relating to cybersecurity and the need for ongoing training and education.

Whilst the paper on a conceptual taxonomy for cybersecurity behaviour (Mashiane & Kritzinger, 2019) presents both work and home conceptual cybersecurity behaviour taxonomies, it doesn't compare and analyse the two different taxonomies in much detail.

The gap that is apparent from the reviewed literature is to consider cybersecurity human behaviour of individuals in both a personal and work life context, and this reinforces the motivations and aims of the research carried out for this thesis.

2.2 Working From Home and Covid-19

During the period of this study, other research was carried out that was focused on cybersecurity and working from home, as a result of the Covid-19 pandemic. One of these papers carried out a survey to assess cybersecurity cultural readiness of organisations due to the

impact of more employees working from home, because of the Covid-19 pandemic (Georgiadou et al., 2022). Whilst this study looked at both organisations and individuals, the aim of the survey stated in the conclusions and future works section was “to evaluate cyber security culture exhibited by organizations…”. Although the paper referred to recommendations and prevention tips being issued by various bodies and experts to assist individuals in preventing cybercrime, it didn’t indicate how well this information was received, understood and acted on by the survey respondents. In the cybersecurity culture model outlined by the paper, behaviour was identified as one of the key dimensions at the individual level. However, information included in the paper on individual behaviour was very limited and predominantly focused on what guidelines or training they had received from their organisations relating to cybersecurity. The study focussed on the ability of individuals to work remotely, awareness and readiness of cybersecurity risks, the management and security of the hardware assets used by the individuals, the changes in applications and services employees were required to use as a result of required changes from Covid-19, collaboration capability when working remotely and cybersecurity incidents encountered. An interesting finding from the survey carried out was that “53% of participants report not to have received any security guidelines from their employers regarding working from home”. The paper highlighted that where guidelines had been issued, they were mainly focused on corporate network access management and less on aspects such as password protection which are more related to human behaviour. The paper does present some findings relating to security of hardware assets, but the usage of those assets and the networks over which date is transmitted is not discussed. Another interesting finding outlined in this paper is that the majority of respondents had not faced any cybersecurity threats during the Covid-19 crisis, with the number one threat reported being phishing. The paper reported that questions were included in the survey to “poll the thoughts, emotions and feelings of the participants”, but the only finding from these responses was regarding the lack of any clear preference for working in the office or from home. One of the key findings in the paper is that “human factor is still not recognized as a core element of the cybersecurity chain”. The paper concludes that individual aspects such as behaviour need a greater focus and that “human factor is the key to information security progress and remains yet uncharted”.

Cybersecurity issues relating to employees working from home was also the subject of another paper which included both a literature review as well as carrying out unstructured interviews of a number of participants (Borkovich & Skovira, 2020). The research in this paper focused on the

cybersecurity risks to organisations of employees working from home, highlighting that “people are exposed as the weakest link in organisations”. The report identified that employee error that was not deliberate, but resulted from careless cybersecurity behaviour was a significant threat to an organisations information security. In line with the findings of the other report (Georgiadou et al., 2022), training was identified as a key aspect, with this research highlighting that cybersecurity training is typically not carried out on a routine basis, only when a person joins an organisation. Whilst the literature review carried out by this research was interesting, it was the insights gained from the unstructured interviews carried out with managerial and professional employees that reinforced the human factor risk, with employees carrying out riskier behaviour relating to cybersecurity when working from home. As stated earlier, the focus of this study was the risks to the organisation. Even when considering the subject of personally identifiable information, the focus was more on limiting the impact to the organisation than the individual. In both of these papers on increased cybersecurity risk resulting from employees working from home due to Covid-19, the focus is on the risk to the organisation, not the risk to the individual. Increased cybersecurity risk for the individual is not a key focus of either study. The research recommends implementing a working from home corporate culture focused on 6 C’s, these being Control, Collaboration, Communication, Cost, Cloud, and Culture. Whilst human behaviour isn’t specifically highlighted in this list, it clearly needs to play a role in the cultural paradigm shift that is required. The report concludes highlighting the need for awareness building and training that should be regardless of the workplace location.

Although human behaviour isn’t the specific focus of either of the papers on cybersecurity and the shift to working from home during the Covid-19 pandemic, both of the reports reinforce that human factor is the weakest link in cybersecurity and needs to be a key focus for organisations. Both reports also highlight the need for increased knowledge and awareness for individuals and the need for this to translate into behaviours and actions. However, neither report addresses the potential impact of working from home on personal cybersecurity, with the focus of both papers being on what is needed to protect organisations.

This further highlights the findings from the review of literature relating to cybersecurity and human behaviour prior to the Covid-19 pandemic, that there is a significant gap in research relating to human cybersecurity behaviour in both personal and work life contexts.

This supports the aims of this research, leading to confirming the research question in the following section.

2.3 Research Question

The over-arching research question was originally framed as follows:
"Are there similarities and differences in the human behaviours that individuals exhibit relating to their personal life and their work life and can insights from these be leveraged to provide improvements in either context". During the course of the research, the researcher's interest shifted towards the new reality of extensive work from home and other non-office contexts during and post Covid-19 and the associated security issues. Subsequently the main research question was re-formulated as:

"What is the impact of the blurring of the lines between personal and work life contexts on human behaviour with respect to cybersecurity"
It was broken down to the sub-questions below:

- In a personal and work context are there behavioural differences that depend on the type of application/data being considered?
- What are the human behaviours that have contributed to successful cyberattacks against individuals and businesses and do these differ significantly?
- What barriers to improved cybersecurity do these identified behaviours generate?
- What are the options to mitigate any barriers resulting from human behaviours and are there learnings that can be applied across both contexts?

In this Chapter the outputs from the literature review carried out have been presented, which has confirmed that the aim of this research is valid. The research question and sub-questions have been adjusted slightly and confirmed. The next Chapter presents the research design and methodology that will be used the answer the research questions.

3 Research Design and Methodology

3.1 Research Approach

An initial literature review was carried out to identify current research carried out in the field of human behaviour and cybersecurity. The findings from this review are summarised in the previous Chapter. The output from this literature review confirmed that there had been only limited research carried out relating to the research question and that this was a relevant study to carry out.

Following the literature review, it was decided to adopt a qualitative approach to gather further data and to carry out interviews of several participants to gain insights into their behaviour relating to cybersecurity regarding both their personal and work life online activity.
The nature of the research question and that it was focused on understanding what behaviour was being carried out by humans in their personal and work lives relating to cybersecurity leant itself more to a qualitative approach than a quantitative approach. As noted in (Crabtree) 2022, quantitative methods are best suited for research that involves experiments such as tests while qualitative methods work well for identifying and describing problems, and generating explanations. A quantitative approach may be useful as future research work to add numerical metrics to the findings identified here, however we first need to understand the behaviour being carried out and the impacts, for which a qualitative approach is more suited.

3.2 Research Design Steps

The design of a qualitative research study provides the research project plan; it starts with formulating the research question and includes determining the study sample, among others steps (Flick, 2022) The research design steps for the research carried out for this study are shown in Figure 1.

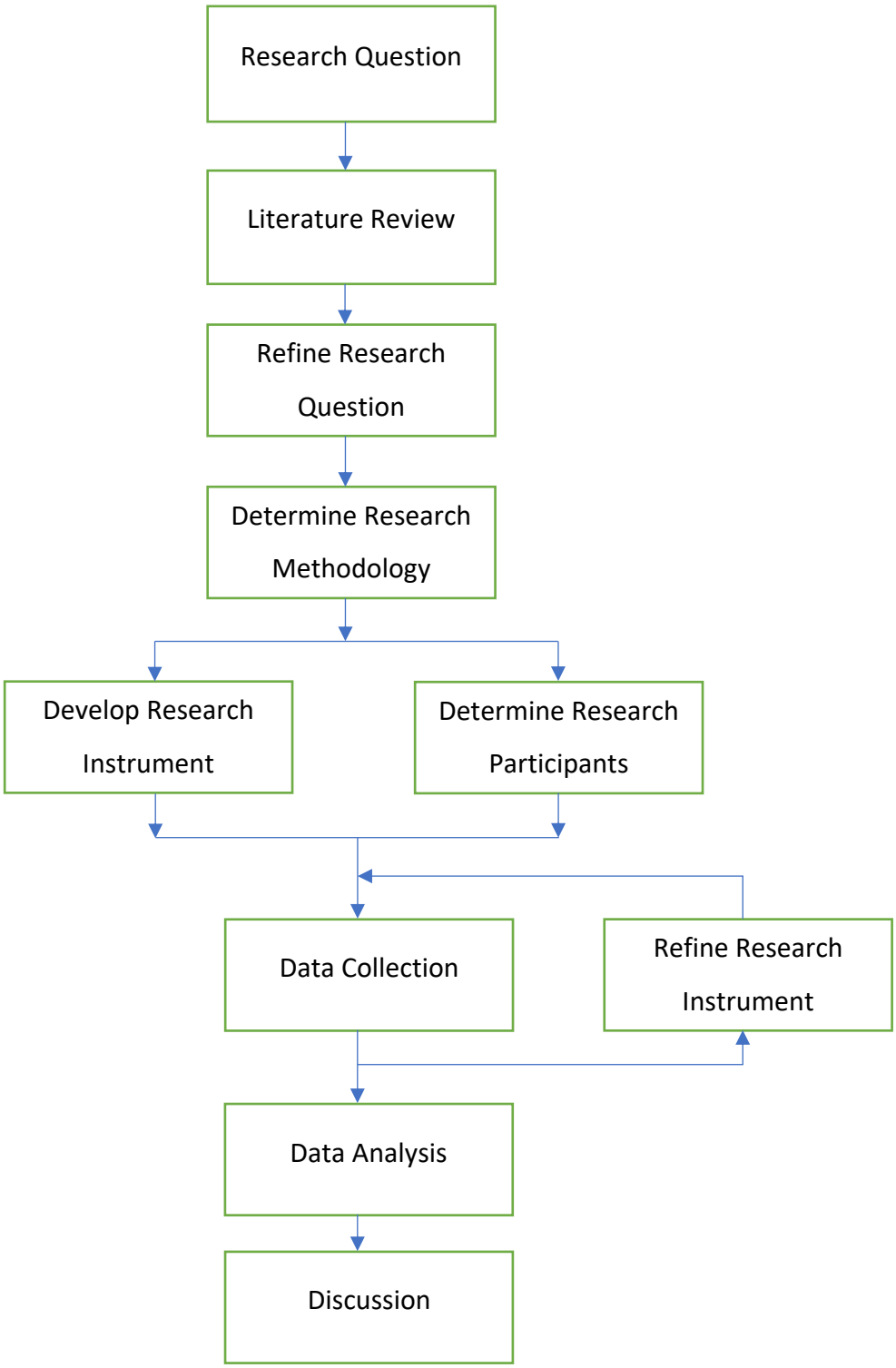

Figure 1. Research Design Steps

The research question, literature review and refinement of the research question are outlined in Chapter 2 of this thesis. The research methodology selected was to use a qualitative research methodology, which is described in more detail in the following sections.

3.3 Research Methodology

The research methodology adopted covers the four dimensions of the research approach or tradition, as outlined in (Durdella, 2019), these being:

1. Researcher roles
2. Data collection methods, instruments and procedural details
3. Data sources, sampling and setting
4. Data analysis procedures

In terms of researcher roles, this research is being carried out by a single researcher (the author) who carried out data collection, sources and sampling and analysis dimensions. These three other dimensions are described in more detail in the following sections of this thesis.

3.4 Behaviour and Cybersecurity Models

From the paper discussed in the literature review that focused on cybersecurity culture when working from home during the Covid-19 crisis (Georgiadou et al., 2022), a cybersecurity culture model was described, which included the different dimensions of the model at both an organisational level and an individual level. At an individual level, the four dimensions were identified as:

1. Competency
2. Attitude
3. Awareness
4. Behaviour

This is shown in Figure 2.

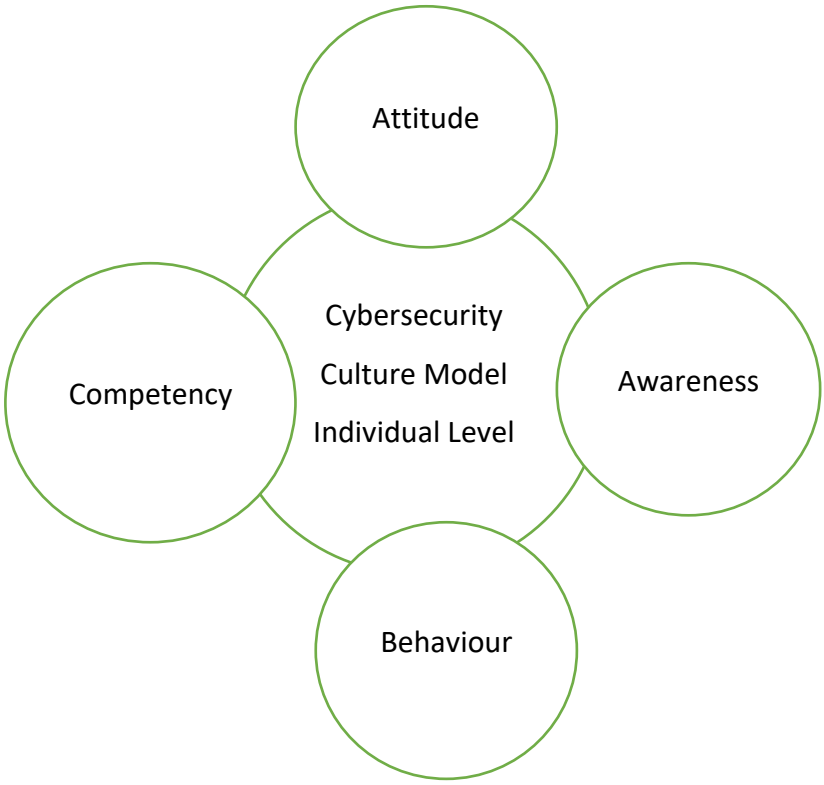

Figure 2. Cybersecurity Culture Model – Individual Level (Georgiadou et al., 2022)

When considering human behaviour relating to cybersecurity, an individual's behaviour is informed by the other three dimensions, i.e., competency, attitude and awareness.

For the purposes of this study, it was decided to modify this model slightly to address how some dimensions are informed by others. Also, some of the dimension names were modified slightly to better reflect the dimensions of this research. The intention of this research was not to consider or assess malicious behaviour and the research participants were selected on this basis. Attitude can therefore be considered as the intentions of the participants. Competency can also be considered as knowledge – i.e., the knowledge that the participants possess in the field of cybersecurity. Awareness is closely related to competency and knowledge. A definition of behaviour is "the way in which one acts or conducts oneself, especially towards others" (Oxford University Press, n.d.). Put simply, this can be considered as the actions that an individual takes based on their knowledge, awareness and intentions. A revised model when considering individual cybersecurity culture can therefore be represented as in Figure 3.

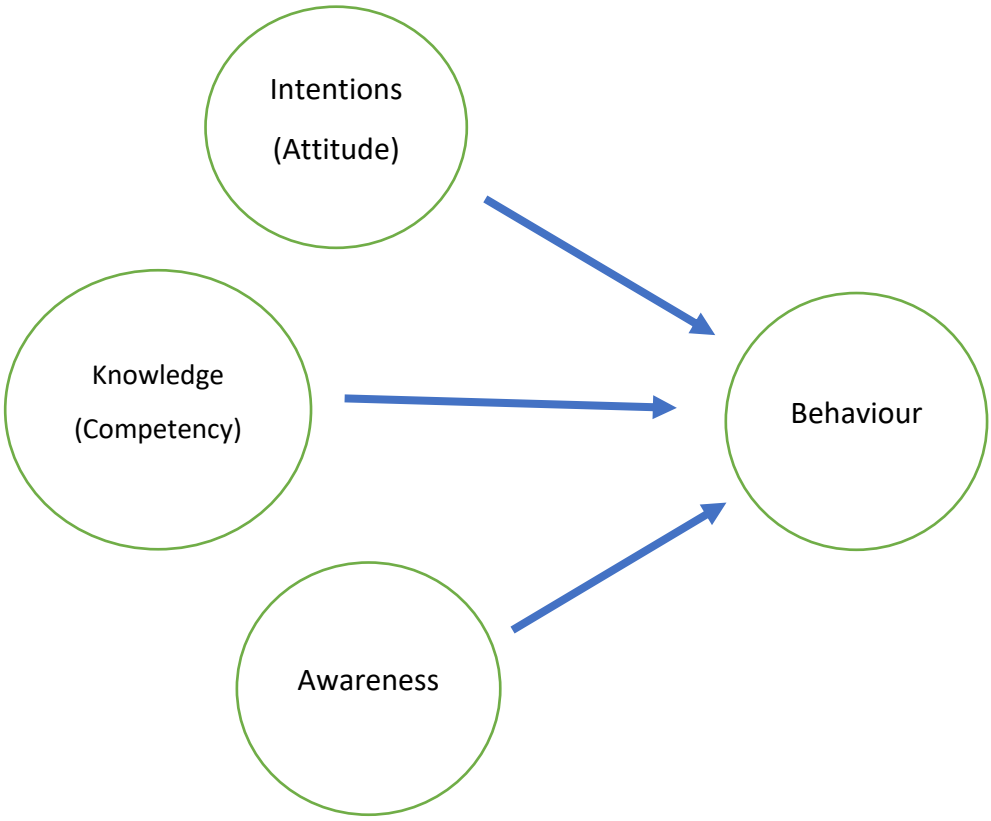

Figure 3. Revised Individual Level Cybersecurity Culture Model

When considering the above behaviour model and applying it to cybersecurity in a personal and work context, we need to consider a number of dimensions, including:

1. The devices being used, which may include smartphones, laptops and tablets
2. The networks over which information and data is transmitted and received
3. The applications being used, and type of activity being carried out.

These three dimensions are shown in Figure 4.

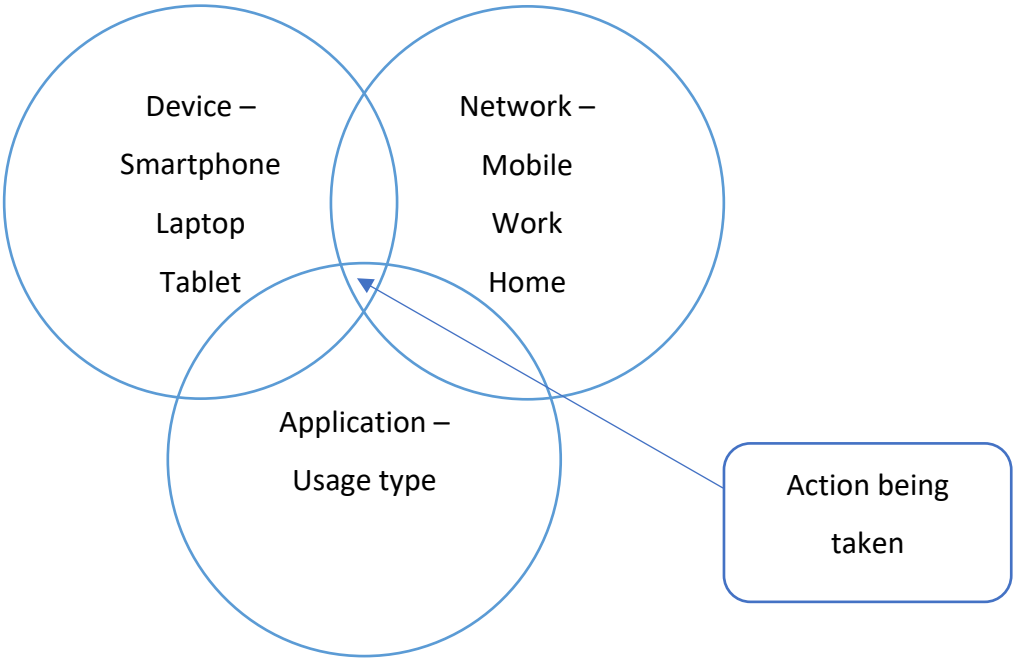

Figure 4. Cybersecurity Dimensions Model

All three of the dimensions shown in Figure 4 are needed for an online action to take place, so we need to consider the behaviour relating to all of these aspects when addressing cybersecurity. This will be used in the data analysis phase.

3.5 Data Collection Method

The method chosen to collect the data was to use semi-structured interviews, making use of pre-prepared sample questions as prompts to help guide the interviews and ensure that they didn't stray too far from the research question being addressed. This method was chosen as it strikes a balance of not being too rigid so as to restrict the discussion so much that key insights may be missed, but also ensuring they are guided and focused on the aim of the research and the research question being addressed (Crabtree, 2022).

A sample list of questions was developed that was used as a prompt to help drive the discussions with the interview participants. It should be noted that this was only a list of sample questions as it was expected that each interview might potentially lead to further questions to explore insights obtained from the interviews in more depth. The initial list of sample questions is shown in Table

1. The sample questions were informed by the cybersecurity dimensions shown in Figure 4, by including the three dimensions of device, network and application. The questions were also informed by the cybersecurity culture model shown in Figure 3, regarding aspects such as knowledge and intentions.

Table 1. Sample List of Questions

No.	Question
1	Do you have separate personal and work laptops and mobile phones?
2	Where you have a choice, what is you preferred access security mechanism on your devices (e.g. password, PIN, fingerprints, face recognition)?
3	Do you use your work laptop and/or phone for personal use, e.g. social media, online banking, online shopping?
4	Do you use your personal laptop to carry out work tasks/activities?
5	Do you use your personal laptop over a work network and if so, has it been modified to achieve this?
6	Do you use your personal and/or work devices on publicly available Wi-Fi networks, e.g. cafes, hotels, etc.
7	What type of activities do you typically carry out over public Wi-Fi?
8	Are there any types of activities that you never carry out over public Wi-Fi? If so what and why?
9	For your personal activities, do you apply different levels of security (e.g. more complex passwords) for different activities (e.g. banking, social media, ….)?
10	How often do you change password for both personal and work devices and applications?
11	What prompts or triggers you to change passwords?
12	Do you make use of any password manager applications (e.g. Apple Keychain)?
13	How you ever been the victim of a cyberattack (e.g. phishing attempt) and if so, what was the impact?
14	Are you concerned about identity theft? What precautions (if any) do you take against this?
15	Have you received cybersecurity and/or privacy training at work? If so, do you apply any of the learnings from this for your personal life?
16	What anti-virus software do you use for your personal devices?
17	To what level do you intentions regarding cybersecurity match your actions?
18	Has your approach to cybersecurity changed as a result of working from home more due to the Covid19 pandemic?

The purpose of the sample questions was to gather insights into the following, and therefore needs to include aspects from the cybersecurity culture model in Figure 3 and the cybersecurity dimensions model in Figure 4:

- level of awareness of cybersecurity
- behaviours relating to cybersecurity in particular contexts/scenarios
- possible reasons why behaviours may vary in different contexts
- existence of any barriers to applying more rigorous cybersecurity disciplines in a personal or work context
- specific aspects relating to use of own devices in a work environment and/or use of work devices in the home environment

3.5.1 Research Sample

Purposive sampling was used to select the interview participants, based on their ability to contribute the research topic. Purposive sampling "is the deliberate choice of a participant due to the qualities the participant possesses" (Etikan et al., 2016, p. 2) . This sampling method was chosen because there was a higher likelihood of collecting data that is useful in answering the research question if the participants met the following criteria:

- Were likely to carry out work activities at the office and at home
- Had laptop computers and/or tablets enabling them to work remotely
- Made use of both mobile devices such as smartphones and laptops or tablets to carry out both personal and work tasks
- Had a mix of own and company provided devices and network accounts

Purposive sampling was also chosen to be able to include some participants that had worked in roles in telecommunications organisations as well as some that had worked in roles involving cybersecurity. To meet this and the above criteria, the participants were selected from members of the researcher's professional network.

A total of 9 participants were interviewed, which included:

- 3 participants that who had worked in roles involving cybersecurity
- 4 participants who had worked in roles in telecommunications organisations
- 2 participants that had worked in other non-technical industries

The research approach to interview participants required approval by the Auckland University of Technology Ethics Committee, which was granted on 29 June 2021, AUTEC Reference number 21/145. The approval letter is included as Appendix A.

Participants were provided with an information sheet providing details about the research and they were each required to complete a research consent form. These two documents are included in Appendix B.

3.5.2 Interview Process

Interviews were carried out online using Zoom. Whilst the video was enabled so that both the researcher and interviewee could see each other, only the audio was recorded and transcribed. The recording and transcription were carried out using Otter.ai. Otter.ai is a technology company based in California that provides software providing real-time transcription and recorded audio. Overall, the transcription was mostly accurate, although some editing of the transcripts did need to be made. Because the audio was recorded, it was relatively straightforward to check the audio and edit the transcript, and it was also relatively easy to understand why the transcript wasn't accurate where it needed to be corrected. The Otter.ai software also performed well identifying which speaker said what, although in some cases it didn't get the start or finish of when one speaker finished, and the other speaker started completely accurate.

Another issue encountered was that for one of the interviews, the recording device had connected to a router further away in the home and the weak network meant that the online transcription did not work well. This was resolved by replaying the recorded audio through the transcription software. It was also a good learning for the following interviews to check network connectivity at the start.

The duration of the interviews ranged between 29 minutes and 48 seconds and 44 minutes and 20 seconds. The average duration across all interviews carried out was 38 minutes and 37 seconds.

The transcripts of the collected data is included in Appendix C.

Some comparison of the findings with other research is discussed in Chapter 5, Further Analysis and Discussion.

3.5.3 Questionnaire Development

A pilot interview was carried out to

(a) to assess the likely length of the interviews based on the sample questions, and

(b) to try to ascertain whether there were any key areas missing and questions that should be added to help drive the discussion.

The pilot interview confirmed that based on the proposed sample questions the length of the interviews would be as expected, with the pilot interview being recorded as lasting approximately 35 minutes. This was in line with what was communicated in both the ethics approval submission, as being a reasonable length for an interview, as well as what was communicated to participants in the information sheet. An additional topic area identified from the pilot interview was whether the size of an application or service provider influenced the participants use of them, which was added to the sample questions.

The initial list of sample questions used is shown in Table 1. It should be noted that the questions were used to trigger further discussion during the interviews, generating additional insights as well as additional questions that were used in future interviews. The approach adopted for carrying out the interviews was an iterative approach, where new insights gained from each interview were captured and which were the used to enhance the questioning for the following interviews. This approach enabled richer insights to be obtained as further interviews were carried out.

To gain insights into cybersecurity human behaviour in both a personal and work life context, the interview questions took a methodical approach, starting with understanding the various personal and company provided smartphones and laptop computers/tablets that the participants used, and

then looking into the networks that these devices are operated over, and then moving onto the types of activities and applications that are used on those devices and over those networks. The interviews and questions also covered aspects such as identity authentication (e.g. passwords, biometrics), training and guidelines that the participants have received, and considerations such as the increasing number of smart devices that are now connected to the home network.

Although initially the questions were informed by the two models, during the first few interviews additional dimensions came to light, such as smart devices on the home network. Several additional questions were added to the list and they were grouped into the following areas:

- Devices
- Identity Authentication
- Networks
- Apps
- Cyberattacks
- Identity Theft / Privacy
- Training
- Working From Home (WFH) and Behaviour
- Smart Devices

These groupings and the additional questions that were added are shown in Table 2.

As can be seen in Table 2, as the interviews progressed the number of questions more than doubled with questions on the following topic areas being expanded in order to explore these areas in more detail in subsequent interviews that were carried out:

- the home network and smart devices
- training and guidelines from employers or other organisations

Table 2. Updated Sample Questions

Area	No.	Question
Devices	1	Do you have separate personal and work laptops and mobile phones?
	Added	Do you have a fixed shared home PC? Is this used for work at all?
	3	Do you use your work laptop and/or phone for personal use, e.g. social media, online banking, online shopping?
	4	Do you use your personal laptop to carry out work tasks/activities?
	5	Do you use your personal laptop over a work network and if so, has it been modified to achieve this?
	16	What anti-virus software do you use for your personal devices?
	Added	Do you carry out personal activities such as banking, online shopping and social media on work devices and/or networks?
	Added	Do you store personal data on work devices and vice versa?
	Added	Do you use device auto-locking mechanisms?
Identity Authentication	2	Where you have a choice, what is you preferred access security mechanism on your devices (e.g. password, PIN, fingerprints, face recognition)?
	9	For your personal activities, do you apply different levels of security (e.g. more complex passwords) for different activities (e.g. banking, social media, ….)?
	10	How often do you change password for both personal and work devices and applications?
	11	What prompts or triggers you to change passwords?
	12	Do you make use of any password manager applications (e.g. Apple Keychain)?
Networks	Added	Do you use your work devices over your home network?
	Added	Is your home network shared with family and friends?
	Added	Do you ever change your home network password? If so, how often?
	Added	How widely is your home network password shared?
	Added	Do you know what level of security is supported on your home network?
	6	Do you use your personal and/or work devices on publicly available Wi-Fi networks, e.g. cafes, hotels, etc.
	7	What type of activities do you typically carry out over public Wi-Fi?
	8	Are there any types of activities that you never carry out over public Wi-Fi? What and why?
Apps	Added	Does app popularity / volume of users influence your choice of what apps to use
Cyberattacks	13	How you ever been the victim of a cyberattack (e.g. phishing attempt) and if so, what was the impact?
	Added	Awareness and experience of different threats such as phishing, ransomware attacks etc.?
Identity Theft & Privacy	14	Are you concerned about identity theft? What precautions (if any) do you take against this?
	Added	Are you concerned about device cameras?
	Added	How do you think about your digital footprint and what you post online?
Training	15	Have you received cybersecurity and/or privacy training at work? If so, do you apply any of the learnings from this for your personal life?
	Added	Have any of the organisations that you work for provided guidance and/or policies regarding cybersecurity and use away from the office? Has this changed pre/post Covid?
	Added	Any training or guidance regarding personal/home usage/cybersecurity?
WFH & Behaviour	Added	How often do you work from home? Has this changed before / during / after covid?
	17	To what level do your intentions regarding cybersecurity match your actions?
	18	Has your approach to cybersecurity changed as a result of working from home more due to the Covid19 pandemic?
	Added	How does trust influence how you behave?
	Added	Behaviour regarding forwarding emails, opening attachments, USB drives etc.
Smart Devices	Added	What other smart devices do you use and are connected to personal and/or work devices, e.g. smart TVs, smart watches, fitness bands
	Added	Are you concerned about wearables giving away your location? Home robberies?

3.6 Research Aim and Selected Methods

The aim of this research is to investigate how the blurring of the lines between personal and work contexts impacts human cybersecurity behaviour.

The selection of a qualitative approach using semi-structured interviews and purposive sampling aligns with the research aim in that it enables collection of in-depth data across the various topics relating to human cybersecurity behaviour in both personal and work contexts, by capturing information and insights from the participants personal experiences and perspectives.

In particular, the semi-structured approach enabled new insights to be explored further whilst keeping the interviews focused on the aim of the research.

A questionnaire to a larger number of participants was considered, and this may have provided more statistical data on specifc questions, but it would not have enabled insights to be surfaced from the more in-depth and interactive discussion that can be achieved with semi-structured interviews.

The use or purposive sampling was also important in selecting participants that were likely to have perspectives and experiences that would help answer the research question.

Recording and transcribing the audio from the interviews was essential in that it allowed the researcher to focus fully on the questions and the discussions, instead of making notes.

3.7 Data Analysis

The transcripts that were captured using Otter.ai were exported as Microsoft Word files. NVivo software from Lumivero was used to assist with carrying out the qualitative data analysis. Nvivo is qualitative data analysis software that helps with the organisation and analysis of the collected data. The Microsoft Word files from Otter.ai were loaded into Nvivo in preparation for analysis. Some data cleaning was required to correct errors in the transcriptions. This was done by comparing the transcribed text with the audio files where necessary. Also, where necessary, any identifying information was removed from the transcripts. As the interview transcripts were

reviewed, a number of codes were created to identify responses on similar questions and/or topics from the different participants.

3.7.1 Coding

Coding of the collected data was carried out using a combination of a deductive approach and an inductive approach. A deductive coding approach uses codes based on existing information on the subject, whereas an inductive approach generates the code from the collected data (Azungah, 2018). As described in the previous chapter, as more interviews were carried out, the questions were structured into logical groupings. Some of these groupings formed a logical starting point for the coding. For example, training is a logical grouping of the questions relating to training, so a code of training was used to mark participant responses that were training related.

Although deductive coding was used initially, the initial use of groupings of codes didn't fully provide the level of granularity needed. As the transcripts were analysed, the coding approach transitioned to an inductive approach, creating codes based on the data that was contained in the transcripts. An example of this is the phishing code, which logically sits in the attacks grouping, but the phishing code was created as the transcripts were reviewed.

3.7.2 Codebook

Table 3 shows the codebook exported from Nvivo, which shows the number of files that the codes appeared in as well as the total number of references for each code.

Table 3. Nvivo Codebook

Name	Files (Interview Transcripts)	References
antivirus	9	12
Apps	8	13
autolock	3	4
awareness actions	8	10
banking	9	18
cameras	4	5
Covid and WFH	7	12
culture	2	4
cyber attack	7	14
email attachments	4	5
guidelines	4	8
Home PC	1	1
home Wi-Fi	10	37
identity theft	9	16
laptop	9	16
laptop access	8	10
MDM	2	2
microphones	3	4
mobile access	8	12
mobile device	9	19
network	1	1
online shopping	6	12
password changes	8	19
password complexity	7	11
password management app	9	16
personal use	9	24
phishing	9	12
privacy	3	5
public Wi-Fi	9	21
Risk	3	3
separate debit card	6	6
smart devices	8	12
social media	7	9
training	9	21
trust	9	23
USB	3	3
work network	3	5
work use	8	22

3.7.2.1 Unit of Coding

The unit of coding varied. In some cases, it was a single sentence from the participant. An example of this was the following response from Participant E, which was coded against the code password changes:

Participant E: "I regularly change the password once a month"

In other cases, the unit of coding is a paragraph, i.e., multiple sentences that are spoken at the same time by the participant that relate to a specific code. An example of this, coded against mobile access and laptop access from Participant F is as follows:

Participant F: "Yeah, so I prefer fingerprint. However, it comes down to the functionality so fingerprint I have on my MacBook, which works really well. And the fingerprint on my phone is not good at all. So I rarely use it because it doesn't work properly. It doesn't seem to recognize my finger well. So therefore it would be PIN and here on my work one we don't have fingerprints, it's just log into the LAN thing. So it's password protected."

Some coding required the question from the researcher to be included to give the response from the participant the required context. An example of this for the code social media is:

Researcher: "you wouldn't do any kind of social media on your work computer?"

Participant E: "Nope. Anyway, you can't anyway. I wouldn't"

And in some cases, short conversations were coded as that dialogue was relevant to a particular code. An example of that is for the code training, where the dialogue between the researcher and participant B was as follows:

Researcher: "yeah, yeah, okay. Um, on your work environment, either this, your current work that you do or previous work have you ever had any cybersecurity privacy training from work."

Participant B: "Yes. But, yeah, fairly low key, fairly low key. It seemed as a team to, you know, a seminar when somebody will talk about the types of attacks and the types of things that worked as to try and defend them and, you know,"

Researcher: "has that training triggered you to do other things in your personal home life that you haven't done before or has cybersecurity training at work, for example, where you've attended a

seminar, whatever. Obviously, which is a focus on improving, you know, or getting better, cybersecurity behaviours at work has that then triggered you to do stuff in your personal life that's"

Participant B: "Uh I don't know its triggered me to change. Well, it is helped me look more critically at, you know, emails that come in, I guess, it made me more weary of emails from reportedly from Spark or Genesis or neon or whatever or Netflix, you know, when they arrive. I am thinking. First thing I'm thinking is, is that a fake. I guess it's made me apply a more critical view to unsolicited emails. Right, yeah, yeah, yeah. Yeah, okay, but that's about it. Yeah."

The Chapter has presented the research design and methodology that has been developed and used to address the research question. The findings are outlined in the following Chapter.

4 Findings

This chapter presents the key findings from the data analysis that was carried out once the data had been collected.

4.1 Devices

One of the key facts to understand from the participants was the range of devices that they have use of, whether these are their own personal devices or provided by their employer and whether they used these devices for personal use, work use or both.

4.1.1 Smartphones

Table 4 shows whether participants had smartphones that were provided by the organisation that they worked for, or their own personal smartphone. All of the participants have just one smartphone which is used for both work purposes and personal use in all but one case, with that participant only having very limited work usage on their personal smartphone.

Table 4. Participant's Smartphones and Usage

Participant	**Own Mobile**	**Work Mobile**	**BYOD**	**Personal Use**	**Work Use**	**Comments**
A	Partially	Partially	Yes	Yes	Yes	Own purchased phone, company contribution
B	No	Yes		Yes	Yes	
C	No	Yes		Yes	Yes	
D	Partially	Partially		Yes	Yes	Own business
E	Yes	No		Yes	Only occasional work messages and Teams calls	
F	No	Yes (Dual SIM)		Yes	Yes	
G	No	Yes		Yes	Yes	
H	Yes	No	Yes	Yes	Yes	
I	Yes	No	Yes	Yes	Yes	

Three of those interviewed can be considered Bring-Your-Own-Device (BYOD) scenarios (Veljkovic & Budree, 2019), including the participant who purchased their own phone but received a company contribution for part of the cost of the device. BYOD phones by their nature are used for both personal and work usage as that is partially why BYOD came into existence. In all cases where the smartphone is a company provided device, those devices are also used for personal use. One of those interviewed is a small business owner so effectively has a phone that is used for both business and personal usage. Another of those interviewed has a dual-SIM device enabling it to be used for personal and work purposes over different networks. One of the participants has their own smartphone that they do not use for work other than to receive work related messages or the occasional Microsoft Teams call.

Company provided smartphones are potentially subject to Mobile Device Management (MDM) by the company, although this was only confirmed in one case.

4.1.2 Computers, Laptops and Tablets

When it comes to computers, laptops and tablets, the situation is more complex, with many of the participants have multiple devices, some of which are used for work purposes, some for personal activities and some for both. This is shown in Table 5.

Table 5. Participant's Laptops and Tablets

Participant	Laptop & Tablet Devices	Usage
A	Own Laptop	Personal use and work use using VDI (BYOD)
B	Family home PC	Personal use, online banking & shopping
	Work iPad, Laptop & Tablet	Work use
C	Own iPad Pro	Personal use
	Work Laptop	Work use
D	Own Samsung Tablet	Personal emails, Contacts
	Work Laptop	Work use, but also personal emails
E	Own Laptop	Personal use
	Work Laptop	Work use, occasional personal use e.g. browsing, online shopping
F	Own MacBook	Personal use, possibly as backup alternative to work tablet / laptop
	Work Tablet / Laptop	Work use and personal use due to touch screen functionality (e.g. signing contracts)
G	Household iPads	Shared household use
	Work Laptop	Work use and personal use – uses work email, online banking, personal documents e.g. passport
H	Own PC (Laptop?)	Personal use
	Work Laptop	Work use, some surfing the net
I	Own Laptop	Personal use
	Work Laptop	Work use, accessing personal email, online banking, personal receipts on work address

All participants except one have a company provided laptop or tablet, with one participant having multiple company devices. The participant without a laptop device from their employer uses their own laptop with Virtual Desktop Infrastructure (VDI) capability to access their work network. In this case the laptop was used for both personal and work purposes. For participants that had both their own laptop/tablet as well as a company provided device, their own device was used for

personal use. In one case it was suggested that their own device could be used as a backup alternative if there were issues with the company provided device. However, there was some level of personal usage of company provided laptops / tablets, as indicated in Table 5. This varied from accessing personal email and doing some net surfing and browsing to using the work computer for personal tasks such as online banking and online shopping. In one case, the work device was used for signing personal contracts because it had better functionality than their personal device in that it had a touchscreen and stylus. In this case this resulted in a number of personal documents being stored on that device. One participant confirmed that they had a family personal computer that they used for carrying out most personal activities such as online banking and shopping.

4.2 Networks

As well as considering the devices that individuals use when carrying out personal and work activities, we also need to consider the networks that these activities are being carried out over. The typical networks that this could involve are:

- The mobile network of the mobile service provider
- The company's office-based network, which could be both a wired network as well as a Wi-Fi network
- The home network
- Public Wi-Fi networks at places such as airports, cafes and hotels

4.2.1 Mobile Networks

Of the participants interviewed, one had a personal phone operating over their own mobile connection and three had work provided phones operating over work provided mobile connections. The participant who purchased their own device but had a contribution from their employers also operated that device over a work provided mobile connection (i.e. similar to BYOD). One participant had a phone with a dual SIM capability with both a work provided SIM card and a personal SIM card. A limitation with this is that data communication only makes use of one of these SIM cards and so the participant using this phone used their personal SIM card in slot 1 of the phone over which all data communication takes place. Their reason for doing this was that most of their smartphone data usage is personal usage. It wasn't specifically clarified with the two

participants that have BYOD devices as to whether those devices are making use of personal or work provided mobile connections.

4.2.2 Work Networks

Work devices provided by an organisation are set-up to work over the office networks (both wired and wireless) when physically at work.

4.2.3 Home Networks

Laptops or tablets that are used for work in the home environment make use of the participants home broadband and wireless networks to connect into the organisation's network.
One participant had their own personal laptop that they also used for work, however their work use was partitioned using Virtual Desktop Infrastructure (VDI). In most scenarios, this behaved and gave the impression that the work use was separate from personal use and therefore not raising any security concerns for the participant. However, an anomaly to this was that when Teams calendar was used, it appeared in their personal workspace. This could indicate the personal and work activities are less partitioned than they originally thought.

One participant stated that their home network has been specifically set-up to be as secure as their office environment. Another of the participants confirmed that they only changed their home Wi-Fi password when they changed or upgraded the router. All participants allowed family, friends and guests to use their home Wi-Fi network by providing them with the password. One participant confirmed that they gave friends and guests a different guest access, although this didn't enforce any specific restrictions different from the family access. One participant confirmed that they have the home Wi-Fi password on the fridge. One of the participants that was interviewed had set up their home network with different zones with different restrictions. This gave them the option give visitors access to different zones if needed.

4.2.4 Public Wi-Fi

Participants were questioned regarding their use of Public Wi-Fi and some of the responses are shown in Table 6.

Table 6. Use of Public Wi-Fi

Participant	Public Wi-Fi Use
A	Phone Yes, Laptop No Regarding banking or online shopping, would consciously think about it – if had to they would
B	Airport Lounges and Hotels Yes, Cafes No But would do if really needed to
C	Would connect to a VPN or use mobile phone – more secure Probably wouldn't do banking on Public Wi-Fi
D	Yes and not really any restrictions
E	No as has unlimited data on smartphone which is more secure Possibly at hotel for work as they need to cater for that
F	Unlikely to use public Wi-Fi in a café as not there for long, but possibly would in a hotel. But not internet banking or credit card purchases
G	Yes at airport, but not banking or online purchases, except purchased an online book Not anything that is very confidential
H	No – would use a VPN and mobile phone
I	Not in cafés / restaurants, but would in Koru lounge including banking and online purchases

4.3 Applications and Type of Usage

To ascertain whether the behaviour of the participants changes based on the task or action being performed, questions were asked during the interviews of the types of tasks being carried out. These questions predominantly focused on financial tasks such as banking and online shopping as financial gain is a key motivation for many cyber-attacks.

Table 7 summarises the findings from the participants, which varied significantly. Some participants only carried out banking activities on their personal smartphone and never on their work devices or networks whereas others would occasionally use both home and work devices and networks. Questions were also asked regarding use of public Wi-Fi networks, such as at hotels, cafes and airports. Again, responses varied, with some participants never carrying out banking on a public Wi-Fi network, whereas others would occasionally.

Table 7. Types of Online Usage

Participant	Online Banking	Online Shopping	Social Media
A	Uses phone for online banking		
B	Would use smartphone and work devices to do online banking. Mostly uses family computer for online banking.	Would do anything on work devices if needed to. Mostly uses family computer for online shopping.	Does a little bit of social media on their phone
C	Uses work devices for online banking		Uses work devices for social media and doesn't have concerns doing that
D	Uses phone and laptop for online banking	Uses PayPal as a means of paying, so rarely uses credit card directly with a supplier	Doesn't belong to any social media
E	Would usually do online banking on mobile or personal laptop. Gets comfort from two factor authentication.	Occasionally might use work laptop for online shopping, but usually would use phone or personal laptop. Will only shop on what they consider to be trusted and well-known sites. They may test out a site with a smaller purchase first.	Wouldn't do social media on work computer. Limited use of social media and limited number of friends. Any social media is typically done on the phone. Rarely uses personal computer for social media.
F	Does not do online banking on work device	They have done online shopping once or twice on their work device	Uses LinkedIn on work device, but not Facebook
G	Does use work laptop for online banking	Has used credit card for online shopping on work laptop Doesn't use phone for online shopping.	Typically, doesn't post on social media, but if did it would be on the phone. Use Messenger to message parents from work computer.
H	Would use phone to do online banking	Tends to use phone for online shopping	Only really uses LinkedIn, which is work related
I	Would use work laptop for online banking	No does not do online shopping on work laptop. Would use personal laptop for online shopping	Only LinkedIn on work laptop. Uses own devices for Instagram.

When it comes to online shopping the participants adopted different approaches to reducing the level of financial risk. Three of the participants make use of a different debit or credit card than their usual card with a lower limit for carrying out online purchases. This was done to limit the

level of financial risk. Another participant didn't use a separate card but would only use a credit card for online purchases as it is covered for fraud. One participant said that they hardly ever save their credit card details online, with a couple of exceptions.

4.4 Identity Authentication and Password Management

Participants were asked what their preferred mechanisms were for accessing their devices and applications. For work related devices and applications, this is controlled and governed by the organisation which removes the choice of the individual for these.

Where passwords were used, participants were also asked how often they change their passwords and whether what, if any, were the triggers for them to change. For access to work devices and apps the password change frequency is typically mandated by the organisation.

Table 8 shows participants preference of identity authentication mechanism for accessing their devices along with any reported work requirements and whether they make use of any password management system. Table 9 includes participants responses regarding password changes and complexity.

Table 8. Identity Authentication

Participant	Personal Preference	Work Requirement	Uses A Password Management System
A		Phone – PIN Laptop – Password + Two Factor Authentication	No – tried but couldn't get into it
B	Password		No
C	Mixture, predominantly PIN	PIN (6-digit) or Facial Recognition, Microsoft Authenticator	Yes, Apple Keychain and Google Chrome
D	Phone – facial recognition, fingerprint and PIN Laptop – password, increasingly sophisticated		Yes, password vault (but coded notebook backup)
E	Biometrics / Fingerprint	Password	No – trust issue
F	Fingerprint – but depends how well it works. Uses PIN on smartphone as fingerprints don't work well.	Password – doesn't support fingerprints	Yes – password manager auto-generated
G	Password	Laptop – password, but will be eye & fingerprint Phone – thumbprint	No. Coded password book
H	Password with Multi Factor Authentication		Yes – different for personal & work
I	PIN (joint with Spouse)	PIN or facial recognition	Yes – LastPass

Table 9. Password Changes and Complexity

Participant	Password Changes	Password Complexity
A	Work – every 3 months Personal – only occasionally, if forgotten or the sensible thing to do	More complex passwords for things like banking and RealMe, but one password used for other stuff
B	Not often. Once in a while for work VPN and online banking	Complex passwords for work VPN and online banking
C	When Chrome saying that password was included in a data breach Work mandates change every 90 days Personal – Google and Apple, never change	Has a lot of different passwords, but some commonality. Has same password across two dozen different things for years
D	Bank password – every 3 months, and other sites where making money (triggered by alarm in calendar)	Some older simple passwords, but moving to more complex passwords at least 10 digits long
E	Regularly, once a month	
F	Sometimes, but not really needed due to password managers. Change if password has been compromised Work – regularly in previous jobs, but not current job	Auto generated passwords, except some historical accounts before auto generated passwords were available
G	Work laptop – change all the time Phone and banking – never change it Only due to failed attempts forces change	So many different passwords for different things, has a little black book (coded). Three kinds of standard passwords with slightly different endings.
I	Two PINs – never changed	

Participant D was more concerned about not getting access when needed than about being hacked. In the 'CIA Triad', this is the Availability dimension.

Participant H noted a perspective that for someone on a farm in the middle of nowhere, having passwords in a notebook is probably quite secure as you would have to drive out there to get it.

4.5 Identity Theft and Privacy

Participants were asked how concerned they are regarding identity theft and privacy. Views and comments expressed by participants are shown in Table 10.

Table 10. Identity Theft and Privacy

Participant	Responses
A	"Don't think about it much, but thinking about it more" Thinking about whether to use a fake birthday
B	"I don't know anybody personally has suffered from it" "I don't have a social media presence, that I'm concerned about protecting"
C	"I'm aware of mechanisms that are out there, try and get hints, tips, information that can lead to passwords" "I just have the view that I'm just not that interesting"
D	"I don't quite understand how they do it or what they do about it. I haven't had the experience of it. So I'm not too concerned about"
E	"It does does play on my mind a little bit" Sees people falling for questions such as "choose the song from the decade that you were born"
F	"I wouldn't say that I'm worried about identity theft, but I'm very aware of it" "I wouldn't be sharing my personal information that would be associated with my identity, willy nilly unless I thought that it was actually necessary to identify myself"
G	"So there's definitely a digital footprint there in terms of social media in general, things like that. I don't tend to give away much of my details, or as little as possible, and I tried to use the security settings so that not you know, it's not open to anyone" "but my information is definitely out there"
H	"if your identity is gone all of those other things go and go with it" "one of my big fears is actually more along the lines of, you know, a relative getting done or something along those lines" "I access the internet, therefore, I have no privacy"
I	"very aware of what I do, how I how I transact, but also the cases what I access from that point of view as well. And it's more probably more around my visa or bank cards rather than anything else" "I'm not on Facebook and I'm not on Twitter if anything on Insta It was either commenting on a friend's picture or commentary or posting something random"

4.6 Smart Devices on the Home Network

Some of the interviews provided information about the participants home networks and the smart devices that are connected to those networks. This is shown in Table 11.

Table 11. Smart Devices in Participants Homes

Participant	Smart Devices	Concerns and Comments
C	Amazon Alexa, Apple TV, Smart TV, Printers	No concerns – doesn't see how you could hack into them without access to the property. "I've never heard of any kind of big security breaches as a result of Apple TV or, or Amazon Alexa so I just don't worry about it"
D	Connected TV, Watch	Just watch Netflix on TV – no concerns around that. Watch is just connected to the phone, so no concerns on that either
E	Smart TV	"I have until recently avoided smart devices in the home" Regarding Smart TV: "I don't know how secure that is"
F	Alexa, Sonos, Smart TV, Smartwatches	"Probably the biggest thing that is concerning is Alexa Voice listening" "I suppose I feel that the benefit of Alexa outweighs that risk or that concern"
G		No smart devices, so no concerns. Watch Netflix on a laptop connected to a TV (not a Smart TV)
H		"having everything on the same network is just insane to me, it's just basically increasing your attack surface exponentially" Doesn't have Amazon Alexa
I	Smart TV	No concerns as any apps used on the Smart TV are set-up with passwords

As can be seen from some of the comments above, the views expressed by participants relating to cybersecurity risks of smart devices connected to the home network ranged from having no concerns at all to considering have all devices on the same network as being very high risk.

4.7 Cyberattacks

Participants were asked whether they had been the target of any cyberattacks. Responses included those that had their credit cards or bank accounts compromised, which could have been caused by other reasons other than cyberattacks. Table 12 summarises the responses relating to this.

Table 12. Cyberattacks

Participant	Cyberattack Response
B	Notified by the bank of a weird transaction on their credit card – resulted in credit card being replaced.
C	Made a purchase on well-known social media application, which turned out to be a fake advert. Had trusted that Facebook "would actually like not take money from criminals". Had spotted the attack quickly and had had to cancel credit card and change passwords used on other sites.
D	Money transferred from bank account by unauthorised party. Password to account obtained from hacked computer. Account passwords weren't being changed regularly. Also had incorrect items charged to Visa card. Received email from known person requesting the participant to buy something and they will pay them back. Contacted known person by phone, whose email had been hacked.
E	Has had credit card compromised – how is unknown. Has also received phishing attacks both mobile email and text.
G	Has received phishing emails at work, which were reported. Partner's Hotmail hacked – informed by contacts receiving emails from it. Credit card was cloned abroad, which was traced back to a taxi ride.

Regarding the purchase on the social media application by participant C, this primarily resulted because the participant trusted that the social media application would not allow that type of criminal activity by third parties on their site.

The compromised bank account of one participant was believed to be due to passwords not being changed by the other account holder.

4.8 Training

Participants were asked questions regarding whether they had received cybersecurity training from the companies that they had worked for. Key insights regarding training are as follows:

- Seven of the nine participants have received some level of cybersecurity training from organisations that they work for or have previously worked for.
- For two of these participants the training was done on a regular basis or more than once.
- Four participants worked for organisations that use phishing tests to test cybersecurity awareness.
- The training provided by one organisation focuses on personal cybersecurity awareness, which it believes is a different approach to most organisations where the focus is on protecting the company. They believe that by taking a personal approach, it will be more effective in developing a cybersecurity mindset in individuals, which will then have benefits for the organisation.
- One of the participants noted that the cybersecurity training that they had received had been from larger organisations and they had not received training from a small company that they worked for.
- One participant indicated that the training that they had received at work had helped them to look more critically at emails.

4.9 Awareness, Intentions and Actions

Table 13 captures some key comments made by participants when asked about how their actions matched their intentions regarding cybersecurity.

Table 13. Intentions and Actions

Participant	Comments
B	"I know I take some actions but not as many as I should" "I've never paid attention to whether I'm on a, you know, whether I should be more concerned when I'm using the airport Wi-Fi or the hotel Wi-Fi"
C	"I think he area where I'm, where I don't follow through to the extent which is kind of ironic actually is probably the most important one is probably passwords"
D	"now identity threats I hadn't really thought about, cybersecurity to me is having people mostly around money somewhere, getting some money from you in some way"
E	"Probably hasn't changed a lot because I was aware beforehand"
F	"I mean, knowing what I know, I should definitely have better practices. But yeah, it's just it's another administrative task, isn't it?" "But then it's also not something that you really talked about with people"
G	"I think I am quite paranoid about stuff. So I think I am cautious. Yeah, I think I am cautious that I cautiously I'm always making sure that everything's logged off or logged out"
H	"let's be honest, you know, not everyone practices, what they preach but having said that, I'm never along the lines of everybody must always do something. I totally recognize that people are human and there are always going to be some sort of exceptions and that's why making sure that people's intentions are correct. And if they're informed and they're aware, they will do the best they can"
I	"there's probably stuff I take for granted but overall it's anything that I'm sharing around personal information, or identity, banking financial I'm extra vigilant around what am I doing, who's on the recipient"

A number of the participants were aware that their actions didn't always match their intentions and that they should have better cybersecurity behaviour practices.

4.10 Working From Home (WFH) and Covid-19

Whilst Covid-19 and the resulting lockdowns forced many people to work from home, three of the participants said that they already had some element of working from home and the capability to do so. One participant has changed from predominantly being five days a week in the office to now three days a week, with the other two days working from home, although they stated that their approach to cybersecurity had not changed. Another of the participants works for an organisation where the workforce is home-based.

One participant had a view that there was more personal and work life separation before the pandemic and that the pandemic had taken people's focus away from cybersecurity as we were all busy dealing with the impacts of the pandemic. They expressed a view that because there were no big cyberattacks or terrorist attacks (in their view) it had made us more complacent when it comes to cybersecurity.

4.11 Categories and Themes

It can be seen from the findings above that the codes have been grouped into categories. Whereas "to codify is to arrange things in a systematic order", to categorize is "to make something part of a system or classification" (Saldaña, 2016, p. 9). The 38 different codes have been consolidated and mapped to the following categories:

- Devices
- Networks
- Applications and types of usage
- Identity authentication
- Identity theft and privacy
- Smart networks and devices
- Training
- Awareness, intentions and actions

The first three of these categories relate to the cybersecurity dimensions model shown in Figure 4, with the last two categories relating to the cybersecurity culture model shown in Figure 3.

From the model in Figure 4, we can see that as a minimum a device, a network and an application are all required for an action or online activity to take place. The device being used and the network over which the communication flows together can be considered as the infrastructure that is being used. The grouping of related codes into categories is shown in Figure 5.

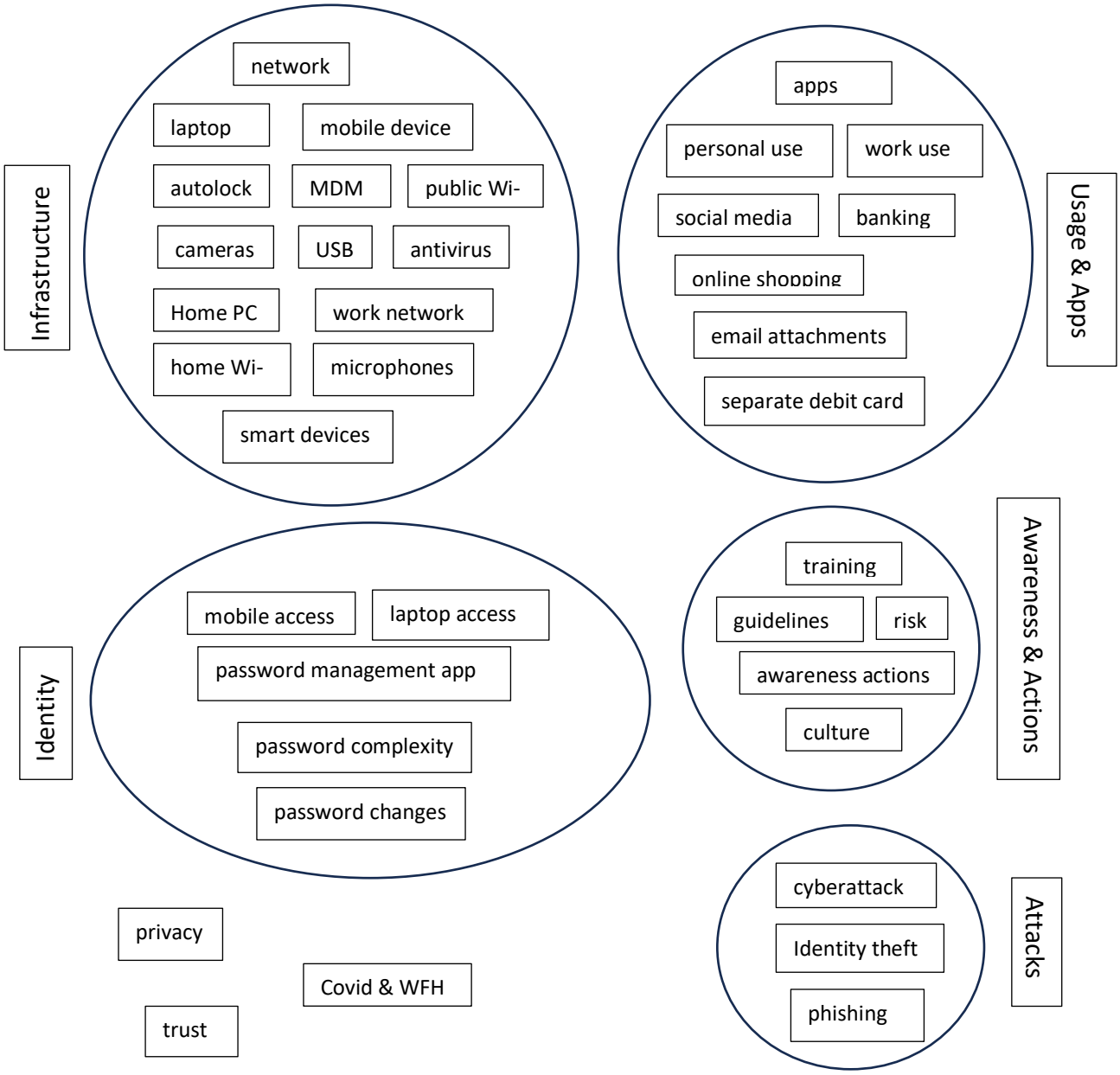

Figure 5. Codes and Categories

In Saldaña (2016, p. 198-199) theming the data is described as “labelling and thus analyzing portions of data with an extended thematic statement rather than a shorter code”. The themes that emerge from the categories are as follows:

1. Infrastructure – what infrastructure is used by the participants and is this personal or work devices and networks or a combination
2. Usage and Apps – what is the activity that is being carried out by the participants over the infrastructure
3. Identity – authentication of users for use of devices, networks and apps
4. Awareness & Actions – what has informed the participants knowledge and hence their intentions and actions
5. Attacks – have the participants been the target of cyberattacks and what behaviour has caused or impacted this
6. Trust – how does trust feature in the participants behaviour.

Covid and WFH (Working From Home) is identified separately as there were questions on this, however this is not really a separate theme.

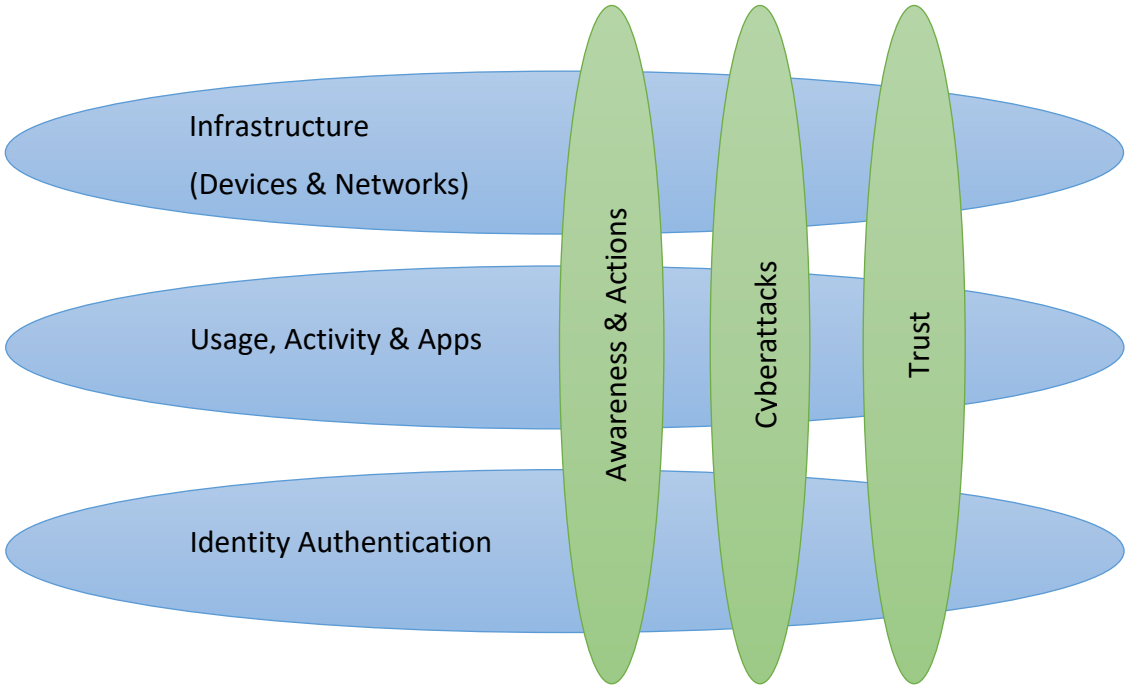

Figure 6. Cybersecurity Behaviour Model / Framework

The relationships between the identified themes were analysed and this resulted in the model shown in Figure 6 above, which summarises the key dimensions to consider regarding cybersecurity behaviour. Any online activity, be it a personal activity or a work activity requires three key components:

- The infrastructure, which include the devices and networks
- The actual usage or activity being carried out and the apps being used
- The identity authentication mechanisms used to control access to the devices, networks and applications

Cutting across these dimensions are the following aspects:

- The awareness and actions of the user when carrying out the activity – i.e., their behaviour
- Cyberattacks that may target any of these dimensions
- Trust that the user places in each of these dimensions

This Chapter has outlined the findings from the interviews carried out. The gathered data has been grouped into categories, from which themes have been developed for discussion and further analysis in the next Chapter.

5 Further Analysis and Discussion

In this section, the research findings are further analysed and discussed, with a focus on the over-arching research question and sub-questions.

Firstly, the impacts of the blurring of lines between personal and work contexts on cybersecurity human behaviour are discussed, to address the main research question. Included in this discussion the behavioural differences that depend on the type of application and data are also addressed, this being one of the sub-questions. To address the main question including this specific sub-question, the impacts are considered in the following four areas:

a) Infrastructure – the physical hardware, software and networks that personal and work activity is carried out over by the individual
b) Identity authentication – aspects relating to how a user's identity is validated, such as passwords and biometrics
c) Online activity and usage – some key types of applications and associated data that are used and associated considerations (i.e., the specific sub-question)
d) Awareness and actions – consideration of what has contributed to an individual's awareness relating to cybersecurity and the actions that this informs

Referring back to the identified themes and the cybersecurity behaviour model shown in Figure 6, it can be seen that three of these areas correlate with the horizontal dimensions of this model, with the fourth area being one of the aspects applying across these dimensions.
Following this, the three remaining sub-questions are addressed, these being:

1. What are the human behaviours that have contributed to successful cyberattacks against individuals and businesses and do this differ significantly? This is one of the vertical aspects shown in the cybersecurity behaviour model shown in Figure 6.
2. What barriers to improved cybersecurity do these identified behaviours generate?
3. What are the options to mitigate any barriers resulting from human behaviours and are there learnings that can be applied across both contexts?

5.1 Infrastructure Impacts

The infrastructure that personal or work data flows over includes both the device being used as well as the network that the device is connected to. The findings show that all participants use both a smartphone and a laptop/tablet device to carry out online activity over the internet, and this included own personal devices as well as company provided devices. Some participants use personal devices, primarily smartphones for work activity and correspondingly use work devices for personal activity demonstrating the blurring of the personal/work boundary from a technology perspective.

5.1.1 Smartphones

With all participants making use of only one smartphone and most of these being used for both personal and work use, there is a need to consider the cybersecurity implications of this behaviour. One of the participants who was using a company provided device confirmed that some sort of mobile device management was used by the organisation. Mobile device management enables the company to have some level of management and control over the smartphone. Whilst this is important for organisations to be able to enforce security and other policies for the device, it also means that that the organisation has some level of visibility of personal activity being carried out over those smartphone devices. The risk for the individual is that their personal information may be exposed to the organisations IT department and is therefore reliant on that information not being misused by those who have access to it. Similarly, when a work provided smartphone is used over a home network, the security of that home network and the behaviour of others using that home network also needs to be considered.

When smartphones aren't connected to a Wi-Fi network, the data transmitted and received by these devices makes use of the mobile network of the relevant service provider. As can be seen from the findings of this research, this could be a personal account or a work account. For scenarios where the mobile connection is provided by the employers, there is the possibility that that employer has mechanisms to allow them to monitor usage of that connection which from the findings could include both personal use as well as work use.

Whether organisations actively monitor an employee's mobile network usage was not part of this study, but examples do exist where employees have faced disciplinary proceedings for inappropriate use, so we know that this monitoring is carried out by some organisations to some extent. Individuals making use of their own smartphones for work purposes may be accessing documents of varying security classifications. This risk of this for the organisation is probably minimal from a network security perspective as those mobile connections are individual to that person and are unlikely to be monitored by anybody else. A possible exception to this is where that individual is a contractor or consultant who may be working for an organisation providing services to another organisation and the contractor or consultant has a smartphone provided by the services organisation that may have monitoring capabilities.

Work provided smartphones typically make use of the company's Wi-Fi network when an employee is at the organisation's premises. Organisations have the ability to monitor the usage of their Wi-Fi networks, including personal usage that an individual may be using their work provided device for. There are also the scenarios where a person's own device is used over the companies Wi-Fi network, i.e. Bring-Your-Own-Device or BYOD (Veljkovic & Budree, 2019), as well as the case that some organisations provide guest Wi-Fi access for visitors An additional consideration here is that once credentials are entered and the Wi-Fi function is on, a smartphone may switch seamlessly between Wi-Fi networks that it is able to connect to and the mobile service provider network that it is connected to. There is a risk here that smartphone users could be unaware of which network the data resulting from a personal or work activity is being sent or received over. For personal activity or communication being carried out over an organisations Wi-Fi network, there is a risk that an individual's personal information is visible to the organisation and the IT employees of that organisation. How much an employee trusts the organisation that they work for is a key factor here. But it is not only trust of the organisation that needs to be considered, but also the IT employees that work for that organisation.

Conversely, work provided smartphones may be used over the home network, in which case there may be work related data being transmitted over the home network. Home networks are discussed in more detail later in this report.

5.1.2 Laptops and Tablets

The situation with the other devices such as laptops and tablets is somewhat different in that most participants had separate personal and work devices. This however did not necessarily mean there was rigid separation of personal and work usage. Whilst personal devices were mostly restricted to personal usage, there was varying levels of personal usage on work devices, ranging from accessing personal emails to carrying out activities such as online banking and shopping. As for smartphones, carrying out personal activities over work devices potentially risks personal information being exposed to members of the companies IT department as well as cybercriminals hacking into an organisations network.

Company provided devices, by their nature will have work related documents on them, which traditionally in the days of fixed office-based computers would remain in a company location connected over a company network. Even before the Covid-19 pandemic, laptops and tablets have enabled employees to work from home and other remote locations. As a result of the pandemic this has expanded significantly, both in terms of number of individuals able and choosing to work from home as well as organisations enabling this. From a company perspective, this means there is potentially much more company information on devices outside of the office environment connected to home networks, with these home networks being used by other parties such as family members and friends.

Whilst most personal laptops and tablets were only used for personal use, one participant did suggest that they might make use of their personal laptop or tablet if there were issues with their work laptop/tablet.

Another consideration regarding company devices, which was not specifically explored with the participants, is that companies typically refresh an employee's device at regular intervals. With employees using work devices for personal use, there is a risk of personal information remaining on those devices after they have been replaced or upgraded. For example, one participant made use of their work tablet/laptop for signing personal related contracts as the work device had better functionality in having a touchscreen and stylus pen. These personal contract documents may remain on that device if not specifically removed.

Company provided laptops and tablets are typically set-up to operate over the office wired and/or wireless network. The Covid19 pandemic forced many more individuals to work from home and many businesses to set up the capability for them to work from home, typically using VPN or VDI capability. A natural consequence of this was that home Wi-Fi networks have become much more widely used for carrying out work tasks and activities. Whereas usage of the office Wi-Fi network is shared amongst the employees of the organisation, usage of the home Wi-Fi network is shared between, family members, friends and visitors. Unlike the work Wi-Fi network where access is controlled and managed by the IT department, home Wi-Fi networks tend to be set-up and then not touched again until the internet service provider is changed, or the network needs to be upgraded. The risk here then is that the boundary of the work network has expanded significantly with much less control over it. Home Wi-Fi passwords may be put on post-it notes on fridges, shared widely with children's friends who may not have the appropriate cybersecurity awareness. Additionally, the home Wi-Fi is now connected to many diverse and different devices such as smart TVs, personal digital assistants etc., all providing potential point to attack the home network which is now also being used extensively for work purposes.

5.1.3 Smart Devices on the Home Network

We live in a much more connect world today. Gone are the days of a single shared home family computer connected over a modem over a telephone line, with nothing else connected to it. Whilst one participant still had a family home computer, this is no longer the only device connected in the home. Today we have smart TVs, virtual digital assistants such as Alexa, multi-room wireless speaker systems such as Sonos, smart watches, fitness bands etc. The connected home is a reality with these devices connecting via Bluetooth or home Wi-Fi networks.
The cybersecurity risks associated with smart home products (also referred to as IoT products) are highlighted in (Chen & Urquhart, 2022). In that research, thirteen experts with significant experience in IoT security were interviewed about the barriers in making smart home products secure from a technical, legal and organisational perspective. The research highlighted not just the security and privacy risks for the individual, but also to what it terms "the operation of the infrastructural network". Aside from the Confidentiality and Integrity aspects of the 'CIA Triad', if smart home products with weak security become widely deployed and are subject to an attack, it could potentially impact a number of homes, from which many more people are carrying out work

activities, thereby also impacting the Availability aspect. From a confidentiality perspective, the article notes that if a compromised IoT product in the home is connected to a workplace network from that home, confidentiality breaches can become more significant issues.

In many cases, the awareness of the participants of the cybersecurity risks associated with these devices was limited, perhaps due to the lack of significant public information relating to this. A concern that devices like Alexa are always listening was raised, but only as a concern at a high level. As highlighted earlier the home network is now connecting multiple different devices, both within the home and from different people, both family members as well as friends and guests. Add to this, we are now doing a lot of our day-to-day work over this network using smartphones and laptops/tablets provided by the organisations that we work for.

A typical behaviour relating to these smart devices is that we buy them, we connect them to our home network and we use them. Whether this poses cybersecurity risks relating to work devices used at home over the same networks is an area for further research.

5.1.4 Public Wi-Fi

With organisations adding significant capability for their employees to be able to work from home, it also enables the capability to be able to work from any publicly available Wi-Fi spot, be that in a café, hotel or airport. How well these Wi-Fi spots are set up from a security perspective is unknown and likely varies significantly. The view from at least one participant was that hotel Wi-Fi is probably more secure than a café as there is an expectation that business people can work from a hotel when travelling for business. Similarly, airport lounges such as Air New Zealand's Koru Lounge were also seen by some as acceptable or lower risk to connect to their Wi-Fi network, as similar to hotels, they cater for people travelling on business. It should be noted that the Air New Zealand lounge in Auckland (and possibly other locations) no longer requires a password to use their Wi-Fi network. This perception influences behaviour regarding the types of activities that get carried out over these public Wi-Fi networks. Time spent at these establishments is also a factor as you may only spend a short amount of time in a café versus a day or two in a hotel. This influences whether you bother to log on to the café Wi-Fi network for the short amount of time you are there or are happy to use your own or works data allowance. The approach that the participants

took when it comes to public Wi-Fi spots varied significantly. Whilst many said they would avoid doing some activities on certain types of public Wi-Fi, this wasn't a rigid rule and a number of them said they would if they needed to. It should be noted that a public Wi-Fi spot is neither the work environment nor the home environment and therefore presents a risk to both work information and personal information. It is also likely that once you have connected to a device, it remains in those devices connection lists and will automatically switch to that Wi-Fi network unless it has been changed since the last visit. The use of a public Wi-Fi spot is much more widespread than your home Wi-Fi network in that anybody can be using that public Wi-Fi spot at any time, whereas your home Wi-Fi network is typically used by people that you know and trust, to some extent. In many places the public Wi-Fi network key is posted where all customers can see it, such as the menu board and therefore is available for all to see. Organisational policies may prohibit the use if certain public Wi-Fi spots for work purposes, however this was not explored in detail as part of this study.

5.1.5 Summary of Infrastructure Impacts

The infrastructure impacts can be summarised as increased risk to the security and privacy of personal data because it is now being stored and transmitted over company devices and networks as well as increased risk of company data as it now being transmitted over home networks as well as personal devices in some cases. Whilst this is not new, with smartphones appearing in 2006 as a suitable technology for corporate use (Veljkovic & Budree, 2019), and remote access for employees on business travel having been available for some time, the Covid19 pandemic has forced this to become the norm rather than the exception and the behaviour associated with using work devices and networks for personal use and personal devices and home networks for work use, increases the level of cybersecurity risk for both parties. The human behaviour relating to use of company provided infrastructure is typically influenced by the organisations guidelines and policies, which do not exist for personal devices and home networks.

An additional consideration relevant for all devices is that these are all portable devices that are transported in cars or on public transport and therefore have an increased risk of being physically stolen. If a device is stolen and it has been used for both personal and work use, the impact can be both for the individual and the organisation.

5.2 Identity Authentication

Identity authentication is an important consideration for devices, networks and applications as it controls who can access what, from where and when. Access to company provided devices and the corporate networks over which they operate is controlled by the organisation. Even with biometric options such as fingerprints and facial recognition becoming more widely available on devices, there is usually a password option in case there are issues with fingerprints or facial recognition working properly. Organisations also typically define the minimum requirements for passwords including how often they need to be changed. However, this is not the case for personal devices and the home networks that they operate over, which is under the control of the individual. The preferences expressed by participants for accessing their personal devices varied, with some preferring the traditional password approach and others preferring biometrics such as fingerprints and facial recognition. It should be noted that not all devices have biometric access capabilities, especially if they are older devices.

When it comes to setting up and managing passwords, this also varied across the participants. Some participants made use of password management tools such as Apple Keychain, whereas others resorted to writing them down in some coded fashion. What was consistent across the participants was that they hardly ever changed their passwords, except when they had forgotten a password and needed to change it to a new password to reset it. Passwords relating to personal devices and usage were not changed as a matter of course, which is a key difference to work devices and applications where the frequency of password changes is mandated by the organisation that is in control of access. The one password which invariably didn't get changed at all and was largely kept the same as what it was setup as is the home Wi-Fi password. There were a couple of exceptions to this where one participant was making use of a guest network for any friends or visitors, although it should be noted that that this wasn't set up with any more restrictions than the main network. The other exception was the participant who had set-up different networks with different restrictions, depending on who would be using the home network.

The impact of having less rigorous identity authentication disciplines when it comes to personal devices could be increase the risk of work data on those devices being compromised, in addition to the risk to the individual's personal data.

Despite the increased use of biometrics such as fingerprints and facial recognition, as well as password management tools such as Apple keychain, device, network and application identity authentication remains a key risk area, especially given the continuing increase in the volume of login credentials that are required.

5.3 Online Activity and Usage

A sub-question of this research was concerned with behavioural differences due to the type of application being used or data being communicated. The types of tasks and actions carried out over the used devices and networks is an important consideration when considering aspects such as financial risk. For online banking, some participants considered the risks minimal due to the two-factor authentication mechanisms used by banks. Regarding online shopping, some of the participants used different approaches to reduce the level of financial risk, as outlined in the previous chapter. This is interesting from a behavioural perspective as it demonstrates awareness of the risk, but not so much as to stop them carrying out online shopping activities.
The type of task or activity being carried out on a device or network is an important consideration when considering the risk associated with that particular action and the human behaviour that that drives. Whilst there are many different types of usage that are carried out online, the findings and impacts are discussed in relation to the following categories:

- Work tasks and communication
- Online banking
- Online shopping where payments are made online
- Social media
- Other personal activities not captured by the above categories

5.3.1 Work Tasks and Activities

Work tasks and activities are typically controlled by various policies established by the organisation. This typically includes security classifications of various documents/artefacts and guidelines on what types of activities that can be carried out on work devices and over work networks. An important aspect of this is not only the setting of the policies but also how these policies are managed and enforced, noting that existing research has been carried out on this from an assurance (Evans et al., 2016) and compliance perspective. The fact that more people spend more of their time working from home, or away from the office, means that there is much more company information flowing over networks that are not fully under the control of the organisation. If we consider the 'CIA triad' of Confidentiality, Integrity and Availability, carrying out work activities on personal devices and over home networks that are outside of the organisations corporate network increases the risk regarding confidentiality of the organisation's information. Communication is no longer limited to the corporate network, with information flowing over home networks that are typically shared with other family members as well as possibly friends and guests. Although organisations have become more proficient at setting up the networks and IT to support remote working securely by using technologies to establish Virtual Private Networks (VPNs), the number of points from which a cyberattack can be originated from has increased due to more employees carrying out work activities away from the office environment. We have seen several high-profile examples of government officials and politicians using personal emails for work purposes from their residences, and there are similar risks for organisations.

5.3.2 Online banking

Online banking is a usage type where the participants typically took more precautions. Banks have implemented increased security mechanisms such as two-factor authentication, as well as being proactive in terms of notifying customers about potential phishing attacks as well as other types of scams. Carrying out online banking tasks on devices and networks that are not your own, such as work devices, increases the risk that others may be able to obtain information enabling them to access a person's accounts. Carrying out online banking tasks over a work network may carry less risk than over a public Wi-Fi spot such as a café or a hotel. Trust is a factor here, with some participants indicating that they were not so concerned because they trusted the organisation that

they were working for. Interestingly, some participants also drew a distinction between hotel Wi-Fi networks and Wi-Fi networks in cafes, because there is an expectation that those travelling on business should be able to work securely from a hotel and this is therefore important for the hotel's reputation. Phishing continues to be a significant risk to individual's bank accounts and money. None of the participants reported any successful phishing attacks and appeared to be aware of the types of attempts that cybercriminals typically use. Of the non-work organisations that individuals deal with from a personal perspective, banks are to some extent trying to educate their customers regarding cybersecurity risks, although this is likely due to the nature of their business. There are still some aspects where improvements could be made, such as requiring passwords to be changed on a more frequent basis.

5.3.3 Online Shopping & Payments

Another area that presents financial risk for an individual is online shopping and the payments made for purchases online. The more devices and networks that you use a debit or credit card over, the higher the risk that someone else can obtain your details and make unauthorised purchases. The risk is somewhat dependant on the company that the individual is making the purchase from both in terms of their trustworthiness, as well as the security of the site that the purchase is being made through. Some of the participants interviewed used different approaches to mitigating or minimising the risk of using their credit and debit card details online. These approaches included:

- Limiting the devices on which they used the debit or credit card details
- Limiting where and the networks over which they carried out online purchases
- Only using credit cards and not debit cards, as credit cards come with some insurance from the bank or financial provider
- Using a separate low limit card for their online purchases
- Only making online purchases from sites or companies that they deemed trustworthy

Regarding the last point, trustworthiness can be somewhat subjective. What one individual regards as a trustworthy site may not be the same as another individual. There is also the dichotomy of organisation or application size. Does a large organisation or popular/widely used app make it a more attractive target for cybercriminals because the potential volume of users and

hence possible increased returns, or does this mean it will have more comprehensive security mechanisms making it more difficult to attack? Likewise, do smaller and less well-known organisations or apps make them less of a target for cybercriminals. Although this aspect was raised during the pilot interview, it did not appear to be a significant consideration for the interviewed participants.

Although some of the participants confirmed that their credit card/account had been compromised, it was not possible to determine how this occurred, except in one case where it was traced back to a taxi ride. Human behaviour can impact the possibility of credit card information being exposed to cybercriminals and with the expansion of online shopping, the risks of this are increased. The lockdowns resulting from Covid-19 have increased the use of online shopping both because individuals have been unable to leave their homes to physically visit a retail store, as well as stores and businesses being forced to transact online when they perhaps previously did not, to be able to continue to trade and remain in business. It is also possible that the unexpected nature of the Covid-19 pandemic forced businesses online without the needed time to implement the necessary cybersecurity capability and infrastructure. Likewise, those who may not have traditionally shopped online have found it necessary to do this, possibly without the knowledge and awareness needed to keep them safe from cybercriminals. We should also not discount the possibility of the physical card being cloned or copied.

5.3.4 Social Media, Identity Theft and Privacy

The use of social media on different devices and over different networks is an important usage type to consider as it is where information about an individual is exposed and could be used for identity theft. Whilst those interviewed as part of this study were aware of the risk of identity theft, it is interesting to note that it appeared to be less of a concern than the financial aspects such as online banking and purchases. Some of the reasons for this were that some felt they did not have a significant digital footprint or were not “that interesting” to be of interest to potential cybercriminals. When we think of social media, we tend to consider the typical applications of Facebook, Instagram, WhatsApp, as well as LinkedIn in the business world. However, if we look at the actual definition of social media, it encompasses any “websites and applications that enable users to create and share content or to participate in social networking”. This can therefore

include applications used for specific interests, such as apps like Strava where you connect with other athletes, or language learning apps such as Duolingo, where you may have a public profile and participate in leagues against other learners. Whilst the level of information shared on these sites may be limited, multiple items of small information may be used to build a more comprehensive picture of an individual's identity.

The increase in both the number of social media applications as well as interest specific applications such as a running app that creates a network of contacts/friends means that there is much more information about individuals available online to be discovered by cybercriminals. Just by making use of an app risks making information available, that on its own may seem insignificant, but when combined with other information could contribute to the theft of an individual's identity. Whilst most participants were aware of the risk of identity theft to some degree, this did not appear to be a significant concern. In some cases, this lack of concern was due to them not making much use of social media and hence not much information being available to contribute to identity theft. However social media is not the only area that cybercriminals can target to build information about an identity. With this blurring of work and personal/home life, are cybercriminals building their information from both contexts? Data about where you work or have worked is a part of a person's identity and can be combined with other information to potentially enable identity theft.

5.3.5 Other Usage/Applications

There are many websites and applications that we use that require us to create usernames (typically an email address, so that it can be verified) and passwords. Some of these enable you to link your login to other applications such as Facebook or Google, although this wasn't specifically looked at in the interviews. Some of those interviewed indicated that they took less care with these login credentials than they did with say online banking, highlighting that if they were hacked on these sites or applications, there was little of interest to steal. Some participants made use of password management apps to manage this aspect, which somewhat removed the need for them to think about this area much. Identity authentication was discussed earlier in this chapter. Whether as user accessed other websites or applications over a work device or network was not covered in detail in this study other than at a general level.

5.4 Awareness, Intentions and Actions

5.4.1 Training & Guidelines

We can see from the research findings that the level of training provide by organisations varies significantly. In a number of cases, this training is a one off and not an ongoing process, with the consequential risks of it becoming either forgotten or at least not top of mind. Without training being refreshed and provided on an ongoing regular basis, it risks becoming out of date and not addressing the latest risks and tactics being adopted by cybercriminals in an area that is fast evolving. Training provided by organisations typically focuses on addressing the risks to the organisation and not the risks to the individual regarding their personal use.

Cybersecurity awareness from organisations other than the companies that we work for is scarce. Banks and other financial bodies are perhaps the most proactive in this respect, regularly informing customers about risks such as phishing. This is perhaps partially because it is in the banks own interest and to minimise the risk to their own financial position, rather than a concern for customers. Few participants indicated obtaining cybersecurity awareness and/or knowledge from other organisations that they deal with or applications that they make use of. When you join the latest new app, there are terms and conditions that you agree to that may include aspects of cybersecurity, but how many people really read and understand these when they are wanting to make use of the latest new application or keep updated regarding those related to the apps and websites that they are already signed up to. With cybersecurity awareness being mainly informed by training focused on protecting the organisations that individuals work for, specific aspects that may be relevant in a personal context may be missed.

There is clearly a gap regarding knowledge and awareness of cybersecurity and its impact on individual's personal life. This perhaps is an opportunity for device providers, mobile networks, internet service providers (ISPs), retailers and other independent organisations. It could even be positioned as a differentiator if these organisations were to become more proactive in this space.

5.4.2 Awareness, Intentions and Actions

Knowledge and awareness of cybersecurity and the risks posed to individuals in their personal lives is only one part of the picture. This not only needs to translate into intentions but, also to actions. Even those participants that had spent some time working in roles that involved an aspect of cybersecurity admitted that their actions relating to what they should do didn't always translate into action. Perhaps it takes an actual incident or impact/loss to raise the priority of this from the perspective of taking the required actions needed to mitigate the risks to individuals. Recently there has been more media attention on examples of individual losses due to cyberattacks, however these reports tend to focus on just one aspect of what is a much bigger picture.

5.5 Human Behaviours and Cyberattacks

The cyberattacks or account compromises identified by the interviewed participants can be categorised as follows:

- Cloned or compromised credit cards
- Bank account compromised – believed to be due to a computer being hacked and password not being changed regularly
- Hacked email account
- Purchase through a well-known social media site from a third-party advert that was fake

There are two aspects of human behaviour to consider from these examples. The first being that the fact that a password wasn't being changed regularly was believed to have been the cause of or had contributed to the bank account being compromised. It should be noted that this participant now regularly changes passwords to do with anything financial every three months, which is triggered by an alarm reminder. Hence a change of behaviour has happened as a result of this attack.

The second aspect concerns the purchase by clicking an advert on the well-known social media site. The human behaviour that contributed to this successful attack was trust in a large well-known social media platform and the third parties that trade over it. Trust is one of the vertical aspects of the cybersecurity behaviour model shown in Figure 6. The impact of this cyberattack

had been somewhat mitigated as the participant noticed it relatively quickly. Even though the affected participant had a good level of cybersecurity awareness, the assumption that a large well-known application/platform would have some controls over third parties that use their platform proved to be incorrect. Essentially, the participant had trusted the social media application and this trust has led to another party compromising their account.

Only one of the participants that had had their debit or credit cards compromised had the likely source of this identified – the use of the card in a taxi. This is a good reminder that the source of financial attacks on individuals can still be the use of the physical card to purchase something. The cyberattacks against individuals in this study were primarily targeted at financial gain for the cybercriminal. This can also be the case for cyberattacks targeted as businesses, although there can also be other reasons such as reputational damage, competitive information as well as trying to take a specific business offline, i.e., the Availability component of the 'CIA Triad'.

5.6 Barriers and Mitigation to Improved Cybersecurity

5.6.1 Barriers

The impacts identified above have highlighted a number of barriers to improved cybersecurity when it comes to human behaviour.

The inconsistent level of awareness regarding cybersecurity risks, especially in a personal context indicates that lack of cybersecurity knowledge and awareness is a key barrier to improved cybersecurity. Whilst all participants had some level of knowledge and awareness regarding cybersecurity, this varied on different aspects and was inconsistent. For example, one participant who regularly changes their online banking password every three months was unaware of the risks associated with making use of public Wi-Fi hotspots. Participants knowledge of cybersecurity was largely informed by either training provided by the organisations that they work for, communication of information from banks, especially relating to phishing and the occasional report in the media, for example of a recent scam that has resulted in significant financial loss for an individual. There is an opportunity for individuals to become better informed about the cybersecurity risks in their personal lives and good practice behaviour that may help mitigate

these risks, at least partially if not fully. Regarding training provided by the organisations that the participants work for, this also varied in terms of whether they provided any training at all and how often that training was updated and refreshed. Not all organisations provide cybersecurity training to their employees, and whilst for some this training is occasionally updated, this was not the case for all. Cybersecurity training provided by organisations typically focuses on protecting that organisation and whilst some of the principles can apply across both personal and work contexts, this isn't the main focus. An organisation that one of the participants works for has deliberately decided to focus the cybersecurity training that they provide on protecting the individual in a personal context, believing that this makes the subject more real for their employees and will therefore have improved benefits for the organisation. The lack of any widely available training and guidelines focused on protecting the individual from cybersecurity threats is a key gap and should be considered a barrier.

Another key barrier is the lack of consistent application of actions regarding cybersecurity, so that it becomes as second nature as locking the door when you leave the house. Even some of those that worked or had worked in the cybersecurity industry admitted that they didn't always apply best practice. In fact, it wasn't always the participants who worked or had previously worked in industries where cybersecurity should have a higher priority and profile, such as banking and telecommunications, that carried out best practice when it came to their individual protection from cybersecurity threats.

A third key barrier is that whilst organisations and businesses have had to adapt because of Covid-19, to enable their employees to work effectively from home, with the exception of insights from one participant, organisation have not set any requirements regarding security of the home networking environment. Networks have been typically secured by technologies such as Virtual Private Networks (VPNs), but at the end points the laptop or smartphone is connected to a home router whose password is typically shared between family, friends and visitors and is rarely changed from when the router was installed. In most cases, there appears to be a lack of requirements or guidelines regarding the home networking environment, which these days may also have many other IoT devices such as smart TVs connected to it.

The culture that organisations adopt and promote regarding cybersecurity can also create barriers to improved cybersecurity. Some organisations cybersecurity focus is on policy and compliance, and whilst these are important there also needs to be a culture of employees adopting good practice because they understand why and not to just tick a box from a compliance perspective. Regardless of intentions and the adoption of good behaviours relating to cybersecurity, humans make mistakes and when it comes to cybersecurity, knowing that a mistake has been made as early as possible is critical to minimising the possible implications of that mistake. A culture that seeks to punish individuals for making mistakes, will likely not lead to early reporting of those mistakes. Blame culture will most likely have a detrimental effect on minimising impact of mistakes.

5.6.2 Mitigations

Availability of training and/or guidelines focused on best practice behaviours to protect an individual from cyberattack is one possible mitigation option. There is an opportunity for organisations other than the company that someone is employed by to be more proactive in providing the cybersecurity knowledge and awareness that is needed by individuals. Banks have been somewhat proactive regarding highlighting to their customers the types of phishing attempt used by cybercriminals, but none of the participants could identify other organisations or types of organisations that were proactive in raising cybersecurity knowledge and awareness for individuals. The is an opportunity for one or more organisations to provide guidelines for best practice cybersecurity human behaviour for individuals. These guidelines need to be both easy to understand as well as widely available to ensure that they get the needed uptake.
A related mitigation is for employers to shift the emphasis of the cybersecurity training that they provide to focus not just on protecting the organisation, but also on the protecting the individual. Making it real for the individual will have a knock-on effect in terms of protection of the company's own data and systems.

Regarding mitigations to their own financial risk, some participants have already taken some measures such having a lower limit debit/credit card that is only used for online shopping, to only using credit cards as they come with some insurance protection. This is something that banks and other financial services organisations could be more proactive in promoting.

Organisations and businesses need to consider more the home office environment of their employees and providing either requirements or guidelines on how these should be set-up and managed ongoing. Whilst this would result in additional time requirements of an organisations IT department, this should be weighed against the resulting reduction in the risk of cybersecurity attacks and breaches.

5.7 Comparison with Other Research

Considering the findings from this research, some are the same as other research, thereby confirming that prior research, some are new, and some are different.
Use of work devices and networks for personal use is not new. Responses from those interviewed in (Borkovich & Skovira, 2020) included “Yes, I send personal emails from my work account and vice versa”. And in the same report it was confirmed that one of those interviewed “used to use the Wi-Fi in Starbucks and at the airport and other places”. Combining personal and work use on a single device has been carried out as long as BYOD concepts have been implemented by organisations (Borkovich & Skovira, 2020). However, both of these articles primarily focus on the risks for the organisations and not the individual. A new finding from this research is that individuals carry out sensitive personal activities over work devices and networks, thereby introducing risks for themselves.

Whilst business have for a long-time enabled employees to work remotely, this is now enabled for many more people from many more home locations. A new finding from this research is that this has mainly been done without any guidance on home network set-up or behaviour, with businesses predominantly relying on VPN technologies for their cybersecurity protection. The home has evolved to a smart home environment, with many IoT products now connected to the home network. The finding that this increases the cybersecurity risk level of the home, reinforces a similar finding from a report into the cybersecurity implications of these new smart home products (Chen & Urquhart, 2022). However, the finding that there are potentially increased risks from the behaviour of multiple people making use of these home networks, which typically have poor security, is new.

The need for ongoing cybersecurity training and guidelines is also not new. A key conclusion from a survey on cybersecurity culture when working from home during the Covid-19 crisis (Georgiadou

et al., 2022) concluded that “employees awareness, familiarity and expertise on security issues needs to be encouraged and cultivated via continuous training programs.” However, what is new is the finding that there is a significant gap in the availability of guidelines and training focused on personal cybersecurity best practice.

This Chapter has discussed the findings from the research carried out, relating this to the overarching research question and sub-questions. Conclusions are presented in the following Chapter, along with limitations of the research and future research opportunities.

6 Conclusion, Limitations and Future Work

The research presented here was driven by two evolving aspects. Firstly, both personal and work online activity has become more mobile, driven by both the availability and use of smartphones, tablets and laptops, as well as the increased availability of higher bandwidth networks. Secondly, the Covid-19 pandemic has forced organisations to enable working remotely for their employees and forced employees to carry out the work from home that they previously would have done from the office. Driven by these two key factors, the research aim was to understand the impact of this blurring of lines between personal and work contexts on human behaviour with respect to cybersecurity. This final thesis chapter presents a summary of the approach adopted for the research, the insights and contributions that have resulted from the research and the implications and opportunities that these present. Limitations of the research are identified, along with potential future research opportunities in this field.

6.1 Summary of Research Approach

The approach adopted for this research was to firstly carry out a literature review to identify research that had been carried out in the field of human behaviour and cybersecurity relating to the proposed research question. Having validated that the research question was a suitable topic to research, data gathering was carried out by interviewing several participants who would provide suitable insights. The data from these interviews was coded against a number of identified codes, which were then grouped into categories from which themes were derived. The main outcomes of this research resulted from the further analysis and discussion of these themes to identify the key contributions regarding insights, barriers to improved cybersecurity and possible mitigations.

6.2 Insights, Barriers and Mitigations

6.2.1 Insights

The key insights identified from the research can be summarised as follows:

- Whilst some of those interviewed carried out some level of separation of personal and work activities on the devices and networks used, this was not a clear demarcation for most of the participants.
- The knowledge of the participants relating to cybersecurity risks and what might be deemed good behavioural practice was variable. Some of those interviewed had received cybersecurity training at work, but only one case was identified where this training was focused on the personal context rather than the work context.
- Even where knowledge was clearly present, actions relating to cybersecurity behaviour did not always match intentions based on knowledge of what should be done.
- Whilst participants appeared aware of the risk of identity theft, it did not appear to be a significant concern.
- The home network has typically not been changed to accommodate the increased level of work being carried out from home, despite this network being shared between family and friends and in some cases being connected to a number of smart devices.
- Trust plays a role in influencing behaviour and misplaced trust can result in cybersecurity breaches.
- Use of work devices and work networks is typically controlled by organisational policies and/or guidelines. There are no such policies that exist for personal devices or home networks.

6.2.2 Barriers to Improved Cybersecurity

From the insights obtained from the research, the following barriers were identified:

- There is a lack of consistent knowledge regarding cybersecurity behaviour in a personal context. This may be partially resulting from the lack of available training and guidelines that have a personal focus.

- Other than the use of VPN technology, there doesn't appear to have been much consideration of risks of the home network environment due to it being shared by multiple parties and it also being connected to various smart devices.
- Good cybersecurity behaviour is a long way from becoming second-nature in a way that you always lock the doors when you leave the house.

6.2.3 Mitigations

Potential mitigations to the barriers identified above are:

- Employers could make their cybersecurity training more focused on the personal context which may make it more 'real' for the individual
- Other organisations could make training or guidelines available for best practice cybersecurity behaviour in a personal context, other than banks that predominantly focus on the phishing risk.

6.3 Research Contributions

There are two main contributions to research from this study.

Firstly, there is a lack of comprehensive guidelines that individuals can follow to protect themselves from cybersecurity risks in their personal lives. Cybersecurity knowledge and awareness has typically been obtained from either training from employers or warnings from banks regarding phishing attacks. In many cases, training from employers has its main focus on protecting the organisation from cybersecurity risks and not the individual. Not all employers provide cybersecurity training and update this training on a regular basis.

Secondly, the home has now become a work location for many, but there has typically been no cybersecurity risk assessment of and/or changes to the home network, which is a network used by multiple people such as family, friends and visitors, and is also now connected to various smart devices with associated security risks. Businesses mostly rely on VPN technology and policies to protect their information, but this does not necessarily address all of the security risks of the evolving home environment.

6.4 Implications and Opportunities

The implication for businesses is the increased risk profile of the home environment which are typically not very well secured. This is also an opportunity to set guidelines and expectations for employees when working from home.

The implication for individuals is the lack of guidelines regarding good practice cybersecurity behaviours and home environment set-up means they may face increased risks of cyberattacks and associated financial and other losses.

There is an opportunity for employers to enhance their cybersecurity training to also address cybersecurity in a personal context. There is an opportunity for other parties, be these service providers, retailers or other independent organisations to establish cybersecurity guidelines to protect individuals in their personal lives.

6.5 Limitations

Whilst the research carried out has provided a number of insights into the impact of the blurring of lines between personal and work contexts on human behaviour with respect to cybersecurity, it has the limitations outlined below.

a) The research method chosen to use semi-structured interviews places practical limitations on the number of participants that can be included in the research. Whilst the approach of interviewing a small number of participants enables more in-depth insights to be obtained, the small sample size may mean insights that might have been obtained from a wider and more diverse sample are missed.

b) The geographies from which the participants were sourced are New Zealand and Australia. Whilst the Covid-19 pandemic was a global event, with lockdowns being implemented in many countries, the research may have missed geographical differences in behaviour that may have resulted.

c) Whilst the interviewing approach adopted was useful in expanding the questions as further interviews took place, it meant that a fully complete set of data on all aspects was not obtained.

6.6 Future Research Opportunities

There are numerous opportunities for expanding on the research carried out by this study. To address the small sample size necessitated by the use of in-depth interviews, the insights obtained from these interviews could be taken and made into a questionnaire that could then be used with a wider population without the need for interviews. This would produce a much larger sample and add the possibility of applying a quantitative lens to the qualitative data already obtained. The questionnaire could also be used in multiple geographies to also address this limitation identified above.

The research carried out by this study focussed on interviewing individuals as this is where both the work context and personal context come together. It would be useful to expand the study to gather insights from other parties, such as the employers, for example, to also get their perspective.

Whilst cyberattacks against larger businesses are typically widely broadcast, individual cyberattacks have typically not been widely reported until more recently. It would be useful to put in a process for capturing and logging individual cyberattacks over time to provide a suitable dataset for further analysis.

7 References

Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity [Article]. *User Modeling & User-Adapted Interaction, 29*(3), 701-750. https://doi.org/10.1007/s11257-019-09236-5

Anwar, M., Yuan, X., He, W., Ash, I., Li, L., & Xu, L. (2017, 04 / 01 /). Gender difference and employees' cybersecurity behaviors [Article]. *Computers in Human Behavior, 69*, 437-443. https://doi.org/10.1016/j.chb.2016.12.040

Azungah, T. (2018, 11/15/). Qualitative research: deductive and inductive approaches to data analysis [JOURNAL]. *Qualitative Research Journal, 18*(4), 383-400. https://doi.org/10.1108/QRJ-D-18-00035

Bhaharin, S. H., Mokhtar, U. A., Sulaiman, R., & Yusof, M. M. (2019). Issues and Trends in Information Security Policy Compliance [Conference]. 1-6. https://doi.org/10.1109/ICRIIS48246.2019.9073645

Borkovich, D. J., & Skovira, R. J. (2020, 10//). WORKING FROM HOME: CYBERSECURITY IN THE AGE OF COVID-19. *Issues in Information Systems, 21*(4), 234-246. https://ezproxy.aut.ac.nz/login?url=https://search.ebscohost.com/login.aspx?direct=true&site=eds-live&db=edo&AN=145743861

Chen, J., & Urquhart, L. (2022). 'They're all about pushing the products and shiny things rather than fundamental security':Mapping socio-technical challenges in securing the smart home [Article]. *Information & Communications Technology Law, 31*(1), 99-122. https://doi.org/10.1080/13600834.2021.1957193

Crabtree, B. F. (2022). *Doing Qualitative Research* (W. L. Miller, Ed. 3rd ed. ed.). SAGE Publications, Incorporated. https://ebookcentral.proquest.com/lib/AUT/detail.action?docID=7107063

Durdella, N. (2019). *Qualitative Dissertation Methodology: A Guide for Research Design and Methods* https://doi.org/10.4135/9781506345147

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics, 5*(1), 2. https://doi.org/10.11648/j.ajtas.20160501.11

Evans, M., Maglaras, L., He, Y., & Janicke, H. (2016, 07/29). Human Behaviour as an aspect of Cyber Security Assurance. *Security and Communication Networks, 9*. https://doi.org/10.1002/sec.1657

Flick, U. (2022). *The SAGE Handbook of Qualitative Research Design*. SAGE Publications. https://ebookcentral.proquest.com/lib/AUT/detail.action?docID=6926217

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022, 06/01/). Working from home during COVID-19 crisis: a cyber security culture assessment survey [Article]. *Security Journal, 35*(2), 486-505-505. https://doi.org/10.1057/s41284-021-00286-2

Hadlington, L. (2018, 01/01). Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology, 12*, 269-281. https://doi.org/10.5281/zenodo.1467909

Maria, B., & Jason, R. C. N. (2019, 07/08/). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs) [JOURNAL]. *Information & Computer Security, 27*(3), 393-410. https://doi.org/10.1108/ICS-07-2018-0080

Mashiane, T., & Kritzinger, E. (2019). *Cybersecurity behaviour: A conceptual taxonomy* (Vol. 11469 LNCS) [Conference Paper]. Springer Verlag. https://doi.org/10.1007/978-3-030-20074-9_11

Oxford University Press. (n.d.). Behaviour. In *Oxford Languages Dictionary*. Retrieved November 22, 2023, from https://www.google.com/search?q=Behaviour+definition&sca_esv=584400697&ei=tSxdZbm_BrXgseMPwY-m0AE&ved=0ahUKEwj57bnbj9aCAxU1cGwGHcGHCRoQ4dUDCBA&uact=5&oq=Behaviour+definition&gs_lp=Egxnd3Mtd2l6LXNlcnAiFEJlaGF2aW91ciBkZWZpbml0aW9uMgoQABiABBiKBRhDMgoQABiABBiKBRhDMgUQABiABDIFEAAYgAQyBRAAGIAEMgUQABiABDIFEAAYgAQyBRAAGIAEMgUQABiABDIFEAAYgARI_ChQtQ1YgxRwAXgAkAEAmAGuAaABpAWqAQMwLjS4AQPIAQD4AQHCAgoQABhHGNYEGLADwgINEAAYgAQYigUYsAMYQ8ICBxAAGIAEGA3CAgsQABiABBiKBRiRAuIDBBgAIEGIBgGQBgo&sclient=gws-wiz-serp

Saldaña, J. (2016). *The coding manual for qualitative researchers* (3E [Third edition]. ed.). SAGE.

Sebescen, N., & Vitak, J. (2017). Securing the Human: Employee Security Vulnerability Risk in Organizational Settings [Article]. *Journal of the Association for Information Science & Technology, 68*(9), 2237-2247. https://doi.org/10.1002/asi.23851

Veljkovic, I., & Budree, A. (2019). Development of Bring-Your-Own-Device Risk Management Model: A Case Study From a South African Organisation [Article]. *Electronic Journal of Information Systems Evaluation, 22*(1), 1-14. https://ezproxy.aut.ac.nz/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=139130818&site=eds-live

Verizon. (2023). *2023 Data Breach Investigations Report (DBIR)*. https://www.verizon.com/business/resources/reports/dbir/

APPENDIX A. ETHICAL APPROVAL

29 June 2021

Krassie Petrova
Faculty of Design and Creative Technologies

Dear Krassie

Re Ethics Application: **21/145 Similarities, differences and implications of human behaviour relating to cybersecurity in a personal and work life context**

Thank you for providing evidence as requested, which satisfies the points raised by the Auckland University of Technology Ethics Committee (AUTEC).

Your ethics application has been approved for three years until 29 June 2024.

Standard Conditions of Approval

1. The research is to be undertaken in accordance with the Auckland University of Technology Code of Conduct for Research and as approved by AUTEC in this application.
2. A progress report is due annually on the anniversary of the approval date, using the EA2 form.
3. A final report is due at the expiration of the approval period, or, upon completion of project, using the EA3 form.
4. Any amendments to the project must be approved by AUTEC prior to being implemented. Amendments can be requested using the EA2 form.
5. Any serious or unexpected adverse events must be reported to AUTEC Secretariat as a matter of priority.
6. Any unforeseen events that might affect continued ethical acceptability of the project should also be reported to the AUTEC Secretariat as a matter of priority.
7. It is your responsibility to ensure that the spelling and grammar of documents being provided to participants or external organisations is of a high standard and that all the dates on the documents are updated.

AUTEC grants ethical approval only. You are responsible for obtaining management approval for access for your research from any institution or organisation at which your research is being conducted and you need to meet all ethical, legal, public health, and locality obligations or requirements for the jurisdictions in which the research is being undertaken.

Please quote the application number and title on all future correspondence related to this project.

For any enquiries please contact ethics@aut.ac.nz. The forms mentioned above are available online through http://www.aut.ac.nz/research/researchethics

(This is a computer-generated letter for which no signature is required)

The AUTEC Secretariat
Auckland University of Technology Ethics Committee

Cc: hayespaul28@gmail.com

APPENDIX B. PARTICIPANT INFORMATION SHEET AND CONSENT FORM

Participant Information Sheet

Date Information Sheet Produced:

22 June 2021

Project Title

Similarities, Differences and Implications of Human Behaviour relating to Cybersecurity in a Personal and Work Life Context

My name is Paul Hayes and I am currently studying for a Master of Information Security and Digital Forensics at AUT. To complete this qualification, I am carrying out research for a thesis on the above project title and as part of this research I intend to interview a number of participants to gain insights into their human behaviour in relation to cybersecurity in both a personal and work life context.

Your input and insights can be really useful in understanding more about this important research topic, as well as assisting me in successfully completing both my thesis and my Masters qualification and I would welcome your participation.

What is the purpose of this research?

This research aims to answer the following over-arching research question:

"Are there similarities and differences in the human behaviours concerning security and cybersecurity that individuals exhibit relating to their personal life and their work life and can insights from these be leveraged to provide improvements in either context".

With the increased blurring of lines between the use of technology for both personal and business use, driven by the increased use of BYOD in the workplace, as well as the increase in employees working from home as a result of the coronavirus pandemic, this research aims to evaluate the similarities and differences in an individual's behaviour relating to cybersecurity between their personal/home life and their work life. The research will assess the implications of human behaviours relating to cybersecurity and whether there are learnings that can be implied to improve behaviours in the other context.

The findings of this research may be used for academic publications and presentations.

How was I identified and why am I being invited to participate in this research?

You are part of my professional network and believe that you may provide good input and insights relating to the research topic.

How do I agree to participate in this research?

Your participation in this research is voluntary (it is your choice) and whether or not you choose to participate will neither advantage nor disadvantage you. You are able to withdraw from the study at any time. If you choose to withdraw from the study, then you will be offered the choice between having any data that is identifiable as belonging to you removed or allowing it to continue to be used. However, once the findings have been produced, removal of your data may not be possible.

If you agree to participate, I will send you a consent form to complete and return via email.

What will happen in this research?

I will contact you and arrange a time to carry out an interview using online conferencing (e.g. Zoom) where I will ask questions regarding your behaviours in relation to cybersecurity in both a personal and work life context. I anticipate the interview will last 30-45 minutes, but it may go for longer in some situations, if that is acceptable to you, and of course you have the right to cease at any time. The audio from the interview will be recorded and transcribed. The transcript from the interview can be provided to you if desired.

If necessary (and you agree), I may contact you following the interview via email should I have any clarifications regarding the information gathered.

What are the discomforts and risks?

There are likely to be minimal discomforts and risks encountered as part of this research.

There may be some discomfort in sharing information about any cyberattacks you may have encountered. There may also be an element of risk if you choose to share information regarding cybersecurity behaviour that is not in line with rules and/or recommended policies relating to specific activities.

How will these discomforts and risks be alleviated?

You will only be encouraged to share information that you are comfortable sharing during the interview and all data gathered will be treated as confidential. You and the organisations that you work for (or have worked for) will not be identified in the research outputs.

What are the benefits?

The potential benefits of this research are to provide a better understanding of and insights into human behaviour relating to cybersecurity, which may lead to improvements in how to combat cybersecurity threats in the future.

The benefit for me is that it will enable me to complete my Master of Information Security & Digital Forensics qualification.

How will my privacy be protected?

Information obtained from you during the interview will be treated as confidential and your details will not be included in any outputs resulting from the research. Your contact details will be stored separately from the data/information gathered.

What are the costs of participating in this research?

This research will require approximately one hour of your time.

An additional time allowance of approximately 30 minutes may be needed if you would like to receive and review the transcript from the interview.

What opportunity do I have to consider this invitation?

Please respond as to whether you are willing to participate in this research within three weeks of the date of this invitation.

Will I receive feedback on the results of this research?

Once the research has been completed, I will provide you with a one or two page summary of the research findings.

What do I do if I have concerns about this research?

Any concerns regarding the nature of this project should be notified in the first instance to the Project Supervisor, Dr Krassie Petrova, krassie.petrova@aut.ac.nz, 021 906 794.

Concerns regarding the conduct of the research should be notified to the Executive Secretary of AUTEC, *ethics@aut.ac.nz* , (+649) 921 9999 ext 6038.

Whom do I contact for further information about this research?

Please keep this Information Sheet and a copy of the Consent Form for your future reference. You are also able to contact the research team as follows:

Researcher Contact Details:

Paul Hayes, hayespaul28@gmail.com, 027 612 7496

Project Supervisor Contact Details:

Dr Krassie Petrova, krassie.petrova@aut.ac.nz, 021 906 794

Consent Form

Project title: ***Similarities, differences and implications of human behaviour relating to cybersecurity in a personal and work life context***

Project Supervisor: ***Dr Krassie Petrova***

Researcher: ***Paul Hayes***

- ○ I have read and understood the information provided about this research project in the Information Sheet dated 22 June 2021.
- ○ I have had an opportunity to ask questions and to have them answered.
- ○ I understand that notes will be taken during the interviews and that they will also be audio taped and transcribed.
- ○ I understand that taking part in this study is voluntary (my choice) and that I may withdraw from the study at any time without being disadvantaged in any way.
- ○ I understand that if I withdraw from the study then I will be offered the choice between having any data that is identifiable as belonging to me removed or allowing it to continue to be used. However, once the findings have been produced, removal of my data may not be possible.
- ○ I agree to take part in this research.
- ○ I wish to receive a summary of the research findings (please tick one): Yes○ No○

Participant's signature: .....

Participant's name: .....

Participant's Contact Details (if appropriate):

.....

.....

.....

.....

Date:

Approved by the Auckland University of Technology Ethics Committee on 29 June 2021 AUTEC Reference number 21/145.

Note: The Participant should retain a copy of this form.

Participant A

SPEAKERS
Researcher, Participant A

Researcher 00:03
Okay so that's my recording. Yep, good. All right, so I'm gonna go and run through some questions. So first thing is really just to understand in terms of your devices or IP equipment do you have. Do you have separate mobile phones for personal use and work use. And do you have separate laptops or computers for personal use or work yeah okay.

Participant A 00:29
So, our mobile phone we only have, we only have one so I have my work email loaded on my mobile phone. It's. I personally bought it but I had a contribution to the cost from my workplace so I don't know if you call them work device or a home device I think it was, it's considered a weak device but you can make your own phone calls on it, you know, right, from personal use. Yeah. But of course, I mean I never use it for phone calls because I'm usually using apps anyway. But, yeah, and Wi Fi. So yeah that's that's the phone.

Researcher 01:13
So the devices that the device, the phone is, is you bought the phone had a contribution to it but it's connected to the network provided by the company they work for. Yeah,

Participant A 01:24
yeah company pays for my monthly right subscription or whatever you want to call it. And I do have my work emails, available on that phone, right. I can read them,

Researcher 01:39
but there's a county paid directly or your subscription or not part of that is that is that something you can I don't, I don't anything

Participant A 01:46
to do with it. Yeah, it's free, okay for me it's free. Yeah, but that's in the box, just to be specific, and then on the laptop. We use a VDI so we've got a virtual app basically so you have to provide your own laptop, but you don't. You go into the VDI through the laptop. So it's an app you download onto your own device and then we have two factor authentication to get into it right

Researcher 02:15
for your work. You mean for the work stuff that you do work. Yes, okay. So you don't, you don't have a company laptop, you have your own laptop that you go through to a VDI type access rate, okay. Now that's interesting.

Participant A 02:28
Yeah. Everyone's hopeful that we'll get our own. We're moving to we're moving to building next to spark next year which is going to be more accurate, urine, the only way. Yeah, yeah, disking and things but I'm everence, hoping that they'll go back to laptops for hot

desking just because of this. Yeah, not that flexible having a VDI but anyway, we'll see. Yeah, okay, it's how it's, how they're going at the moment. There are some pros and cons,

Researcher 02:59
there are, there's always pros and cons. I've been involved in the topic, know the topic, I'll bet off track, but I was involved. I was brought in to get involved with the new building project with with SP, so that's quite interesting because that's how activity based work activity based working and agile working or kind of, you know, concepts that sometimes

Participant A 03:22
they say building in the mount.

Researcher 03:25
Mount Yes, yeah, yeah, that's my, that's my building. I did that. Anyway, getting off track. So, on your, on your devices work or or home, personal but there's obviously an overlap with yours. Do you have a. Do you have a preferred access mechanism in terms of your password or PIN or fingerprint or facial recognition, or do you know, do you have a choice about that or I,

Participant A 03:59
so I, my, my mobile phone. I have to have a pin. Let's find out the easiest way, you know, in terms of all the different ways you can choose it does, does also have face facial recognition, but I actually, we're also required by wit to have a pin on our phone and writing. Yeah, somehow they can check that to make sure you've got a pin, because you've got your work emails on there so. And then on my laptop, I, I have a password, or a password to get into my space and then when I open up the VDI is also his two factor authentication whether you know app on my phone that I have to go into to get a pin number to go with my, my weak password.

Researcher 04:52
Okay, good. Yeah, makes sense. Yeah, yeah. Um. So this, again this is obviously, this question is, it may or may not apply, obviously because what you're using the same device for your work and home but do you. The question is do you use your work laptop or phone for personal use. Obviously because you're using the same laptop and phone then you're using it for both work and personal use.

Participant A 05:20
Correct. Right. Yeah, so I guess the short answer is yes,

Researcher 05:25
short answer is yes. But presumably when you're so on when you're in the VDI on your, your laptop, then, is that like, is that something I'm not used to, but is that something like Citrix or is that it's

Participant A 05:40
more like it's more like an app having an app, open, right. Like you go, you open it up through authentication or opens up a view of your desktop. So, just like if you were working straight into your work you know an open Yeah, I mean it just leaves it when you close it down. You don't have to log out, it just leaves it where you are open, so if you've got weird open and some other windows open, they just still stay there and you close it down and you can get into it, or ever you. So when I'm in the office I open up it'll look

exactly the same as going through this app that's on my laptop, so I still get the same picture, right. This is just go into it says access.

Researcher 06:28
And that's regardless of whether you're at home, presumably using your own access network, your, your own Wi Fi or is that, or tricks Yeah, or, or in the in the office on like,

Participant A 06:40
it's like opening up Instagram, I can use any device you like but you get the same information, put up in front of you right so you can go into Instagram through a different, different mechanisms, other than the fact doesn't got a password but you still say exactly the same thing wherever you are just using different, and it's just the same.

Researcher 07:01
When, but when you take your lap, your personal laptop to the office does the thing, default to the office network or does it automatically does it plug in anywhere or go to office WiFi take

Participant A 07:11
it to, if you tape it to the office, you have, you can't plug it in, you've got to use the office visit. A Wi Fi, that you can use so effectively if you're using your laptop in the office, it still uses a VDI IP from memory. Yeah, if it's your own device so we also have a whole lot of people have the kind of BYOD thing where you've got your iPad or some other people bring in tablets and other kinds of things that are more transportable which I don't hear, But that is again you connect by Wi Fi I think you use an app. The system works so that you can only ever see one version of your desktop or one so if you're on my laptop at work, it wouldn't. It would, it would close down the VDI and then similarly if I went and logged on to the VDI, it would close down the laptop view so only his one active view at any one time, if that makes sense.

Researcher 08:15
Right, yeah. But you'd only have, you'll be accessing the VDI on your, your personal laptop anyway, is that right. Regardless, Yeah,

Participant A 08:24
yeah. Friday, I generally don't take it in because I hadn't got there working quite well and I quite the videos are, you know, super large screen and you can go to any workstation and the office then,

Researcher 08:37
so the office. So the office has got workstations.

Participant A 08:41
Oh, yes, and the office we have a screen and a keyboard, right, and all of the computing, I think it's a little box now on the back of the there's some localized computing power, but most of it sits somewhere centrally. And you can log in to any, any thin client I think it's the language. Yeah, and get your desktop app desktop Yeah,

Researcher 09:07
yeah. Okay, that's fine. So. So again, probably some of these questions are a bit redundant for this scenario in terms of do you use your personal laptop to carry out work

tasks. Yes, obviously you're using your personal laptop to carry out work task because you're opening up the VDI session on your.

Participant A 09:28
That's right, yeah, I get it I'm working within that, within that environment theory,

Researcher 09:31
yeah. Do you use your personal laptop over work network. And if there has, has it's been modified to achieve this, so presumably the VDI, is a VDI software loaded onto your laptop was that just like an app or type scenario that has your IT department has the IT department at work had to modify your laptop to run that VDI or

Participant A 09:56
not modify, or they get in a locker, go to the site download this piece of software, right. So, it is an app that sits on my laptop but it's self installed or installed by me it wasn't doesn't require someone else to do it but you do need that on your laptop to make it work. Yeah, and I'm just remember whether I think it's, you know like you have to get a special email from, you know how to IT support to actually download it and throw me with Excel weeks or not. Sorry, it's,

Researcher 10:33
yeah that's fine done. Yeah, yeah. So do you like when do I do you have any concerns around because you've got work do you have any concerns around that that work, that work or, or the business company you work for having the ability to access your personal stuff on your laptop or

Participant A 10:51
no because I, in general for everything I use it's, it feels quite separate because it's not. It's an I'm going in through a window into a central server I don't feel like they can come back out onto my laptop, whether that's true or not. Right. I guess I personally don't have a concern about that, and then picks, because I don't have too much of a laptop either, but I don't think that that's a good question, is it a risk or not I'm not sure. I'm concerned with anyway,

Researcher 11:23
for example you're carrying out your work through the VDI window into the corporate net bother your desktop, but at the same time you could be the same time or during the day that you're on that you could be then doing some I don't know online banking, for example, would that be a concern, would you, would you have concern the fact that you had your VDI open and you were doing your online banking or would you kind of close one day and then separately.

Participant A 11:43
Generally, close the window down but I guess it's still open, but I haven't. And I tend tend to use my phone for online banking, but yeah, I haven't been concerned about it. Should I be that might be a different question.

Researcher 11:59
I don't know. That's but I suppose that was part of this research is that you understand, I shouldn't

Participant A 12:05
be it feels like there's a lot more there's a lot of authentication around it and I guess. It's an interesting point because if you have trust in your company, then you're not for me I'm. I don't feel there's a way that the video I could then control your machine but having said that sometimes when you, you know have problems with sound and things like that, when it often comes back to, you know, entering the help desk, they end up having to get onto my personal machine to change some settings, all right,

Researcher 12:36
live I like to, I like TeamViewer or something like that or

Participant A 12:40
is that yeah that's remote X remote access, yeah, yeah. And you, you agree to let them in, but I mean it's still, you know, again, it's kind of a trust thing isn't it but this is where you can have external people on your own personal laptop. So, yeah, I mean I, it's an interesting question and there's some people I know feel very strongly that we, we should have provided devices, rather than being expected to provide our own so. Yeah, that's interesting. The only other thing. The one thing that does annoy me is this something to do with the way we've got my Microsoft Teams deployed in our VDI and it does pops up on my own personal workspace for some reason and I can see my calendar and I think that's probably a problem with how they've set it up because we aren't really using Microsoft Teams yet, as a business but that's when I start to think about, oh, that's feels wrong. Feels like my work is invading my personal laptop space,

Researcher 13:46
that makes sense. Yeah, cuz it sounds like it's quite, from your perspective how you use it, it's quite segmented in terms of that, you know, your personal stuff is your personal stuff and then your work stuff within that VDI. Yeah, yeah.

Participant A 13:57
So the fact that this pops up and there's nothing wrong with it at the moment, keeps telling me I have to do some sort of courses into occasion but it's not inside the VDI, and I mean I probably should bring the help desk and try and sort that out but that's kind of so you know, the bits and pieces that you think well it's not working quite how I think it should work. So,

Researcher 14:15
so your work stuff is then appearing in your personal outside of the video is that right the team's side of things.

Participant A 14:21
Yeah, just my team's just the calendar, you know, kind of in day out days take teams either teams calendar but I can see. Yeah, and I might fix right so it's, yeah, I know that the sitting problem or. But, you know, to the point about trying to hit with things correct compartmentalised. That makes me feel that feel that gives me the seats are secure, whether it is another matter but.

Researcher 14:47
Right, yeah, yeah. Okay. And is that a similar scenario with the phone I did that the phone use VDI or is that completely different is that the

Participant A 14:56
phone doesn't at the moment on the phone I've just got, you know, an email box loaded. And let's just using an email app and you think it's an Outlook Exchange, or exchange. Exchange here. Yeah. And so the only the only security on that is that password, and then some people have got Skype for Business loaded on their phone, from our workplace but I've never managed to get that to work on my phone so I don't have that,

Researcher 15:29
right, and so phone or you may not be aware of this, does your phone have anything, you know, cuz I haven't obviously I understood that saying iPhones have like this supervisor mode or they are sometimes companies put mobile device. Mobile device management on your phone to, to be able to access more on your phone, or not.

Participant A 15:51
I think no, I don't think so, but then they can tell when you've got to persuade, so they must have some were understand that they can do that, I don't know.

Researcher 16:02
Is that an iPhone, or no, the Galaxy. Galaxy, a Samsung Galaxy. Yeah, Samsung Galaxy something

Participant A 16:13
still technically you can tell,

Researcher 16:16
but you brought you, you bought that yourself and then claimed allowance for that. So but they haven't they haven't taken that phone in and done anything to it, they've just No, you've just downloaded your, your, your mails and added your ad exchange access one yet. But you say, I can tell you whether you've got a password on it or not, they can connect if they can tell.

Participant A 16:36
That's what I've been told that, but I don't know if it's true or not but they did ask for you to put a password on but they actually tell you you haven't got one. I don't know. Right. I think company policy is that you had to have a password resets here. Right. Yeah.

Researcher 16:50
But you don't know whether they've got any mobile device management, or not at this point in time,

Participant A 16:54
no I don't think so because I've never held the seat up so I

Researcher 16:59
know. Yeah. Okay. and then. Yeah, for both your, your laptop and your phone which you use both for personal and work use Do you ever. Do you ever use those ever public Wi Fi, like, you know internet cafe cafes with internet access or hotels where you access stuff or

Participant A 17:21
laptop no phone Yes,

Researcher 17:27
right. You don't you don't go when you go travel on business you don't use a laptop or a hotel Wi Fi network or something like that. No. Okay. And are there, do you have do do have restrictions in terms of what you do on your phone over those type of networks, if you're using Wi Fi and I know. So what would you do, what would you do all sorts of activities like riding social media or online banking or shopping.

Participant A 17:58
Yes, well certainly, social media, probably not so much online banking or shopping baps oh well at home I wasn't. That's not what this account is public.

Researcher 18:14
Now we are talking about if you're out if you're out and about and you, you know,

Participant A 18:19
probably a social media. Right. All right, things like you know, the best,

Researcher 18:25
the best app. Yeah, yeah, exactly. It's pretty different things you use when you're out exactly all the stuff around, how do we ever get around without phones. How do we ever meet up with people.

Participant A 18:37
He's like, put your phone away because I always look a backup now but first it gets away. Put it away, you, you grew up with a phone. He's like, he's sort of like his auntie. It's quite funny, he's a 19 so he's kind of like you know the, oh, you just need to find a way to get from A to B, you just use a brain and I would just faster with the phone because I hit submit. Anyway, yeah.

Researcher 19:02
Okay. Um, so, so, so typically public Wi Fi on your phone, he would typically use apps like Google Maps or bus apps or social media. Are there any, any activities or apps that you wouldn't, you'd never use ever public Wi Fi is actually I'm never going to use banking stuff or I'm never going to pay for credit, pay for something over a credit card or, or not. What I you know

Participant A 19:33
I probably know I wouldn't say that I consciously think about that if I had to I would. Right,

Researcher 19:39
yeah, yeah, yeah, okay. And in terms of how you, you manage your, Obviously we all have multiple apps these days where we potentially have different logins for different things, different login with Facebook or LinkedIn or whatever or banking whatever do you apply a higher level of higher level of security for different things I do say I'm gonna, I'm gonna, I'm gonna apply a much more complex password for my banking than I am for my social media for example because I don't care about my social media because

Participant A 20:17
I'd say yes and probably the only things I banking is one of them. And then there's a few things like, oh, you know, like my real me, identity, right, yeah. Yeah, a few things like that

where I have complex passwords, but then for whole other stuff I don't use the same password.

Researcher 20:37
Yeah, okay. Do you do you ever use i These, these password management apps like apple key chain or stuff like that, do you ever

Participant A 20:47
tried to use one because one of the, one of the somebody recommended them but I just found it really annoying. I couldn't get into it so I've tried it but no.

Researcher 21:00
Yeah, do you remember what that was what record

Participant A 21:03
was a few years ago. He was a real, it could have stolen my phone probably. Was it across Sibley visa now but I can't think what it was at the time it was called might come to me while we're talking. I can remember him. I can remember some things he was that he was their head of architecture is always promoting it, but was it

Researcher 21:36
does matter. Stop, not relevant, politically for the questions but I was just interested.

Participant A 21:42
Nice. Anyway, I remember properly I can miss a shoe.

Researcher 21:48
Okay, if you remember, let me know. Yeah, yeah, yeah. Now if you do, definitely let us know on your work on your work access or your work stuff. Do they, do you get, do you have to change your password regulate do they prompt you to change your password every so often,

Participant A 22:04
every three months, you have to change your password. Yeah. Okay.

Researcher 22:07
And do, do you, in your own passwords for your own access to banking or Facebook or anything, any real mean whatever do you do regularly change passwords or not.

Participant A 22:20
No. No. Ever. Occasionally,

Researcher 22:28
and if you do, if you do what prompts you to change it.

Participant A 22:32
Sometimes, knowing that it's a sensible thing to do but not very often. Mostly, or sometimes I've forgotten the password, because I have kind of one ish passwords and then there's some sites with it require, you know, numbers and letters and some special symbol or something else. Yeah, if I know sometimes, or it's a sign I haven't been to and then you can't get back in so then you change it again. So, those sorts of things would

prompt me to change it. I have had an invite just recently I had somehow got my, my. I've got two kids and one of them got stolen so I wasn't quite sure on what site and where so I changed a few cards. Few passwords after they happened, just to see whether it was right, like a takeaway so I saw something worked and it wasn't as secure. Yeah. Okay, all right yeah cuz I hit someone who put charges onto my credit card, it was trying to say.

Researcher 23:35
Yeah, okay. And have you ever been the victim of of our like a cyber attack. Have you ever been impacted by that.

Participant A 23:48
I don't think so. I'll just remember I think. But when I was years ago, my son was playing hit the key hit one. When he was playing lots of games I don't think I've ever hit one though. I say no. Okay, that's fine.

Researcher 24:03
And do you find those sort of like a tat like phishing attacks for example I'm not that's not the only an example but phishing, do you find those kind of fairly easy to identify when stuff comes in or,

Participant A 24:17
or I say yes, because the cipher. Well, at the moment anyway, lots of them have, you know, they're really strange addresses when you start looking into the detail of the email, it comes from an odd place usually and

Researcher 24:31
so the way you pick that up is by looking at the email address where it comes from or,

Participant A 24:36
yeah, yeah, yeah, and then some, you know, banking is usually my bank has usually been very proactive about sending out stuff saying, or giving examples of what sort of phishing things around or reminders about that so that's quite good in terms of keeping it front of mind and Tim's are looking out for those things they're quite good at it. Sort of proactively messaging you to keep kicking that you're not being asked for the wrong things. Phil I haven't hit as many recently, sort of a spate of them for a while back. Yeah, to know.

Researcher 25:12
Now then they come in spectrum they come in at certain points in time iPhone as well so I find with the iPod the iPod, for example, it's a classic where it comes in touch, you've got a refund you go like well there's, there's no way I've got a refund because I did my own tax return. Refund. Yeah, yeah. Okay, um, and how concerned are you about, or how much do you think about identity theft.

Participant A 25:43
Um. Oh, good question. I think I'm increasingly concerned I guess but I guess at my level was low, but then I've been hearing just recently people talking about. Do you give your real birthday when you're putting, you know, a lot of these sites, ask you to like shopping sites, asking you to put your birthday in, and I was at a conversation where people were talking about Well, no you shouldn't give me your real birthday because it's an opportunity for identity theft so I've been thinking about it more. Just recently, about whether you

should have a fake birthday. So, I think, I'd say. Don't think about it much, but thinking about it more is probably a good that I had before. This is my summary where I made.

Researcher 26:43
When you get these questions on social media where they're asking for, you know, what was your first car or what you know what, what plate set Have you been to do you ever think about that in terms of, do you think about that in terms of, it's just a game, or just a game or thing on on the social media or do you think about it in terms of okay they're trying to harvest information from me to try and build a

Participant A 27:04
probably think about the letter T to ignore those things just because that whole, I don't know, having watched the Cambridge analytic and that you

Researcher 27:16
haven't watched it now. We're difficult yeah

Participant A 27:19
yeah but that kind of sentiment about, you know, being able to take away data, I mean, you do see that if you click on a whole lot of links to advertising or you Googled something turns up, two seconds later, get all these ads and social media so you can see that your information is personally, you know, it's been used. Yeah. Which is how it works but, yeah, you know like, interestingly, but my kids don't use Facebook at all. Like they're still on Snapchat and Instagram but it's kind of a wave away from some of those more traditional apps, partly for I think all these different reasons.

Researcher 28:03
Yeah I think generations use different ones alike so I'm on Facebook right now and both are gals are on Facebook but they're more likely to use Instagram or Snapchat gets bounced.

Participant A 28:16
By my kids like Facebook. They haven't quite deleted their profiles but

Researcher 28:28
to stay a different topic i. So, at work or in your current organization work for previous organizations have you received, you know, cyber security or privacy type training at all.

Participant A 28:41
Um, good question. Okay should remember any but probably have had some create some privacy training, I guess. I mean I'll say no because nothing really comes to mind.

Researcher 29:07
Right. Yeah, that's fine. Yeah, and on your devices do you do you or does the company mandate you to use your both internal your phone or your computer or laptop devices. Do you use any antivirus software.

Participant A 29:27
Um, no, I don't use any antivirus software.

Researcher 29:30

Any reasons for that at all.

Participant A 29:34
So on my laptop I use tip antivirus software for years. And for some reason, you know, it was one of those subscription things, I guess I've read quite a bit of consumer, which they still recommend you should have it but I, then I currently but I did, I did have might be a little while ago I did have it oh no I'm removing I might have had a, some sort of cybernetics analysis, a few years ago and took it and got it fixed. I think they loaded something on to the laptop. Probably no reason other than just a notion. And then on they're fine. I've never had anything on my phone either.

Researcher 30:25
Okay, well that's fine, and was talked about phones and laptops but do you think about security or do with the Terms of Use and connections or with other devices in their home or at work so you know in terms of First you've got your, your home network and you've got a potential to have a smart TV or you might have. Smartwatches of, you know, fitness bands or stuff like that, do you think about that in terms of use of security risks or anything like that.

Participant A 31:05
So I guess just got the normal password on the Wi Fi. And the other, the other thing I guess is, I mean that, I think probably the scenario was when my kids were younger, we would come around and they'd be giving away your password for your Wi Fi, left right and center. So that's probably when I was more top of mind. Yeah, not now. No, I don't know.

Researcher 31:38
Okay. And do you say do you think, with. Do you think with working more from home in terms of a COVID scenario. Do you think that has, has, has affected the risk from for cyber attacks either, either at home or work because you're doing, you're doing work stuff then over your home network, and then.

Participant A 32:03
Yeah. So, we you know the one that was done a few weeks ago were impacted by that because that was focus one, and our VDI set in a data center, where the, I think it was the links into that data center were somehow. I can't actually remember the details of that tech but they meant, all of our videos across the whole company went down for about an hour and a half. Right, so that was that was never happened before, but quite a risk. Now in terms of realizing how dependent you are on the company to have a robust network. So it wasn't actually the device, it was something to do with the network. I do think it's it. I pissed off that we're in the throes of lockdown and things like that but at the end of this, you can't help feel that it's something you'd want to review just because we've got really is quite unusual and I think people are moving away from it again and whether that's not just a security point of view but whether it's the best solution for how we've worked, It's quite difficult to have a consistent experience and everyone's got a different device, you jumping between apps and like on my device and sometimes it works randomly and other times it doesn't and I go to the, you know, the actual the actual IT support required, And I guess security is part of it could be a lot higher with people trying to use their own devices at home. So, yeah So short answer yes, thinking aloud. Yeah,

Researcher 33:51

okay. And so what do you think about your approach to cybersecurity because it's always a hot topic these days. To what extent do you think your actions match your intent, as in, do you do think about it and then think actually, and I then do actions based on what I'm thinking or do I do you think about it, then forget.

Participant A 34:16
I think I do what's required in order to do my job I have to use security, a user apps and things to get access. I'm a little bit more conscious, particularly since I paid my credit card numbers stolen about where I'm sharing it to. And I think I guess, interested in dinner as a topic just because it's been very topical in the last couple of months, but I don't think I'm, I haven't changed any of my own actions, in terms of my own setup.

Researcher 34:54
So when you say when you had your credit card details stolen. That's, yeah. So as that did that resulted in loss to you or.

Participant A 35:06
So it was, it was a something like $22 charged to my account in the middle of the night, and I found it fairly quickly. And so I've got that money because or the way the bank works, but we couldn't work out who had, you know how that has happened, that's occurred I I've got like a separate card I use the debit card so it's got quite a low right balance on it for using, you know, I've got it set up to use online for. We don't feel the securities is tight so that's actually something I guess I've consciously thought about doing, and using, because I don't necessarily trust websites, security, so yeah, actually I've taken.

Researcher 35:57
So once the action you've taken sorry is to do,

Participant A 35:59
so I bought I've got another credit card that I've got a low balance on so that if it gets stolen, the risk to me, will end and the bank covers it anyway but just, you know, you can't. You can't do a small transaction

Researcher 36:16
on it until you use that one online for online stuff in preference to others as well.

Participant A 36:21
Yeah, yeah, and particularly for for sites I think dodgy. Right. Site takeaways I mean it's like there's no just me deciding that they're kind of randomly, don't kill it they've got much as much security,

Researcher 36:34
what, okay, what would you yeah what, So when you, when you go to that press to thinking of what what type is dodgy What do you how do you think about that, what do you think, do you think actually that this is dodgy I'm not going to bother you know,

Participant A 36:46
some of them, like, someone that you have pictures from before, or it's not a kind of chain store which I kind of assume as he got better security, or, you know, some one of those takeaways places seem to use like the same kind of app when you so I'm never really sure

about how secure they are sort of a simple way, looks the same, so I think okay I'm just gonna use that card for that so it's kind of where we're at feels like there's a higher

Researcher 37:18
risk. Do you When, when, slides, acid asked you to remember your credit card or debit card details or not, do you not typically do that or not, all

Participant A 37:31
generally know the, you know, I mean the other thing of it. Yeah, yeah, I'd say no I don't say I say no, I'd rather read into them but then some of them seem to remember that, regardless of what you say. Anyway, not quite sure how they all work now. Sometimes I go into sites and they go I haven't need to load it again and pops up again, Google Pay thing. Does that say, right. Yeah. And do you work here. Sorry. Getting married here. Yes, yes, time goes on, yes.

Researcher 38:06
And in terms of. Do you have any thoughts about APA yeah what type of applications you use so do you. Do you have any thoughts about avoiding, you know, big popular applications, because they are likely to be more. They could be more subjected to a cyber attack because they've got lots of people on them or do you, do you not think about that deja Shizuo apps you want to use basically.

Participant A 38:34
And I probably will lead by some of those game apps end up sending you multiple. But I take care of you feeling a little bit so that's one of the things I try to avoid those because I ended up getting around by accident, the other day and then wouldn't let me teach like I couldn't do anything on my phone at all so I'm like, delete it as fast as possible. So I do, I guess I've tried to make sure I'm using it positive, at least, some will seem to be credible, or highly rated maybe and you're looking through the, through the extra if you're buying it, you know, or not buying them probably downloading free ones but which ones are rated higher read I'm not really a great big app user so I'm probably not. I've just got my set of IPS I use nets. That's right. Yeah, they tend to change the match.

Researcher 39:31
Do you ever download. What do you ever do you ever use apps or download apps that are not because I suppose you know Apple, the App Store is one example where they obviously they stuff that's approved in the App Store and if you try and load something on an apple that that's not in the App Store, you will flag to you and say, Are you sure you want to do this, do you ever download stuff that's not not approved or not being verified or. Okay, cool. I think that's

Participant B

SPEAKERS
Researcher, Participant B

Researcher 00:02
Okay, so what I'm going to do is I'm going to run through a series of questions some yes some of may or not be relevant depending on your particular scenario. So you know if there's, if there isn't an answer there isn't an answer if and if there's no that you're uncomfortable answering obviously just say you know you're not comfortable answering. Okay.

Participant B 00:23
As long as I've got under this thumbs up here but on these zoom calls as we hit them with 15 people on rather than saying Is everybody okay, we go like this.

Researcher 00:32
So, on the camera and not the not the not the one on teams where you can press a clapping or whatever. Yeah, okay. All right, so I think the first thing I want to understand I suppose is just the types of devices that you're using for access to, you know internet or technology or whatever. So, do you have like separate, you know, separate work and personal mobiles, or do you just use one for everything, or just one

Participant B 00:59
work mobile right slash personal one mobile,

Researcher 01:03
yeah. Okay, as that started work mobile is it. Yep. Okay. And what about things like laptops or tablets do you have work and separate work and personal ones or

Participant B 01:16
no that I just use all the work ones so I have a work mobile phone, a work, iPad, a work laptop and work tablet, just to make it complicated.

Researcher 01:32
I work tablet and I work iPad.

Participant B 01:37
But even though, this thing is it's a Microsoft, this is, this is the one I use for team meetings is probably another, I call it a laptop or.

Researcher 01:46
Yeah, yeah, yeah, we have like a I guess a tablet tablet with a touch sensitive screen of some sort. Yeah, okay. So you say that, but those are all work devices provided by the company you work for, for you see your work. Okay, cool. And, you know, for your devices the like that, an account may vary between devices. Do you have a preference or do you have a preference for your security mechanism that useless devices Id prefer password or PIN or fingerprint or facial recognition or

Participant B 02:21
on the password guy, really. Okay. Under under under APL by use the, you know, use the thumbprint in the facial recognition on the phone, because that's what drives you to do. Yeah, I'm pretty passive but do whatever the device requires really in my natural Fallback is still a password.

Researcher 02:49
Okay, and, and as a company, company work for mandate and a particular type of mechanism I know some companies have say you must have a six digit PIN or whatever on your phone or whatever if you're using banking staff or

Participant B 03:04
not for general access to the device, but for access to the company's MRP system there's you know, a level of complexity required and your password. And for, you know, access through to the company, you know, big approval payment system there's some, you know, again some fairly strict requirements about the password.

Researcher 03:35
Okay. All right, good. Thank you. And so given you, you're obviously got four work devices that you use for for work so do you. When you, when you're doing personal stuff i.e. personal emails or social media or online banking, or online shopping or stuff like that. Are you using those devices.

Participant B 04:05
The phone Yes. Mobile phone yes but pretty much everything. Otherwise, we've got a you know a family computer in the house and I do, I do most of you know, online banking or online shopping on the family home computer, but I do a little bit of social media on my phone.

Researcher 04:25
Yes. Okay, so you've also had science in addition to what device you've got a home computer that you use that, and that's for the whole family not just fi, not just for you. Oh, yeah, yeah. Okay, so use

Participant B 04:39
it everybody else in the family has got a laptop, a personal one.

Researcher 04:43
Yeah. Yeah, I remember that scenario I was, I was saying back in there, back in the day when I was at telecom I pretty much had to wear a laptop but I didn't have my own laptop but everyone else had a laptop so yeah, I recognize this scenario. Okay so, so you did a little social media on your phone. But you say you don't you don't generally go and do personal stuff on your, your other like your laptop or your, your work laptop or iPad or tablet you don't tend to go and do personal stuff on that, or,

Participant B 05:20
no, not, not very often I mean I'll watch, I'll watch the occasional movie on the work iPad if I'm, you know, being kicked out of the house and have to go somewhere else, but that's the data right here, I try and keep work devices for work, right you know within.

Researcher 05:36

Are there are there any are there any activities that you said, generally, are there any activities do you would never do on our work. Work device at all. Just the fact that I would never get it like for example, you might say well I would never go and I would never go and access my, my online banking on my work device because I don't know whether it's secure or not or,

Participant B 05:54
no, no, no, I would if I needed to do I would do anything.

Researcher 05:59
If you needed to do with anything, okay. Yeah, yep. And on the reverse side would you do you do any on your personal on your shared family computer do you do, do you ever use that for accessing work at all and any scenario, no, no. Okay. All right. Great, thanks, um, and obviously when, when you're using your work devices now like so in a particularly pandemic COVID environment where you're working from home or presumably you're using those devices over your home Wi Fi network. Yeah. Right, yeah, that's all. That's all devices or

06:48
generalists, yeah, yeah, yeah. Okay.

Researcher 06:53
And in terms of your work devices when you're, when you're out and about or traveling or, you know, when we're allowed to go and meet with people for coffees or whatever, they would you do use those on these like publicly available Wi Fi network so in cafes or hotels or whatever they use those devices over those type of networks or

Participant B 07:18
yes I do occasionally met you know, mainly the man in the Wi Fi network and airport lounges, right, you know, yeah the the main one that I would use Yeah.

Researcher 07:30
What about cafes, provide free and fair access so stuff like that, or,

Participant B 07:34
no,

Researcher 07:36
no. What about hotels if you're traveling on business

Participant B 07:39
hotels, yeah, yeah.

Researcher 07:42
Any other stories where you might be using those devices over another network or some something other than the corporate network or your home network or their mobile network.

Participant B 07:56
No I don't, I don't think so. I mean I, you know, if I go to another work location I either tethered to my phone to use the mobile app, or fans are plugged in at work or the work Wi Fi, I guess, but I never work in a cafe or a library or anything or a shopping mall.

Researcher 08:17
Just what about personal and what about personal stuff. Would you ever do pastor stuff over that like there would you use those. I don't know if you needed to write. No, you have no coffee want to check out whether some stores got some devices available or whatever or

Participant B 08:33
theory really I might. The other day I was in a shop and they it was down, so I use the, I guess, I use my mobile phone to do an internet banking while standing in a shop, but that was over the

Researcher 08:50
head with a mobile network might have a body of work. Yeah, okay. Okay, cool. Okay, um, so, though, and when so when you're using the Wi Fi in the airport or in hotels for example so you're you're traveling on business or your. Is that just for work activities or,

Participant B 09:16
or you're primarily for what, but I'll, you know, I'll see if the internet, you know, read the newspaper, right, you know, check out the football results. Yeah, that kind of thing.

Researcher 09:29
Yeah, what about other things like social media, or financial banking staff or shopping staff or.

Participant B 09:39
Not really, no. Just, just, not out of any great reason I just I'm not a big social media or online shop or war person so, you know, that really occurred to me to do that stuff other than when I really need to.

Researcher 10:00
Is that because you're not you don't really do that much of that stuff or is it because you think in your head, actually I'm not going to, I'm not going to put my credit card details in over, over this network or was it a combination.

Participant B 10:12
It's the it's the it's the former I just don't do that stuff, right, it's not, it's not a conscious, or I don't want to do this on a stranger's WiFi network, it's just, uh, just don't do that kind of stuff.

Researcher 10:25
Right, if you had to say if you had to do if you had a scenario where you had to do something like that, what would you do it, or, or not, or what do you tell.

Participant B 10:32
Yeah, I probably would. Yeah. Yeah, lucky if I was in Australia for work and my wife called me up and said that bills come through from the contractor for this, can you pay it. I would, I would. Yeah, I would just log onto the device and make the payment.

Researcher 10:57

Right, okay, cuz I wouldn't be constantly you wouldn't think actually I'm not an artist to go on our credit Thank you. So when he, when you think about the applications that you do use online. Personally, do you, do you apply a greater level of care, on, on some, some password accesses and others, Id you depend on what you're doing like do you say well I have social media not worried about it, therefore I'm just gonna have a fairly basic, easy, easy password or mechanism on that online banking I have, I'm going to, I have more focus on that and being more secure or Sundew without getting into detail obviously how you do that. Well,

Participant B 11:47
you know, for the for the for the online bank. It's the one, you know, reasonably complicated password that I don't write down anywhere. And you have. Yeah, and it's and it's unique for everything else. You know, they're all. Yeah, no list on the phone. Yeah, you know, yeah, and remarkably similar because these days. It's incredible. Why will you get 50 of them, you know, yeah, one of the neon ones of this one but.

Researcher 12:24
Yeah. And do you do you ever use these no password manager type applications like you know an iPod as opposed to Apple key chain and stuff like that, Do you ever use those. All right. And is there a reason for that or

Participant B 12:41
not just not really aware of them, right, what they are or how they work, just don't know about. Okay, yeah, I was still born in the wrong century poor

Researcher 12:50
as as as xxxxxxx. So if I do this questions with a, with a different demographic than okay some different. Yeah, yeah. The reason I asked that question is, some people, some people use them because they're not aware of them or because they never got into using them and, and others, others, others may not use them because the guy actually I am a bit worried about all my passwords being in one in one location right. Regardless how much encryption is used or whatever. Okay. And the for your, you know, for your devices or your application that you do, do you change passwords. Passwords at all or often or

Participant B 13:41
not, not hugely often but you said Do you know, I do for that for, for the, you know for, well, for online banking, and for access to the work VPN, which are the two that I started those are the two that I view is, I have complex passwords for that are keeping the heat. Now we were aos. And those two I do change every once in a while. Mainly when I get prompted to change the work one or change the bank one.

Researcher 14:14
Okay, how often you get prompted to change your work one every six months. Right. Okay. And so typically you then change the bank whether they got somebody or person was only paying one at the same time. So, it's a trigger for my what is a trigger from a works change a password, then I need to change the password on other stuff then is that,

Participant B 14:33
yes, change the big one I don't change anything else. Okay, yeah. When you bring it down and you know you get forced to change them.

Researcher 14:45
Because you can't use the previous one you use. Okay. All right, and have you ever been victim, have you ever been the victim or become close to being the victim of a cyber attack. Have you ever fallen you know I've ever, kind of. Now your bank card compromised or you face

Participant B 15:06
it the bank, call me up and say, you know, there's been a weird transaction on your credit card, right, you know, in, and I've had to chop it up and get a new one.

Researcher 15:17
Yep. Is that, but is that a result of anything you've done or just that somebody else has compromised it or

Participant B 15:23
just somebody else has compromised it well as I understand it, I can you know they've just said, somebody must have obtained your bank details over the that we have or something like that, and there's, you know, there's a couple of purchases in Latvia. Yeah, they say, we've canceled your, you know, we've canceled your card. Yeah. You don't have to pay the money or anything but you need to add that up, and we'll send you a new one.

Researcher 15:54
Okay. And that's with the bank, contacting you, not the other way around not using our access but today I've spotted a rogue transaction on my

Participant B 16:03
account was the bank, bank contacting me.

Researcher 16:07
Okay, any other types of attacks where you, you've done something that, that led to a potential loss of of personal data or finances or, or do you find those sort of things kind of like phishing attempts, do you find those fairly easy to spot or

Participant B 16:26
certainly fairly easy to spot a few of them that you know these days. And these, these mainly come to our home email address because word filters seem to do a pretty good job of killing most of them but, you know, we get, we get some at home from, you know, reportedly from Netflix or from SPAC type stuff that look quite professional. You know and I and I. And I do that thing of I check the, you know you always check the email address that it's come from, to see weather looks like a real thing and just generally if it's saying, you know, we're about to terminate your account or something like that. I just assume that that's a. I'm not sure I assume it's malicious and delicious and don't respond, because I always assume if somebody is genuinely about terminate my account, or something that, in my account will terminate and I'll fix that knee, you know. Yeah. So, you know, most of them are easy to spot but some of them these days I've find quite, you know that they get by look really close to genuine and overtakes you know and I think on one occasion, I've run Spark and said, I've just got this, you know, I think it's, uh, you know, fake but I've just a bit. It's so close to the bone. I'm not sure and I said you know it's definitely, you know, fake email and we should delete it.

Researcher 18:11

Right. Yeah. Yeah, okay. And, and how, how concerned are you or are you concerned and, if so, how excited are you about identity theft.

Participant B 18:32
Yeah, only mildly, you know, I mean, it's, I guess it's, you know, I hear about it happening every once in a while in the newspaper and that kind of stuff but I don't know anybody know personal I don't know anybody personally has suffered from it so it sort of feels like one of those things that would happen to somebody out, you know, it's not, it's not something I worry about a lot on it at least mildly mildly concerned about,

Researcher 18:59
and how much is that, is that because he's gay and you don't know whether you do you don't know anybody who's been subject to it or is it is it also related to do you have a big, is there a lot of somebody find a lot, a lot of information about E on the network or or not or,

Participant B 19:20
I guess, you know, I'm thinking I'm the last white man in Auckland, not on Facebook, you know,

Researcher 19:26
that's becoming more public.

Participant B 19:30
Yeah, so, you know, I don't. You know, I don't have a social media presence, that I'm concerned about protecting. You know, I work, you know, I worry about the, you know, people getting access to your credit card, but I have. So I have two credit cards, one with a lower limit that I use online, and one with a higher limit that I just only use the old fashioned way, in a, you know, in a shop type thing. And that's about the limit of where I get to.

Researcher 20:14
Right. Yeah, and I, I, I am concerned about privacy in general or any aspects of privacy or.

Participant B 20:23
Yeah, I am I am not. Not enough to do much about it, you know, but, you know, I'm conscious of the fact that every time I search something on Google or buy something from somewhere. You know that somehow that stuff gets connected up, you know like, I buy a jigsaw puzzle. You know, online from somewhere, and I'll start getting ads on my Instagram to

Researcher 21:02
kick some puzzles. Yeah.

Participant B 21:04
And that concerns me modelY how that is, but not enough to try and do anything about it, You know the new Apple software upgrade now when you open an app that gives you that choice, it says do you want me to allow this app to track your movements across all other apps or not. And I say no every time today. Yeah. Okay. So, yeah, so I think about it, but I, but I, but that's about it, you know,

Researcher 21:46
yeah, yeah, okay. Um, on your work environment, either this, your current work that you do or previous work have you ever had any cybersecurity privacy training from work.

Participant B 22:04
Yes. But, yeah, fairly low key, fairly low key. It seemed as a team to, you know, a seminar when somebody will talk about the types of attacks and the types of things that worked as to try and defend them and, you know,

Researcher 22:24
has that training triggered you to do other things in your personal home life that you haven't done before or has cybersecurity training at work, for example, where you've attended a seminar, whatever. Obviously, which is a focus on on improving, you know, or getting better, cybersecurity behaviors at work has that then triggered you to do stuff in your personal life that's

Participant B 22:49
Uh I don't know its triggered me to change. Well, it is helped me look more critically at, you know, emails that come in, I guess, it made me more weary of emails from reporterly from Spark or Genesis or neon or whatever or Netflix, you know, when they arrive. I am thinking. First thing I'm thinking is, is that a fake. I guess it's made me apply a more critical view to unsolicited emails. Right, yeah, yeah, yeah. Yeah, okay, but that's about it. Yeah.

Researcher 23:33
Okay. And that presuming that training has been is like rare or not a continuous not continuous training innate is more one off a one off thing that's happened. Yeah. Okay. And for your personal device whether or not your pilot for I guess for your personal computer do you use antivirus type software on that or

Participant B 24:01
I don't know whether I do or I don't, I don't know, you know if it was if it was there when we, when we bought it, you know, but not consciously

Researcher 24:11
and on your, you know, on your phone, you know obviously your phones provided provided by your company. Do you know if that that's using any kind of mobile device management or, you know, iPhone supervisor type mode or whatever where the company is more controlling that device more or,

Participant B 24:34
I don't know. I don't, I don't think so. You don't think.

Researcher 24:39
But the phone presumably was provided to bought for all by and provided to you by the company was it. Yes. Okay. Okay. Good, thanks. And that's a bit of a general question. Obviously where from discussion you obviously well where's the cybersecurity aspects around stuff that could happen so what. Yeah, to what extent do your actions run on cybersecurity match your intentions i You're aware of things that can happen to what extent does that translate into stuff that he do to prevent stuff happening.

Participant B 25:25

Well, I don't know, it definitely is one of those areas where it's like, I'm aware I need to lose weight, but I don't do much about it. I you know I take some actions but not as many as I should. So I guess that would be the same, same, we're that did take some actions but probably not as many as I should, in the sense, as I've talked about I keep some passwords. Only in my head, and change those important ones, or use one credit card for online and only against that risk, in I, you know, pay attention to emails and if somebody sends me a bank account to make a payment to. If it's, you know, if it's a material amount I'll bring them and check first because that's a, you know that's a work requirement so that's driven into my head, you know you got to do it. You've got to have to two sources of verification of the truth, right. Yeah. So, but that's about where I start, you know, this is, you know, just talking to you has made me think, well I've never paid attention to whether I'm on a, you know, whether I should be more concernd when I'm using the airport Wi Fi or the or the hotel Wi Fi anything I never really think of my certainly my actions never change in those scenarios, right.

Researcher 27:14
Okay, now that's good. And, has, has your approach to cybersecurity changed as a result of working from home more than a pandemic or COVID-19 pandemic has that triggered you to think actually, you know, is there more risk from doing this or either in home or to work or whatever or has work said actually all they worried about is a word worried about people working from home, then became more compromised from.

Participant B 27:44
Yeah Look No, it hasn't changed. It hasn't changed me I mean I used to work there were to log into a, you know, VPN, right, to do, and you know we, we are aware enough for these things that we have a password on our home, Wi Fi so you know I assume it's only being used by the people in my house, type thing. And that's about it. Yeah, you know, you know, and his work concerned about it the other way around. Yes, yes it is and they keep working, a very close eye on who has x, you know keeps a list of who has access to what. Right, where, you know, what devices and what, exactly, and we, you know, not me but I know we monitor good ability to monitor, you know, activity on work devices from from home.

Researcher 28:48
And so I just saw your wife, Sonia Wi Fi talk about that before. Do you have concerns around you and your family's using it but yeah concerns around that Wi Fi password being shared with, particularly with children's friends, for example.

Participant B 29:02
No, I never thought about that, right, you know Yeah,

Researcher 29:08
or when people come in to say oh yeah people your visitors or whatever come in and they say hey we got your Wi Fi access or whatever and

Participant B 29:13
oh yeah we'll occasionally we had people, you know, adjust to their house and I always tell them the Wi Fi password, you know, the people you're trusting to stay in your house.

Researcher 29:24
Exactly. Yeah. Yes. Okay. Thanks. Yeah, nothing too tricky that hopefully.

Participant B 29:41
Sounds like interesting stuff pool is the same as the family. I'll just kids now

Researcher 29:48
I'll just stop this recording and that will conclude.

Participant C

SPEAKERS
Researcher, Participant C

Researcher 00:00
I'll just crack into it and say shouldn't take more than 30 minutes 3040 minutes or whatever. So, yeah, so, just want to understand the types of devices you have and whether they are personal devices or what devices so, because if you have a mobile phone.

Participant C 00:18
Yeah, so I've got, I've got a range of devices so I've got iOS devices, I've got work provided iPhone, I've got my own iPad Pro, I, I've got a company provided laptop. I've got a Google Pixel tablet as well. And then I've obviously provided devices for all of the different members of the family so then mainly mainly iOS but also PCs.

Researcher 00:53
Okay, PCs as in fixed term computers or laptops or no, they're all laptop or laptops, okay so you don't have any home PC that's not a laptop based. No, no, no. Okay. And in terms of your devices, either work or personal ID, do you have a preferred access mechanism that you use in terms of these passwords or pins or fingerprints or facial recognition or

Participant C 01:16
it's, it's, it's a mixture so my work stuff. So I've got my, my iOS devices that I have worked stuff on the security is the security is mandated by the company and the company I work for is extremely security aware. So, you know it's six digit pins, it's face ID, we use Microsoft authenticator, you know, we've, we've got everything is kind of two part authentication, it's very, very locked down in terms of, you know my work PC, you know, that's all. That's all password. And then in terms of the stuff that I've provided for the rest of the family, that's predominantly PIN.

Researcher 02:09
Right. Yeah. Okay. And so in terms of your, your work devices I our work fair and all your work laptop. Do you use those solely for work use or do you also use that for personal use, I do you do like social media or online banking or online shopping or stuff like that on those or.

Participant C 02:30
Yeah, I mean they're my go to devices. So, so they get they get used for, they get used to absolutely everything. I'm able to install my own apps and things like that on, on those they're not that lockdown. Right, and, and yeah, I, I don't really, you know I don't have another phone or anything like that and, and this laptop, tablet, I'm using the iPad is my kind of main tablet.

Researcher 03:00
Okay. So so the iPad is like a work device or your own device or no I

Participant C 03:05

paid for it, but I use it. I use it a lot for work because it just happens. It's just, it's just a very, very convenient form factor, right. And so, so, so I used to

Researcher 03:18
say on your on your site you use your iPad or an iPad for work on your home, or the home devices do you use those for work at all, or is it just your iPad or

Participant C 03:28
no so I use the, I use the phone or the PC for for work. My PC really doesn't get used for anything except work really, and then my iPad tends to get used for all sorts of all sorts of different things so that's that's the device. If I'm going on holiday. That's the device I'll pick up if I'm going sailing that's the device that I'll pick up and take with me.

Researcher 03:51
Right. Okay, so basically why because I want my understanding, you don't really have, you don't have like a personal device that you use for personal use and work devices at work for you to use they're interchangeable in terms of what you use them for.

Participant C 04:04
They're interchangeable we've got enough flexibility on the devices. Now, the way that we've configured them that that's possible. We used to have things like we used to have it such that you couldn't say for example, save, Word documents and things like that on the iPad Pro which was just really annoying, but now we've kind of configured everything if everything just go straight into the cloud. Obviously everything is massively encrypted. So because of that. It's actually, it's actually pretty flexible that I'm able to use. I'm able to use this device very flexibly, while it is also secure.

Researcher 04:40
Right, okay. And presumably when you're home obviously all your all your communication, regardless of devices over your home Wi Fi network presumably.

Participant C 04:49
Yeah, everything's over home Wi Fi, obviously that's encrypted. Yeah, or sorry that's password protected rather yeah I don't know, I presume it's encrypted I don't know, but protocols.

Researcher 04:59
Probably automate a lot of stuff. And, and your personal device may like to stay on your iPad but he when you, when you actually back in the office outside of pandemics. Is that does that connect over the, the, the, off the office network at all or does, yeah. And as I've been modified to do that or is it just straightforward.

Participant C 05:21
So, so I had to. So there was a bunch of applications that I needed to, or there's been, those applications I needed to download some mac mainly, it's a, it's Microsoft authenticator which enables that. So, we use Microsoft authenticator we use ages the browser. And, and, and, as I on a frequent basis there's essentially kind of an audit that's done on the device to make sure that it remains compliant so it's not the Upstate operating system it's, you know, got all different applications and they're all actually working, such that I can. I've essentially authenticated to remain to continue to access to continue to access the work network,

Researcher 06:06
and how often is out that audited to,

Participant C 06:09
I don't, I don't know to be honest with you, Paul. I know that there's, I know that I have to re log in. I mentioned a couple of weeks or so, right, and I would assume that as I'm doing that that that's when it falls, check but I don't actually know,

Researcher 06:28
in the background the background so it's not something that you're necessarily aware of it's just obviously taken

Participant C 06:33
a few times just because because of things that I've done and, And it's understand kind of gone through, or I've been, I've had visibility of the of essentially the map I mean, look, I can maybe do it right now, just one second. You've probably lost the video for a second, but you probably still got

Researcher 06:51
audio about audio yeah that's all good.

Participant C 06:54
Yeah, so. So what I've got. So it says it's on as your ad, it's basically to set up, it's to two step authentication, and, and the device is essentially backed up. So, yeah, there's, there's some there's something else that's that can be available but I don't know what it is to be honest with you, it's not visible right now.

Researcher 07:19
Okay. And in terms of your iPhone, your company provide an iPhone, that's your only phone like you say that, you know if that is that like, Does that have any mobile device management that's controlled by the company like supervised mode or, or,

Participant C 07:32
yeah, so we do have mobile device management, and I don't know which one it is, but if you give me a, if I can check if there's something that you want me to verify on it right now. But basically what we've got on this is. Hang on, let me just. Yeah, so basically what we've got our own kind of, we've got our our app store. So a company AppStore, actually. Yeah, that. So there's a whole slight set of of applications that are, you know, some of those are obviously related to kind of work applications that we need. Some of them are, are ones that are kind of related to security and and management of the device. We used to have, we used to use BlackBerry we still use BlackBerry on here so the BlackBerry application, and we moved over to essentially everything being on Outlook. When we went over to authenticator probably about 18 months or so, and that's been, that's been really good very very seamless.

Researcher 08:44
Right. Okay. Um, so because of us. Because you do like personal social media or banking on your work devices do you have concerns around security in terms of the company you work for having access to that or people at the company you work for having access to that or no I'm

Participant C 09:05
not, I'm not worried about that. I'm not worried about, I'm not worried about access, the company has taught me.

Researcher 09:13
And we've asked question I suppose in terms of is a company worried about so with obviously more employees working from home. You know there are a lot of COVID-19 that is, does a company have concerns around, then their, I guess their, their systems network being more compromisable from a personal perspective or

Participant C 09:34
I think most of the compromises that we would get relate to kind of silly things that users do. So, you know, using the same passwords across a whole range of different applications, you know, filling in stupid forms that, that hey, what's your mate with money. How's your mother's made pay with on Facebook, you know, things that people fall for. So there's, you know we do training for everybody in the firm, and we'll also send out. We send out kind of phishing links internally as well. Right, He who clicks on them. Yeah, but use that as an opportunity to then educate people so you know people have clicked on something, it's actually we've set it out and we're like, Hey, this is like look at the URL you should never have clicked on that with us this time. Yeah, yeah, that could have been somebody nefarious. Yeah, no, be careful. So I think mainly it's, it's, it's, it's about user, user education. I'm sure that, yeah, we will have and again I'm not versed in all the, you know, our approach, I'm sure it's kind of zero trust kind of end to end, kind of environment that we've that we've that we've that we've created, but I don't know any of the details behind it that's

Researcher 10:56
fine, I mean not not particularly what the research is about but yeah it's more about the human brain. So in terms of you talked about you obviously do training and you do you then do some tests in terms of phishing tests with, with company, is that, how often does that, how often do you do training is that a regular training or is it a one off or is it her.

Participant C 11:17
So it tends to be ad hoc. So, you know, people get that when they joined the company so there's an induction and they're totally all about those sorts of things. Then in terms of the things like the you know the fishing stuff. I guess I would say it's, you know, I might spot a couple of them a year or something like that. And again I filter, a whole bunch of emails I mean my junk folder just builds and builds and builds. So I don't know how many more there are that are kicking around that I just don't even engage in at the point in time I probably got 4000 emails that are unread

Researcher 11:58
by my inbox. Yeah. Okay, so good. That was good. Um, in terms of your devices, um, you know when you're traveling. When travels available again. You know when you're in hotels or airports, or you know, cafes or whatever, do you use, do you use public available Wi Fi networks with those devices and

Participant C 12:24
yeah I do so, we, we've always had. We've just changed the way that we do this now, actually. So, up until about three months ago we used a Cisco VPN. So whenever we were

connecting from hotels or public Wi Fi and. And now we've now we no longer have to connect to that ourselves so I don't know they're clearly layered in some additional level of security that means that we don't need to do that I don't know what that security is but a bit that's relatively new.

Researcher 13:04
Okay, so does that, that mean that so regardless if you're using that over a public Wi Fi network either yeah for coffee and you're doing some work in a cafe, for example, using their Wi Fi network does that mean there's a layer of security that the company has embedded in that or

Participant C 13:18
there's a layer of security that the company has embedded I just don't know what it is, so we used to say the layer of security essentially was was intrinsically embedded in the VPN that we have connected to. But, but, as of, probably about two or three months ago that that's that's come out.

Researcher 13:42
And are there any type of activities, you know, say personal activities like online banking, or online shopping for stuff that you wouldn't carry out over a public network Are you are you filling it's fairly secure.

Participant C 13:57
Good question. I can't think of a time that I've, I think online shopping if I was just doing something like on Amazon, I don't think I'd have a hesitation around that. I wouldn't. I don't think I've done any banking on a public network, and I probably wouldn't. I mean, given I can connect to a VPN I've got VPNs on both devices. Yeah, I think that if I was going to do that I will first connect to a VPN, right, to give the extra support, or do it on my phone right so my phone is on a macro network. Yeah and I, at least my perception would be that that is much more secure than using a public Wi Fi so I probably actually that's probably what I would do, I probably tethered to my phone and I would probably use that

Researcher 14:42
as a family system and normal block 4g 5g network or. Yeah. Yes, that's right, yeah. Okay, so you typically do your bank and stuff on your phone out basically as opposed to anything else. Yeah,

Participant C 14:52
yes, yes, I typically do, but I would not feel, even though I know that we've put in all this extra security on these devices, I probably wouldn't feel comfortable doing banking on public Wi Fi I've kind of, and again I don't know if the specific vulnerability that might exist, it's just, I just don't see the point in taking that risk.

Researcher 15:17
And when you think about your, your, you know, past activities or you know, social media accounts, banking, online shopping etc apps that you download, do you do apply a different level of severity I suppose when you're, when you're, when without obviously telling me how you, how you made pass what do you do, do you use more complex passwords for more important stuff or do you use password Application Manager your password manager type devices or.

Participant C 15:51
Yeah, Probably. Probably not, not a model citizen here, and I should be better than I am. So I probably had the same password across two dozen different things for years and years to be honest with you. And the thing that jolted me was that I then got some alerts, Thinking Chrome, saying that that password being included in a data breach, so I then had to kind of go and change everything. Yeah. And so, so, I've, I've got now, I've got a lot of different passwords, there's some commonality, so if I, you know, if I'm registering with, with, you know, Bunnings or something that is just, you know so I can perform a transaction. I've got kind of one kind of go to password across all those devices, all of those kind of commerce type got forms that I regard as being very very low risk, so I kind of know what, what that know what that is. Then, if there was something that, that I would. I mean I would never give my password never put my private details into something that, that I feel is dodgy so I definitely kind of look and scrutinize only really transact with organizations that I would regard as trusted in some way shape or form. And then in terms of password management so yes i i used password management that exists both within Google, and within apple. Right. And, you know, I'm, I'm comfortable that my Apple ID is secure, I don't use that for anything else and I'm comfortable that my Google password is secure and I don't use that for anything else.

Researcher 17:45
Okay, so use something like apple key chain for managing passwords or

Participant C 17:49
correct, yeah, so I use apple key chain, and then the embedded piece in Chrome, which, which works across all of my Google applications and on my Google device,

Researcher 17:58
right. Does that give you any concerns about having a whole lot of passwords in one place or not or not.

Participant C 18:04
Not really because, I mean, I've got to keep them somewhere and I can't keep 5050 in my brain. Yeah, I need I need the convenience of being able to use them across different platforms and I think that, you know, I will be. It's very unlikely that somebody is going to be able to crack into my phone and or crack it. I crack into my Google account.

Researcher 18:28
Okay, and how often, how often do you change passwords, either for work or for work, train you to change it or all your past

Participant C 18:37
work mandates change I think it's every 90 days, right. And then in terms of things like my Google and an apple, privacy, I never change.

Researcher 18:50
Okay. I've had the password you change out are primarily triggered from a work perspective that forces you to change a password from a corporate profits yeah

Participant C 19:01
that's right. So basically there's two triggers for me, one is a regular work one or a kind of security concern. Right.

Researcher 19:09
Yeah. Okay. Um, And in terms of, have you ever been a victim of a cyber attack in terms of Have you have you fallen victim to something that's caused you issue or loss or.

Participant C 19:23
Yeah, yeah, so I bought or thought I bought some, some shoes on, on Facebook, and it was a fake ad. Right, and so I foolishly trusted that that Facebook would actually like not take money from criminals. Idiots. And, and I used a because I thought I was actually transacting with what I would consider a trusted organization, I used a password that was kind of a, for me, which is kind of one of my low level go to passwords. And then I realized just after I've made the transaction that somebody came up but it's just like shit that doesn't look right because it was supposedly noisy site and then the dollars came up in the confirmation email in US dollars, I bought the cat just be done. So at that point, I cancel my credit card by, and then I changed. I went through and I changed in any site that was using that password I essentially blitz that password so that was that that became that became redundant. Okay. And it's only happened once.

Researcher 20:42
And as a result of that, as a result of that, have you changed how you, how you think about things like Facebook and those bigger sites, those sites in terms of, obviously you don't as trusted sites are there for you, you've applied left,

Participant C 20:54
I would never buy I would never buy anything on Facebook anymore. now, and I am much much more, much more careful about URL so I just double check, if I if I'm going on to any site I'm constantly checking the URLs to make sure that it looks, it looks legit. Right. Yeah. But, I mean there's certainly, the place I've got Facebook is on my phone, I don't have it on it. I don't use it on, on my computer I don't use it on my, on my iPad. So yeah, so this is the only device really that does any kind of social media. Yeah.

Researcher 21:38
Okay. And, and so in terms of has that cause you to think at all about or, you know, apply any kind of thoughts around. As far as current application like Facebook or Instagram or, or, yeah, big network, big, big, big applications with a large user base. Do you, do you think about not using them at all or are because as they're, they've got a lot of people on board therefore they're more likely to be a target for cyber attacks or not, or does that not

Participant C 22:11
so. So, I have a I mean I use Facebook in the sense that it is a useful communication tool. So you know keeping you know keeping in touch like yourself or you know I live in lots of different places. Right, yeah,

Researcher 22:27
yeah absolutely yeah all over the world. Yeah, you know,

Participant C 22:29
so there is a, there's it fulfills a function. My wife hates Facebook she thinks it's invasive she doesn't use Facebook. She uses xxxx. So it kind of is by de facto is a bit of a shared account between the two of us. But I, but, you know, I don't go beyond that function so I would never, as I say, I wouldn't, I wouldn't collect through ads on Facebook I would never

buy anything again through face, through, through the Facebook platform. Yeah, you know for me it's. And part of that is part of those security concern but part of it is also just me sending us a small message which is just that, that it's just not okay for a global platform, you know, one of the most valuable companies in the world to take money from criminals, you know, and, and do so on a absolute frequent basis. And as far as I can tell just expose their customers to high levels of risk and advice no consequences. I think it's absolutely scandalous. Yeah. And so I won't support that. Yeah, absolutely. Yeah, so I will use it on my terms, to the extent to which I can extract value, and then I have my endeavor that is to give as little value back as possible.

Researcher 24:03
Yeah. Okay. Kind of related question so how, how concerned are you about identity theft, and how do you combat that do you combat that, in terms of how your digital footprint in terms of information available, how do you do you manage that.

Participant C 24:21
So, I mean there's, I dare say my digital footprint is quite extensive. You know, on a certain age but around certain length of time and yeah. And, you know, my whole adult put really has been in the internet age. I don't, I'm aware of the things that are. I'm aware of mechanisms that are out there, try and get hints, tips, information that can lead to passwords, we talked about this earlier on, you know, I see those sorts of things I'm aware of the function I steer well clear. Yeah, I do check through things like through things like go transactions, things that have gone through in the bank where I've, on occasion, I've had what I've regarded to suspicious transactions and then just queried it. And, you know, change your passwords and all those sorts of all those sorts of things. I think in all of those cases has actually been a false alarm. And that, that banking details have never been compromised and it's like, oh, okay, so we did buy that okay got it. But, but we'd always err towards, you know overreaction. Yeah, cancel everything start again, as opposed to, you know she'll be right and just, well we'll see how this pans out. Right.

Researcher 25:55
Yeah. Yeah. So, and you mentioned obviously the phishing test that you have at work that would you say you're fairly good at spotting those type of attempts for you or as they're fairly obvious.

Participant C 26:10
I don't think I've missed one, I mean the last one we came in, I actually emailed ahead of it and said hey, looks like we've got some, we've got, we've got some sorts of people that are attacking our, our email, email accounts you better look into this is is up to me. I think I'm reasonably I'm reasonably aware, I mean, as I work in a partnership. There needs to be one partner that is ultimately responsible for the IT function. Yeah, so the head of it formally reporting to me. Yeah. So, it would be a very very bad luck if I, so maybe that's also kind of triggered additional sets of. I really copy a decade here.

Researcher 26:59
Absolutely. Yeah, okay. And as one thing I found out in terms of doing some of these is actually some people use a different credit card for online purchasing that has a lower credit limit is that something that you do or,

Participant C 27:13
no, no,

Researcher 27:15
that's not what I do either, but I just I just come up a couple of a couple of times that's quite interesting insight that I found out, so.

Participant C 27:24
Yeah, I think it's a really good idea actually. Yeah, I get that, I get that some thought. Yeah, now

Researcher 27:31
it was nice to me. Okay, I just see someone. I keep that as many airports look up virtually. Yeah, okay. Yeah. All right, and then D, what's your what's your view or do you have concerns around. I suppose it's kind of identity definitely about privacy in terms of data rights do being private and people managing your data, what's your. Do you have any concerns or concerns around that or thoughts around that,

Participant C 28:04
or, in terms of, I mean this this different levels to that question right so yeah you're talking about things like so I transact with Amazon and Amazon's got a whole bunch of information on me or Yeah, or what Google or Facebook might know about me. And I don't lose any sleep about it, to be honest with you. I kind of, I know there's a huge amount of data that is, is out there right so I would do a lot of work in telecommunications, as you know, and, you know, on phone companies aren't smart with data that, you know, I travel all over the place. If Telstra really wanted to know what all my movements are. It would be pretty easy to actually build the capability to do that, you know, I, you know, I, you know my search history, all these sorts of things, it's all it's all absolutely doable. I just have the view that I'm just not that interesting.

Researcher 29:06
You are xxxx you are.

Participant C 29:08
It's like, you know, if I was, if I was you know, Elton John, you know, I might be worried about this sort of stuff, but I'm not. And, and so it's out there, you know, I think that data is only useful in an aggregated form, or actually I'll rephrase that, it's largely useful in an aggravating form in which case it becomes anonymous, where it is personal, which means that I might get a, you know, an advert on a, you know, a banner ad or something actually relevant to me as opposed to something that's irrelevant to me. I'm actually fine with that, you know, I'm interested in sailing and music and and what uh you know I scan a lot of adverts around saying and music it's like well, fine, I think that's you know far better than, you know, a whole bunch of ones that are trying to introduce me to some very, you know, personal medical treatments, which seems to be the alternative.

Researcher 30:09
Right, yeah, yeah, yeah, fair enough. And on your devices. Do you Do you use any or does the company use or get back on me properties but do you use any antivirus type software or device applications.

Participant C 30:27
Yes, so the all of the well, PCs, yes. So we've got antivirus stuff that is that, that obviously the company uses on all the home devices. I've changed I used to have McAfee I've now

got, I think it's just the Microsoft one that I'm using on all of the other devices now. But absolutely, we use antivirus have for very, very many years. Yeah, I've always, I've always kept that up to date, and that's one of the things that I've not had no problem paying for. Yeah, okay.

Researcher 31:09
And in terms of the other devices on Wi Fi now, we're obviously, we've always talked about your phones, laptops, iPads, but what about other devices. You know, like, have things connect to the network these days so you got smartwatches you've got smart TVs you've got smart fridges you've got, you know, a whole load of stuff that's now interconnected via network, do you have concerns around, you know, does that a concerns around security threats through that. Does that affect how you treat those devices at all or how you, how you manage those or how you behave with those.

Participant C 31:44
No, no, I don't have any, any concerns around those devices I don't have very many so I don't have a smartphone, I mean my, the main devices I've got connected to the network, things like Amazon Alexa's. I've got Apple TV, I've got smart TV, printers, you know, These things, that is, uh, that each of them is kind of a physical endpoint. And I don't know of how you would. I can't conceive of a way that you would without actually having access to the property, You know hack into that advice and device and use it as a, as an entry point into, into the network and steal data now and that's maybe just naivety on my part, but I, I, it never occurred to me that those are you know big vulnerabilities are particularly it's because it's all kind of pretty mainstream stuff, you know, I've never heard of any kind of big security breaches as a result of Apple TV or, or Amazon Alexa so I just don't worry about it.

Researcher 32:57
And, okay, and then, so just generally, I, how would you say, Does your, how does your intentions or, you know, you're obviously very, very smart and understand a lot about service good How does your, how did had to what level do intentions. Regarding cybersecurity match your actions do you think,

Participant C 33:18
well that's a good question. I think the, the area where I'm where I don't follow through to the extent which is kind of ironic actually is probably the most important one is probably passwords. If I was. If I were to raise my hand of stance, one degree higher, it would be in the way that I manage passwords, you know, so for example, you know, it would not be totally out of character for me for my password to expire, and I increment a number by one. You know, that's pretty silly in the grand scheme of things, but that's not totally out of character.

Researcher 34:01
Okay. And do you think the whole COVID-19 pandemic and more people work from home has that affected how you think about cybersecurity at all.

Participant C 34:12
I think what it's what it's caused people to do, I mean I, I work in a, in a business that, obviously, you know, technology and change and all sorts of stuff, a part of it. What I find really interesting is, is how the, how some of the behaviors that we could never have. We could never have got across the line before the pandemic are accepted now. So for

example I've got clients that have set up operations in places like India and the Philippines. And, you know, the wherever we've done that, that sort of whenever there's work has been set up in those sorts of places. You know, we've had to have, you know, dedicated building with keycard access and you know segregated walls between all these people. Yeah, and now actually, you've got somebody who's processing a whole bunch of transactions from their bedroom in downtown Manila somewhere. And, and the fact that we've just recognized that that's just an inevitability and we've got to deal with it, and therefore, we've actually got to think very carefully around the security that we layer into the technology, knowing that we've got less physical role to be over the physical and the behavior. I think he's a really interesting chain so I actually think that's kind of liberating because I think that just then changes the way that, that we, it provides higher degrees of freedom than we that we might otherwise have imagined, you know, could we have thought the week of might mobilize teams that are working on an m&a transaction. You know where they're all, you know, remote working remotely. Well, previously, we'd have everybody, you know, in a war room, you know, are probably. Probably isolated, you know with specific keycard access and all sorts of things it's like well actually we can't do that anymore. And, and so we've actually got to be pragmatic and thoughtful and use technology to its fullest. I think that's I think that's a very positive outcome of, of the fact that we've been forced to solve that problem

Researcher 36:29
size, effectively what you're saying is it's actually a sidebar with it behavior change in terms of, understand that that's the way you've got to go, it's actually put more requirements on the technology to be able to support that

Participant C 36:42
hiring clients on the technology is possible, technology was always available, and was always able to do that, I don't know. But, but what it's caused people to do is actually understand what is available and to recognize that rather than just kind of going into well this is how I've always controlled things. And therefore, irrespective of the capabilities of the technology I'm going to mandate. It's actually caused people to rather be dogmatic to actually look at their look with kind of fresh eyes, and well one of the real vulnerabilities here what do we actually control what's the, what's the level of risk we're prepared to tolerate in this given circumstance, given that we, we played, continue to continue to need to operate. Yeah and I think that that's got great benefits for, for all of us in terms of being able to manage our lifestyles. Yeah. Yep,

Researcher 37:37
absolutely. Okay. I think that's, um, that's all my questions

Participant C 37:43
okay well I hope that's, I hope that's helpful I think that a lot of it was a little bit, a little bit vanilla or a little bit generic but hopefully you're building the big enough, broad enough picture that it's becomes meaningful.

Researcher 37:54
Yeah that Do you think there's any, any aspects that were missed in the, in the questions at all, or

Participant C 38:05

I think they look on a stormy person, so you know when I think about cyber security. The thing that I think about, I'm much, much more worried about what goes on on my kids computers right than I am about my. So, you know, I'm worried about it, applications that they might have downloaded. I'm worried that I mean iOS ones I can police because of all the stuff but yeah they could just download an E xe file from somewhere. And then there's something sitting on my home network. Right. and I don't know about you. Yeah. And also, you know, there's just things like, you know, I'd like to make a decision around how I'm using, how I'm using social media. But, you know, I've got two teenagers here that, you know I've got their own computers, and in COVID They're, you know, they're in different rooms with the doors closed because they're on video calls the whole time, whereas historically, we might have had all of those computers in a very kind of common space, so you know no one's kind of going off and doing something in the dark web, or, or, you know, being groomed by a pedophile. There's much more that can happen in behind closed doors now. Then, as historically been the case. But so, my concern is much more a targeted towards them, what they're doing what they might be exposed to. Because it is, it's obviously, it's obviously harder for me to police that then than it used to be

Researcher 39:54
right because presumably they'll be using the same network as you're using so therefore, does is that then the risk of that what they're doing on their devices are going to affect both a your

SPEAKERS
Researcher, Participant C

Participant C 00:00
In fronting, but you can explain it to a teenager. There are these risks, I mean we all know that your ability to assess risk. As a teenager, is terrible. You know, that's your ability to to assess risk actually matures for for girl I think it's in the early 20s For for boy it's kind of 25 Right, so they are, they're programmed to take risks, and, and those risks. You know no longer foraging for food, they're foraging for, you know, entertainment and, And you know that, you know, some sort of affirmation in in the in the web. That's that that is something that, that absolutely does concern.

Researcher 00:47
Right. Yeah. Yeah. Okay. Do you share that,

Participant C 00:53
I don't know that's covered in any of your other discussions or whether it's whether it's just the product of having teenage girls.

Researcher 01:01
No, no, I think it's been raised I think it's made, perhaps an error I need to kind of enhance I guess the questioning, around, around that, I think, because one of the things I think is actually, you may be like Heidi Do you share, share your passwords for things like Netflix and stuff like that, or,

Participant C 01:18
you know, and then well I mean only within the family. I mean, by definition, we have to do right, yes. Yeah, if you, if you know, if that is available on different devices. You have to individually log into those.

Researcher 01:33
Yeah. Yeah, absolutely. Yeah, and I said well I understand, obviously got two teenage daughters and obviously one down in the need and now so you know, but she's using the same same logins with Netflix and Disney plus I use.

Participant C 01:47
Yeah, yeah. Okay, got to that point, but I'm sure that will come. I wish you I wish you well.

Participant D

SPEAKERS
Researcher, Participant D

Participant D 00:00
All right, just doing a test again. This is a test where I'm talking to Paul. Paul can hear me but this machine can work wake up machine.

Researcher 00:25
Okay, that looks to be working. It's got a bit of delay on it, but let's see how we go.

Participant D 00:31
All right. So we go back and start again.

Researcher 00:34
I haven't so yeah, so you were saying about the different devices you use for personal work.

Participant D 00:38
I have three devices. My phone has both my personal and my business matters on it. So I use it for both. This laptop is primarily my business, but it does also hit my personal emails. I've got it set up so I can go and check them from time to time but fundamentally, it's my business. And I have a Samsung tablet for my personal emails and contacts and stuff.

Researcher 01:06
Okay, so your tablet you just use for your personal staff. Absolutely. Just your your your laptop is mainly mainly your business but you start out you do have personal emails occasionally on it. And then your phone you use for both.

Participant D 01:22
Exactly right.

Researcher 01:24
Okay. And if you have a choice of your security mechanism that you use under the Go devices, do you prefer using a password or a pin or fingerprint or facial recognition? Do you have a preference for those?

Participant D 01:39
On the phone I've got both facial recognition and fingerprints and with better password or has number as opposed to a password. So I like that that works for me. But then I know where my phone is, on my laptop, I tend to have most things are password related rather than bio security matters. Just because I'm not quite sure how to do it on my laptop. So I've just stayed with and I've got increasingly sophisticated passwords now. Some of them are 16 or 17 metres long. I can I have a system of recording them in a vault on my drive.

Researcher 02:24

Okay, so you use that you use a like a key vault system or password vault system. That's yeah, yeah.

Participant D 02:32
So I've got that. I've got that password. That was never written down. Right say I can go into biometrics for that. I haven't done that yet. But at the moment, I've got a password that I remember. It's built into my password,

Researcher 02:50
and doo doo doo. Are you concerned around having all your passwords stored in one vault or do you think that's pretty?

Participant D 02:58
I also have the backed up. Notebook. Right? My biggest problem was trying to keep the two of them synched. Yeah, because I had to remember why didn't I you can send around that.

Researcher 03:10
You can turn around that somebody could hack the vault or and get all your passwords or I am

Participant D 03:14
concerned that somebody could hack the vault or that I'm more concerned that I won't have access to it when I need it. Right. I won't be that. I mean, I've got two layers of security. One is a layer getting into my laptop and then another layer of getting into my vote. And the passwords are different. The means of getting to them are different. They're going to be pretty clever to figure that out. And I don't go into my vote very often. So you know looking for something that I've read it would be tired. You wouldn't find it very much because they've given to the board we've tended to use my notebook around the house here. It comes with me when I travelled to Hamilton or something on if I'm going to stay that night. I take my little note with me. Right it's not totally secure. It's

Researcher 04:09
if somebody if somebody if somebody broke into your car or wherever, wherever you're staying and stole your note, but would there be easier to relate to those passwords to your to what you use them for or not? When it's when they start some

Participant D 04:21
work to do. There's a there's a I don't have the name of what it is. I have a code for so people would have to go. The disarray means what? But they could go and try it. They could try something around that. So it's not totally secure and I appreciate that.

Researcher 04:46
And do you have clear separation between the types of passwords you use for work staff are at the top of passwords usually for home personal stuff, or is it just it doesn't it's just a mechanism that you use that

Participant D 04:57
or just use it and I don't have to I don't have to get married.

Researcher 05:00

Okay. All right. Good. Thank you.

Participant D 05:04
So you've already said you use your laptop

Researcher 05:05
primarily for business. I use it for personal emails. D use it for other stuff like online banking or social media or online shopping and

Participant D 05:15
don't use it for social media. Because I don't belong to any social media. I do use it for online shopping. And I do use it for online banking. So I use the phone and laptop for my banking and I use PayPal as my means of paying. So I very rarely use credit card directly with a supplier from supermarket which doesn't accept paper groceries online. It's the only one credit card is actually actually interviewed by credit card directly into a secure site and trust them. Why is that trust paid now

Researcher 06:11
I do social media but you do. And obviously your you say even though your laptop is your work laptop, it's your business. So it's not it's not it's not a it's not connected to any other company or corporate or anything like that. That's got access to it. No,

Participant D 06:25
I don't have a living connected to my wife's laptop. She has her own business. She's just over there. Right? And she has a business like, right. I have my business here. And we just run them on our laptops. We save everything to the cloud. So the cloud, our laptop is our backup. And our cloud is our main storage, storage and most of all my files and I come down to my laptop every week, just in case something and I can't get it all weekend.

Researcher 06:57
But you had both you're both you say you're both using separate devices but I guess you're using the same network and they in the house. Are you on the same

Participant D 07:05
network? Yes, we have fibre we installed fibre fibre system and he Anelka.

Researcher 07:13
We both use the same same cloud storage mechanism or

Participant D 07:18
she has her own cloud storage and I have my own cloud storage. I have a personal cloud storage and I have a business cloud storage, two accounts

Researcher 07:28
and when you get that and maybe when you get visitors or children coming round or you know people come around or whatever do they do they also use the Wi Fi your Wi Fi network.

Participant D 07:38
They use my Wi Fi network Do

Researcher 07:40
do you have concerns around that in terms of them giving out passwords to their friends or them getting access to?

Participant D 07:50
So I don't have you ever thought about it to be honest. So I don't have any problems with people accessing it. Not just anybody using it. Particularly we have an unlimited data chip. So it's not as long as I'm told they can't access my laptop. I'm told that assurance I have seen is you can use

Researcher 08:17
and when is when you bought say you said you mainly use PayPal for for stuff you buy over when you when you use a credit card Do do you have? Some people have a specific like low value credit card they use for online stuff? Do you have that or do you just use it you're single you're saying

Participant D 08:33
just use I've got a business credit card and a personal credit card branch chain and I share the personal credit card and my business credit card and both of those sit in Paypal and I write Comelec to pay pal which when they've got differences or that they've got their locations. Groceries go to the personal one. Fish coast and I've seen we've got HelloFresh that comes through Pay Pal right darling Oh countdown lesson go home. I just said every time

Researcher 09:08
okay, the only using Pay Pal. Do you do you have any concerns about them them getting hacked or getting access? To your

Participant D 09:16
they've been hacked in the past? know we've had a talk to the guy PC hardware do my security to the same antivirus software and look after my IT company in Hamilton and they told me that a pal was secure. So I believe in the business.

Researcher 09:42
That's fine. And when when you say when your work so when in your work when you're working with a client and you you basically maybe you go to a client's premises and you you you you connect your laptop to the network and use that network do you then do you then do you then do work stuff over that laptop only or do you do would you then use that laptop to do I don't know online banking or or online shopping?

Participant D 10:13
And this things I'll do when I'm working when I'm in my clients office. Yeah, I need things I'll do is to access my cloud storage because that's where the files okay and I'll be needing to work with don't then say oh look, I just want to transfer some money. Yeah, I'll do that myself. And if I need to sync my phone too, so I do use my phone as a mobile hotspot. It was something that they've taught me how to do. Yeah, I can do that. Right. There is one exception. There's a company down here called xxxxxxxx, and I know that two dudes who seated up really well, they're younger versions of me. And they have asked me to mentor some of the people. So I spent time in their office so my mom the network, and I have occasionally use the network because I'm sitting there for three or four hours sometimes

working with these guys to do something personal. So I have made that exception to my rule about never using a client.

Researcher 11:25
And that exception is based on the fact that you know them and you trust them. And it's a trusted relationship and

Participant D 11:31
they have a good rest of it. Yeah, so they are people that I've known and our relationship as well. Sort of intimately aware of the business. So they share a lot with me. I don't share much about my business for them because I'm basically I'm retiring down here and just seem to click a few times and a few more come and I use this company because they bite me with the big red vest syndrome if something happens to me, got project managers and development managers and others really available to step into the breach. I use these services to help with my projects. And now I'm actually mentoring the development managers to do this sort of stuff.

Researcher 12:30
Alright, thank you. And similar question. VF phone or your laptop or your your tablet. What do you what do you use that in a I don't know when I say went to a cafe and you wanted to to use our Wi Fi in a cafe or you went to an airport lounge or like public environment public Wi Fi stuff would you use? What do you use your your devices over that network? And would you have restrictions on what activities you did over

Participant D 13:04
those networks? Do you use them over those networks? And no, I don't have any restrictions. I will use them to certainly access my account, my Cloud account. I've used them to access my bank accounts, transferred money and stuff. I just haven't thought about it so I use them just as nervous as if you're opening so I go into a cafe and I will exist you xxxx sneaking in and out of my office.

Researcher 13:49
Okay, so you will so if you go to a cafe or go to I don't know whether you're staying away from staying away down in I don't know where you're wherever. And you've got a department Wi Fi you do you'd log into the Wi Fi and you do all

Participant D 14:03
the Wi Fi No I've never thought about that as a security risk. So yes, I just logged in the evening. I'm staying and normally it's in the house like motels Max. I normally rent a house of some sort for a couple of nights. You know one of those Airbnb and I won't go into the internet. I will use their internet for things I need to do at home.

Researcher 14:32
And you would you've not thought about any concerns around

Participant D 14:37
that you're raising them

14:41
as part as part of this study okay

Participant D 14:53
and you've talked you've

Researcher 14:53
talked about the fact that you have different you have a you have a system for doing your passwords. Do you apply that? Do you apply consistently or do you have like some people have like, they have much more complicated passwords for their banking for example, do you have do you have a much more complicated stuff like some that you classify as being much more much more important or do you apply them the the the methodology you've got

Participant D 15:16
generally apply that the only difference will be where if it's something that I just access for information like I access a a colour quality or quantity survey site to be able to keep records of what's playing. And I put a simple password for that, right? I'm changing that Prentice and now everything gets the same password or the same type of password that my banks get, which is generally at least 10 characters, and it doesn't have any just has no that's fine. Doesn't make any sense at all, on all sorts of characters. So I'm moving that way. But some of them I know just really simple old passwords because I've not bothered

Researcher 16:14
not being bothered by it. And do you do do you do change passwords often?

Participant D 16:19
Change my bank password every three months. So that gets updated every three months? Yeah. Alarm that goes off the calendar just helps me and within a week or so all updated everything. And that includes any sites where I'm making money, right? They all change, but they are all changed differently. I don't know like, I might have one password or two. Banks. And that'll be the extent of a password meeting or than who thinks I'll use it. I've got a second tier of security like my banks. I can go into it, but then they have to call back to try and to get me into the site. Right when I've got that I might use the same house.

Researcher 17:12
But you say you only trigger is Yeah, got it. So what triggered you to change the password is basically an alarm set every three months to change your banking, passwords and anything to do with payments that you make

Participant D 17:22
as well. Okay. Yes. Okay. That's gonna be doing for years so have you ever

Researcher 17:32
been Have you ever been the victim of a cyber attack? Have You Ever Have you ever

Participant D 17:37
have that's been so we've had somebody said access to my credit but the first time the first incident somebody accessed by a ASB account. This is going back. Probably what taught me how to be a bit more secure than some but not as secure as I should be obviously listening to access my ASB account and took money transferred money, but I had a $2,000 maximum $2,000 So they took 1999 and that triggered an alarm in ASB in suspicious payment xxx is this you and but they let payment go. Or they had to go through

a ASBs security stuff. And somebody had accessed our bank account through by viewpoint case, as a party to the ASB. She had access to it because of things she had that she belonged to somewhere. I can't remember exactly how it happened. But that was the first incident.

Researcher 18:50
So what So what caused what caused that that what was the cause of that

Participant D 18:55
I used to do you didn't change your passwords? I thought she was changing her passwords, but she did. Right. And they hacked your computer right and got the password to the ASB account. And hacked the ASB account and transferred money to a rotorua account of ASB as it happened and went from the ASB account in rotorua and disappeared because we got on to because it was an odd number and the ASB called us they gave us that money back. We didn't really say anything to kind of tune it. But at taught listens about not being so blase about it, but that was he's been gone for 16 So to be five years before Yeah. Told me to be a bit more. And since then, I've had my Visa card. Stolen, we were in South Africa, and we used our Visa card and the trader obviously just installed the betta can details. We had left the BNZ with instructions that only thing odd. We told them where we were going so they knew where we were going. And they got ahold of us and they got some money because we had set that in place before we left the set money back and I don't know what happened. It was in theatres and just recently transaction that occurred in Holland and we have no idea how that could in Holland. A bought something for about $3,000 We don't know what they've done, please it doesn't know what they've done. They think it was just one of those big computers that just randomly going around and trying to match up because we haven't had any incidents of attack or at least none that we know and that they cancelled our Visa cards, gave us our money back and we're off again. And it only happened three months ago.

Researcher 21:15
And when you when you when you say you you said your office went away on holiday and you you told the bank before you you went to display of any suspicious Is that something you do whenever you you travel because that's something

Participant D 21:30
that's we travelled quite a bit. Yeah. But it was one of the things when we got one card for travel travelling we put currency euros at something on a one card and the BNZ had sent us down and said Tell us what you're doing. Okay. And they did that was such a long time ago, and 10 years ago. They sat us down whenever when code first came out. They said they sat us down and told us that we followed that magnificence. That being said, because it's mainly the BNZ Academy ASB Is My Business account. BNZ it's my personal account. So we were travelling at all going through the BNC piece, okay. We told them what our itinerary was and if anything came up. Look, don't get in touch with us.

Researcher 22:25
And like the you know, the phishing attempts where they're they're trying to get you to click on links or whatever or D D D Have you ever had been subjected to that or have you ever do you find those easy to spot or

Participant D 22:41

found an easy to spot so far? We've not been we've not been caught out. A they come in through my trunk. So read I drop them into the trunk and go through them all the time. And they're still there arriving in I don't see them till I go and look at every now and then. When will come up on the computer. They're quite easy to spot. It is easy to spot when it comes through on my phone. Right? So about half an hour ago. I got a phone call from a number that looked like it was coming from the Hawks base and we deleted it there and it seemed to me that it was visa it was an automated message saying visa security and there's been two payments on your Visa card. And you know push one was the reorg go or push to to say the not just read have been reported and deleted. Right? I know what these are like when they come through to me they talk to me guess I'll go on the website because all other stuff that has to happen before anything. None of its over the phone that just came through on my phone so my phones obviously and other people have got and I have another one that was with my ISP account came through and I actually reported a TSP account. And it was an email that came through. It said that I needed to update my tech certificate because there was something in Oregon here. That looked really really good, really professional but the fact that I've asked it didn't say I called please log in here and just said please log in here and gave me a link. And that was one of the things that were important there as being able to pick from those emails. So those two scams are the ones that have been over the last three, four weeks. that I thought were very, very well done. Really good.

Researcher 25:04
thing more sophisticated.

Participant D 25:08
More more sophisticated all the time. I'm sure we will as I get older and slower cilia gonna do something stupid.

Researcher 25:18
Exactly. And you can turn Do you have any concerns around identity theft at all?

Participant D 25:25
No, I don't. I have a very good friend Robert. Is he's into this it stuff and he told me about it all the time. But I don't know because I don't quite understand how they do it or what they do about it. I haven't had the experience of it. So I'm not too concerned about

Researcher 25:43
now. Well I used it obviously early on. He said he didn't have a social you don't use social media. So therefore perhaps they have less information available on the

Participant D 25:51
on the networks and for others maybe I do have a Facebook account that you will have to be very, very clear proposed to me. Okay, it's it's got a Gmail email address Yeah. Is one I use when I'm overseas, I can make things on Gmail for my family. No, it's me. CNN it was me.

Researcher 26:26
So do you like to I guess because you're not concerned about identity theft, but the the do you deliberately do stuff to prevent that or

Participant D 26:39

not doing anything particular ability. I mean, I do have things like my passport and my licence in my vault, because I need them sometimes. dual identity stuff that I have to do, but stays here because I think that secure airport worried about people stealing. And

Researcher 27:07
so, in a work in the work context, in companies you may work from the past or clients that you work for Have you ever received any any cybersecurity training or, or be any cybersecurity guidelines as to what you can and can't

Participant D 27:25
do? Not really this nervous no not that I can remember anything like that. To you. One other thing that has happened is somebody sent me an email that looked like an account of who I know really well. Asking me to buy at all the iPad things as you know, I Spy this and I'll pay you back when I see. But I kind of wonder what he wanted it for. So I phoned up and it wasn't him. Somebody had hacked his email, sent me a request, apparently. So I got hold of particularly for PC hardware, and they said to me, oh, yeah, those CAD will they want us to number and they can cache it. So they just wanted you to go and buy something read them the numbers and they'd be gone. You've never seen them again. So that happened about but in terms of training from everybody, No, I've not received anything in terms of guidance or what they can and can't do. from anybody.

Researcher 28:47
And and from any service obviously weren't any organisations or whatever in terms of what you know, obviously you talked about one card beings and and one card or any other

Participant D 28:56
PNC Bank. Yeah, they do. They simply do. We have been they they sort of told me about what I can and can't do on my computer and what sites I'm allowed to and all the sites of integration. They just said you know, those videos are really easy to hit. I did know years ago I used to watch videos in Europe, because that's where the OECD for putting up building videos. And, you know, you'd be watching new building technology. And Paul said, you know, we're really struggling to keep our level of security when you're watching videos coming out of Europe because people just attach anything to a video. It's easy. Really. Okay. I've stopped. I don't do that anymore. Interesting. Interesting. So yes, those two those two organisations are the only two that I can think of given me any specific training or guidance.

Researcher 30:02
And no, no, no, no. No guidance or rules on clients are going to work for where you go to work for client and they give you access to the network and they they say like you must do this or

Participant D 30:11
I was repossessed. With a it's mostly but yes. Actually, in relation I mean, they just sort of gave them to me and I don't even remember what it was some from history and my current clients now.

Researcher 30:30
Antivirus software, do you use that on your devices at all?

Participant D 30:34

I do. On my phone. I've got whatever Samsung's standards. All of them are loaded. On my laptop in my blood. I have a sector non 32 by standard software. So that's the mail and work. And I also have Microsoft something which I can't remember what it is. It's a standard Microsoft, which Paul PC had we told me to have that as well. The to work okay. Don't let anything else because the non theory too often will particularly in McAfee, he said get rid of all that. It's just rubbish. And contradicts it doesn't gel. I'm gonna do stuff with you. So that's what I just did not 30 to get the standard that they told me to put on white paper on themselves actually. Okay, all right.

Researcher 31:47
What about other? What about other devices that you use, like other devices in our house that are more to the Internet things where a number of devices are talking to other devices? Do you? Do you have concerns about that? You know, I don't know smartwatches or I don't know. TV like a smart TV or whatever, that are all connected the network. Do you have concerns around? And that from a cybersecurity perspective?

Participant D 32:11
A television connected with we don't watch television, we just watch Netflix on it. I haven't gotten any concerns about that. I've got no concerns about my watch people I thought well watch was just connected to the phone. That's all it is. Right? Just okay.

Researcher 32:31
Any other devices are they there are kind of you'd say would be networked and therefore might be a a point where somebody could get get access to your

Participant D 32:38
house or stuff like that think of there's just xxxx's laptop and she has exactly the same software by him. He said she goes through PCI, everything's done through the laptops. Good document. I have a Microsoft account. So all our stuff comes through Microsoft programmes. We don't have anything else that I can think of. We do as much if anything comes up on LinkedIn open, I can't think of anything else.

Researcher 33:24
And that's fine. And in terms of in terms of apps that you use, I various apps I use on online on your phone or whatever do you you do have an approach that differentiates those based on size and size and popularity? I do think that because lots of lots of lots of users and lots of big and well known brands are likely to be more susceptible to a cybersecurity attack or don't you think consider that at all you just use the apps when you need them mostly. And obviously in a in a COVID pandemic over the last couple of years. A lot of us have you know because for Your love has finished working from home a lot more a lot more and have to work from home and work online. How has that has that changed the way you've approached cybersecurity? Has that kind of triggered you to do things differently

Participant D 34:16
or really, we do and I don't really have an office city right now. But it hasn't prompted me to have more layers of security or to have different attitudes to going into someone's office or to I don't think I've changed my cybersecurity working from home

Researcher 34:48
not because you think it was between to be good before and that was that.

Participant D 34:53
It seems to have been working for me in the past. PC had seem to be keeping up with things. You do have an office we use over and Hamilton we've set up so what really own the building and we've set it up in ourselves that we use one day a week 10 and I we've got our data, that it's all quite separate. It's it's got its own Wi Fi and just go in there as if we were Republic building and gone to the Wi Fi. We can come away again. We've got no security. No, a PC had visited not for us but no particular issues with it. It's all just quite straightforward. Okay.

Researcher 35:49
Okay, I think that was all my questions. Is there anything else that you think is kind of relevant to this topic that I've not not covered? Or

Participant D 35:59
be of interest? Really? Yes. I mean, cyber security to me now identity threats I hadn't really thought about cyber security to me is having people mostly around money somewhere, getting some money from you in some way. And that's probably where I focused most of my attention. Yes, the data. The data hasn't been, you know, like somebody accessing my data and locking it off, telling me they were brilliant, quit locking it. A number of people experienced that. And one or two of them have been people that I've been associated with it or not because I can't do any work and accounting payment Rotorua has been through the roof to a client of mine as I work but it's never you know, I've never been subjected to portable hardware tell me that level of security I've got on my computer should be sufficient safeguard against somebody will do that to you. That shouldn't be hurting you. long as you don't do something stupid. Like gremlins. Don't let them in your house. You have to invite them that yes. So just that's so other than that, I can't think of anything that you would need to know about our cyber security here. To do one thing that did. I was just talking about it. xxxx and I have different views. xxxx has her own bank accounts as she's my wife. She has her own bank accounts and I know her own bank accounts seem to be still more vulnerable. She just kind of do the same things I do around the joint accounts. She'll do that for me. I'm happy that our joint accounts do vary a little bit. I just wondered if there's an avenue through there. People could use to get into our system and thought about I've always been my mind to it. Maybe the sort of vulnerability around people.

Researcher 38:38
Maybe I don't know I Yeah. Yeah, that's interesting. Actually. I'll have a think about that one. Yeah, that's an interesting. It's an interesting question because I've thought about it in the context of like, people working from home so you know, in a family like you know, the mum, the mum and dad are working from home, but also the kids are at home, and they're all using the same network and they're all trying to do their work or whatever. And they've all got their devices. And yeah, there's obviously that increases security when it vendor abilities for a corporate for example, if particularly if maybe people in the same family were for similar industries or competing industries. I hadn't thought about it in the context of Bank. Bank staff are different different people apply different different security mechanisms to get to where they are, they'll post security I hadn't thought about it in terms of whether that would be an increased risks for you or not.

Participant D 39:26

I hadn't really. I mean, I was sick term steak account. If I had a joint bank account with a chain and I go and change my password every three months and then I go and do all that. And xxxx doesn't. That means they've got no access to my account and through that they might have access to more than my account. Right and I don't know what else they would the work could start in all sorts of directions. Yeah, I do have a chapter about how often do you upgrade your passwords? Good question. She doesn't do a very good question. Okay. Never did. To me, go ahead. She didn't become better. Okay, no, but I can't think of that you would need to know that. I'm happy for you to give me a

Researcher 40:14
call back or when I say I would like to obviously I'm doing I'm obviously doing a few things and then I can consolidate results and actually go through them and pull out some insights. But if I've got follow up questions, if that's alright, if I can get back to you that that would be appreciated.

Participant D 40:26
Yeah, absolutely. No problem. Great. Awesome. I just

Researcher 40:31
stopped the recording. Now. Hang on, just bear with me.

Participant E

SPEAKERS
Researcher, Participant E

Researcher 00:01
Just testing to see whether this works. Can you say something? Something Excellent. Good. Seems to be working it seems to be working.

Participant E 00:13
Oh good, good.

Researcher 00:16
Okay. So the first the first questions are just around I guess devices that you use and etc. So, you do do you have separate like work and home computers or laptops and similarly Do you have separate mobile devices do you have different one for work or for for personal use? Or not?

Participant E 00:36
Okay, so I have separate work and home laptops, but I only have one mobile device and that's my personal one. I don't have a work device at all with mobile.

Researcher 00:47
Okay. And in terms of your in terms of your devices you know, what's your do? Do you have a preferred security mechanism on your devices, you know, do you use passwords or PIN or fingerprint or face recognition or,

Participant E 01:05
I use whatever is available on the device. So on my home device, fingerprint recognition, so that's that one on the work device. It's basically it's user ID password is they set up on the mobile it's face recognition. All the biometrics where I can I prefer that right easier, but the work on is not set up for biometrics,

Researcher 01:30
so the work one is determined is determined by obviously the organization you work for in terms of the policy they use.

Yep.

Okay. So for your work device, and you don't you don't have a work phone, you have personal phone. That's right, isn't it?

Yeah.

For your work computer. Do you just use that purely for work use

Participant E 01:49
Yes.

Researcher 01:51
Do you Do you do any personal stuff on it or home stuff on it?

Participant E 01:57
Very occasionally, I will browse the news or a particular website, but then again, that's what I can get to as determined by the work policies as well. So but I don't do any, I guess, home based or home total personal type of work as such. So it's just something I might occasionally see around browser. Like this morning I browse the AT website, which was more related to my personal thing rather than the official stuff rather than work, but that's about the extent of it.

Researcher 02:34
Right? Okay. So you wouldn't do any kind of social media on your work computer?

Participant E 02:40
Nope. Anyway, you can't anyway. I wouldn't. I wouldn't either.

Researcher 02:46
Okay, so it's restricted in terms of that. There's quite a lot of restrictions on okay.

Yes. Yeah.

And you wouldn't do any. You wouldn't do any kind of banking or shopping online shopping or

Participant E 03:05
I wouldn't say never. But theory of the very rare most of my banking I do mobile or on my personal laptop reconciliations on personal laptop but individual stuff will be on the mobile. Occasionally, if I'm thinking about shopping, I might just do that on my work computer but again, most of it I'm probably doing on my on my mobile if I'm doing any sort of shopping into phone need a sort of bigger screen than I'll use my personal laptop.

Researcher 03:36
Right. Okay. And in terms of when you may use your work laptop for for doing the occasional personal thing, is that would that generally in your home environment, so, you know, working from home or would that be at work or

it could be it could be either,

you don't differentiate in terms of where you're located in terms of how you're using it. Okay, all right, good. Okay. Thank you.

Participant E 04:03
Um, now, just so that you know, I'm actually now on my home laptop for this for this particular call. So yeah, I've decided that I'd actually do it on my home laptop rather than go through the rigmarole of actually attending a Zoom meeting on a work laptop.

Researcher 04:21
Yes, I'm guessing I'm guessing it's all I find that so corporate corporate world it's all teams. Teams basis. Yeah, yeah. Yeah. And corresponding, I suppose Do you do you do Do you ever do any work activities on your, your personal laptop or computer?

Never.

Okay. And I guess what about on the mobile phone?

Participant E 04:46
So occasionally get messages work related messages on my mobile, but that's about the extent of it. There's no no actual work as such.

Researcher 04:55
You don't do Yeah, you don't do like things like teams or or Outlook access on your phone or no,

Participant E 05:01
that's that they should. Occasionally I'll do a team's meeting. So join as a guest and a with a password, not that sort of thing. I'll only do that if I actually happen to be out and about at the time going, going to or from a either a personal doctor's appointment or something like that. So I can generally be in the car formula seems.

Researcher 05:26
Yeah, yeah. Okay. And so you know, what do you work on your personal laptop but you'd never use you would never use your personal laptop. To access over work network, for example, you you completely separate?

Participant E 05:49
No. I mean, there's a possibility that you can do organizational layers, but there's not one that I choose

Researcher 05:57
to your personal your personal laptop is purely for personal stuff and you don't you like and so when you're when you're out and about maybe you're away at a hotel or you're in a cafe that's got Wi Fi or in the airport, that's got Wi Fi do you do then use you either your laptop or your personal laptop or your mobile and do you use it over there now the Wi Fi networks in those scenarios?

Participant E 06:26
No, I used to but now I've been I've got basically unlimited data on my mobile so you always use my mobile device I don't use public networks.

Researcher 06:38
Right? Okay. So you never use public networks for for any of your your personal laptop or your work laptop or your or your mobile.

No

Okay, so would you if you need to do work stuff would you then would you then Pair it with your personal phone? And use the data on your personal phone or

Participant E 06:57
very occasionally, but like generally, again, it generally won't be doing work stuff in a public environment. Right. So I've got a hotel here that there may be I'll connect to my personal

mobile been but that's if I'm away. Otherwise, I'll actually probably go into work and work or I'm actually actually out of out of the work environment, I tend to switch switch off

Researcher 07:26
and so say you use say you don't use public Wi Fi in hotels, airports, cafes, whatever. Is that because you've got you've got unlimited data on your phone, or is it because you've got security concerns around using them? Or is it

Participant E 07:43
a bit of both? Obviously, I've got unlimited data don't worry about that as much about security concerns. But from a I guess, from a public network perspective, I would have to think about the you know, the security concerns if I was to use it, I mean, you know the hotel for example, I'd be a bit less concerned about using their Wi Fi. Given that, you know they need to cater to the corporate, corporate traveler as well. But certainly at a cafe or on the ferry as a good example, I wouldn't be using the Wi Fi it all for work purposes. I wouldn't use it for personal either. Okay. It's more around security.

Researcher 08:33
Okay. So, but you might use the hotel for work for example purposes because you'd regard a hotel is more when you've got it as more trustworthy or because it needs to cater for that sort of scenario or

Participant E 08:48
bit of both I'd regard it as more trustworthy because they need to cater for that particular scenario. Yeah.

Researcher 08:56
Is there would you limit is there any limitations you put on your on your activity? If you were you know, the sounds like you don't use a DD but but if you were using public Wi Fi would you be would there be some activities you would never do on on public Wi Fi for example?

Participant E 09:09
Yeah, I've never really thought about

Researcher 09:12
that. Okay. Yeah. Yeah, that's right. Okay. And so, and I don't don't really do to share any information that's, that's, you know, private. But do you how do you think about security Do you Do you have different mechanisms of security for different types of activities that you do either personal work or how do you you know, do you have you know, for example, do you have different you know, for your banking Do you have different, you do are you much more, you know, in terms of how you secure that D Do you think think more about that, or then than saying other things or?

Participant E 10:00
Not really. I mean, I guess, for example, with banking, yeah, the security that they put up in terms of two factor authentication, and that sort of thing actually gives me a lot more comfort that what I'm doing is secure. But I mean, to be fair, I do rely on the, I guess the installed security software on my laptop anyway. Regardless of what I'm doing

Researcher 10:32

on your personal laptop, or your work laptop

Participant E 10:35
personal laptop, personal laptop, yeah.

Researcher 10:38
When I say you didn't need to install security, do you mean the password management apps or stuff like that or

Participant E 10:46
my password management apps in my head. Okay. Yeah, that's for the virus virus protection. firewall software, which is, to large extent integrated within the Windows environment. So

Researcher 11:06
yeah, okay. Okay, so you don't you don't think about having more so you basically rely on I guess your banking I suppose. You rely on the the mechanisms provided by the bank, for example. What about things like when you're buying stuff on your phone, you know, do you do apply different level of thinking about security when you're doing online shopping for example, or do you know

Participant E 11:29
Yeah, look, I only shop on what I consider to be trusted and well known. Sites. Right gun shop. What would you yeah so like, I've been on things like wiggle is a good example where I've established a relationship I regularly shop, the good lots of stuff back never had any problems, those types of things. So, you know, I trust that particular website. If it's a new, a new site, I'm sort of thinking well, what's the you know, what's the global reputation of it? Do they actually have a global reputation? You know, things like Amazon and mark on my phone Yeah. myself one of these other sites that I do, actually, you know, I've been I've got a series of sites and I've gotten kind of, to ally Express. It's an interesting one on sort of, a bit dubious sometimes about about that. But again, if you're shopping through a through a site like AliExpress, or Amazon, then they've got a reputation to protect as well. Yeah, so I mean, I've only got a few that I've actually will generally shop through and what I do with one pepsin Hey, it's a new site, a new site visitor. First of all, is a base base in New Zealand. Yeah, that's a good good indication. So I'll research the you know the address the physical address. Find out a bit more about them. So don't do a little research on the FICO. I did some, some shopping on for some hardware, basically, joinery hardware. Yeah. It's not something I do very often I didn't go to your room that might have been or the bunnings which got a good reputation that we taught us. Like there was a New Zealand hardware, which I'd never dealt with before. And I thought, well, we'll test them out. They're obviously you know, they are they're a New Plymouth. That's research on the site, tested them out. Made a smaller purchase first. came through, establish that level of trust. Now, I've sort of gone to them a few times for various things.

Researcher 13:52
And that is that is done either on your personal laptop or your on your personal mobile phone.

Participant E 13:58
Yeah, yeah, totally on the X amount of weeks could be one particular case of the either because they don't have any, they just have a website.

Researcher 14:06
And do you just not correct on the Nano. And do you have do you do you have any special like say I know some some people that have a special you know, low balance or low low limit, like debit or credit card that they use online different to the normal credit card, or do you do just use?

Participant E 14:26
Yeah, yes, it's a standard one. Okay. Having said that has once been compromised, and I don't know I still don't know how but it has been compromised. So. Okay, well, it was picked up by the by the being very quickly.

Researcher 14:41
Alright, we'll talk about that in a minute. And we'll get to that. In terms of where you work, because you obviously you said earlier he or she preferences to use biometrics either face recognition or fingerprint, where you have password to where you're required to use passwords or where you've got passwords online or whatever. How often do you do change? Do you think about unchanged and then we'll change them how

Participant E 15:02
I regularly change the password once a month. irrespective actually personal or work

Researcher 15:09
or work. Okay. Yeah. Okay, and do you you said your password management is in your head so you don't use any kind of password management apps like Apple keychain or stuff like that, or you know, those type of okay, any reason why or

Participant E 15:24
I'm not familiar with them and have a trust thing is that you put in your password and an app has it? How secure is it my head is reasonably secure.

Researcher 15:36
Yes, indeed. Okay. Okay. Are you talking about the Oh, you? You tired of being compromised? So, general question and has not just that but are there other that example or other examples where you've been subjected to, I guess I a cybersecurity attack, or is that is that the only one or

Participant E 16:00
So yeah, that credit card was compromised? That was the only one where it's actually where it's actually been. A real situation where it has been compromised. I still don't know how it was. But the I've been subjected to phishing attacks, both mobile email text

Researcher 16:24
subject to phishing attacks that you've but you've not, you've not been, you've not been sucked into them. You've actually seen them and it's sufficient time.

Participant E 16:32
Don't believe I have? Yeah.

Researcher 16:38

Yeah. How easy that they are spot from your perspective. Do you just how do you go, how do you how do you go actually, well, that's a phishing attack to you just the mechanisms for that

Participant E 16:47
to be fair, I mean, I don't click on any link links in an email that I've that I'm not expecting or familiar with. Obviously, I've clicked on the link and your your, your invitation because it's, you know, we spoke about it and it's expect to get that's okay. Yeah. But yeah, look at there's something which I'm not expecting then definitely won't click on it. I've actually had situations where I've had what have been legitimate emails with a look at them and not clicked on them because I thought hey, that's this just doesn't seem quite right. And they've gone back through various other channels to contact Southern Cross, an example. sent me an email with a link which. And I thought, well, that's unusual. Yeah. You're particularly asking, asking for the central lecture into your your login details. That's that's a big no, no, and the banking world surprise an insurance company will do that.

Researcher 17:53
Yes, indeed. Yeah. Yeah. Okay. Yeah.

Participant E 17:57
It actually turned out to be legitimate, which was like a bit of a serve on that one.

Researcher 18:02
Yeah. Okay. So yep. So you say aside from your credit card being compromised and you don't know Do you don't no idea how that happened. You've not had any not suffered any losses or any any ransomware attacks or stuff like that, or okay. How, how concerned are you around? Identity theft, you know, and harvesting of like personal information to steal identities and stuff like that.

Participant E 18:31
It does does play on my mind a little bit a bit of a concern not not so much from me, but around some of the some of the subtle ways people will actually have this information. Which I see other people falling for and lots of people falling for the older choose the song from the decade that you were born type of thing. Yes, yeah. Yeah, those types of things. We think, hang on a minute. If there's enough of those, I can actually build up quite a bit of a profile of you without actually knowing what's actually happening. And I see people falling for that it's fine it's fine even though you want them okay.

Researcher 19:20
But you so how can you say you're fairly Teddy you fairly concerned about that and as we find that easy to spot on social media, so you don't

Participant E 19:27
necessarily you don't respond? I just don't respond to that at all.

Researcher 19:32
Okay, and a fairly secure in terms of how you share your social media or terms of how you, you know,

Participant E 19:39

lockdown tiny people that I accept as friends. So I've got a very limited range of friends on social media. In fact, I use social fury limit limited in my use of social media to be fair. It's a think, I think about Facebook as an example. I'd say that's quite a good mechanism for sharing information that you'd like to share with your friends. And that sort of thing. But so clogged up with ads, that actually, and things we're talking about aren't are of no interest, that you actually miss a lot of what you'd like to say and becomes becomes useless to be fair. Then there's apps like Strava, which I think is that social media is actually an exercise as well what does that but it's a very, very specific purpose, and it's not clogged up with ads and yes, yeah. Yeah. Which I'm a lot of a lot more comfortable with, but you also think well, you know, all these who are these people following me or want to follow me and you know, do I know that?

Researcher 20:47
Yes, yeah. Yeah. And so and you said earlier, you don't you don't? You don't use social media on your work computer at all. So your social media activity will be on your personal computer or your phone generally,

Participant E 21:04
generally on the mobile actually. Very seldom actually go to the social media side of my personal computer

Researcher 21:09
and your phone is generally it's using mobile data. It's not put onto any network. You don't use

Participant E 21:16
my personal Wi Fi at home when I'm not

Researcher 21:20
okay, and you would know you know, when you go to work, you don't you don't you don't log on to a work Wi Fi for your on your personal phone. Okay.

Participant E 21:29
Okay.

Researcher 21:31
And you know, in your in your in your work roles or previous work roles, is there. Have you received any? Do you have to do any cybersecurity training or do you have to do any stuff?

Participant E 21:44
Yeah, we, we do cybersecurity training. We've got some compulsory training that we do. And we're also tested every now and then. So a fake phishing email, we see it every now and then just to see if we're onto it, see if we can spot it. We're basically over it because we have certainly within our work, we have a few receiver receive a phishing email because sometimes they will slip through the cracks, then you're expected to report it is very easily various mechanism for doing that. And so they'll send us those just to test to see whether we can actually see them and see them. So yeah, definitely lots of training and lots of lots of, I guess, informal news, Internal news coverage of phishing attacks and that sort of thing as well.

Researcher 22:38
Yeah. Okay. And what about so obviously, that's for working right, but is there any is there any, I guess, any organizations or any, any deal, let's talk about personal use, is there any how how do you is there any, not training so much, but any, any, I guess, informed information, information or whatever that comes from organizations. When like you because all we're assuming your work, cybersecurity training is focused on work and protecting the company's data that you work for.

Participant E 23:13
It's also predicting customers as well. Yeah. Okay. Yes. That's part of both. Yeah. I do know that every now and then when I'm logging. I mean, I'm still baking with bean seeds, which I'm no longer working for. Though, every now and then in the in the mobile app, they'll send you a message saying, hey, look, there's been an increase in phishing attacks and give you a bit about how to spot them and all that sort of stuff. So there is actually that education, I guess piece within from from them. I have obviously, I can't recall whether I have seen emails. But there's always the reminder as to the banking and banking sector we will never see do emails asking you you should turn your log on. So we're seeing your LinkedIn last logon details. We've always wanted to go to the go to the main website. So there's always that yeah, there was some of that education, particularly from from the banks. Yeah. Yeah. I'm really seen it from other side

Researcher 24:20
to be to be fair. Okay, that's gonna ask is just just the banks as far as anybody else know,

Participant E 24:27
that I can recall.

Researcher 24:29
And what about privacy, dear privacy training at work as well or for more relaxed

Participant E 24:36
and that's a good investment more around focused around our customers, making sure that we have keep our customers information, private classification of information that type of thing.

Researcher 24:47
And with you know, with with with COVID and obviously you know, a lot a lot you know, a lot more people working from home I see me work from home more than you used to do before COVID.

Participant E 24:57
Before go very rarely.

Researcher 25:00
How has that how has that changed about how you either think about cybersecurity or how you how you act about cybersecurity from a from either a personal perspective and or a work perspective.

Participant E 25:14
Probably has changed a lot because I was very aware beforehand. So like, just the one the one thing that's probably changed is more around how we log on into the work so that

was secure. IX fitfully a secure VPN. Yeah, it's sort of hasn't changed a lot. Yeah, I guess the one the one message that the work has given us as you know, if you are using the secure VPN is to make sure you connect to it as quick as you can. Because it does provide some added layer of protection around people maybe surfing your home, Wi Fi, which is also I think, reasonably secure. I've got a very difficult password to to get guess. Yeah.

Researcher 26:11
What about so I only home network? What about other family members or friends or family members that might have been given your home Wi Fi password for example, do you have concerns around that and either access to personal data or work data or

Participant E 26:29
no, don't have access to consumers access to work data. I don't really have a good answer on that level of trust. If we only give it to people that we do actually. Trust, right? Home Wi Fi password. That's probably the one that doesn't change as much, which again, I suppose if there was actually a there's a risk there, we've given it out now we're gonna have to go and change it. Right, yeah. Yeah, there's risk to other family members who might not look with us. They might have given it out. But again, they're all pretty aware of not to just go share it willy nilly. So.

Researcher 27:09
Okay, and just going back to the training, when you've had training, you've obviously to training at work then as that triggered you to do a few taking that and that's that triggered you to do this stuff differently or, or take action in terms of your personal security, cybersecurity actions. Oh, really, because? Because you were,

Participant E 27:25
I guess, yeah, been in the industry with cybersecurity was, I guess, being in the telco industry. Originally. That's that's one of those things that you become very aware of during that time that you're there and yeah, I've always taken affiliate seriously. So the trainings actually made a lot of difference to the way that I, I act,

Researcher 27:49
because of because of your background of working for Taco taco. And yeah, I guess is that that also does that that helps in terms of understanding how I guess how the whole system works in terms of devices and networks? Yeah. Okay. And so, you know, this is probably a good thing. Obviously, got the answer to this question already, but I'll just ask it anyway. So in terms of how do you think your your intentions regarding cybersecurity match your actions

Participant E 28:20
are pretty pretty good. Pretty pretty well aligned, I think.

Researcher 28:28
Yeah, sounds like it, but I just wanted to say, Yeah, what about when you think about, you know, all these devices interconnected with everything, so you know, smart TVs, and, you know, Bluetooth devices and IoT and stuff like that. Do you think there's risks around that where you do ever think about that? When Yeah,

Participant E 28:46

yeah, that's actually I mean, I have until recently avoided smart devices in the home. I think the only thing I've got now is the Smart TV. And yes, there is some concern around that. I don't know how secure that is. Hopefully, it's reasonably secure because of sitting behind the behind our firewall, but

Researcher 29:12
don't really know. So it's a concern, but you know, it's a concern, but you don't necessarily know what to do about it, other than not to happen. Yeah,

Participant E 29:19
yeah. Yeah.

Researcher 29:21
Okay. What about things like, cameras on laptops and stuff like that? You know, do you have concerns around those being hacked or people snooping

Participant E 29:33
against something behind the firewall? I mean, the only thing I've got the camera on the laptop sitting behind a firewall are less concerned about that than I would secure security cameras, which are sort of streaming somewhere. Yeah, so I've got nothing really to hide either. So that's a bit of a bit of a Okay, so somebody could take my laptop and what did they say? I've seen? Yeah. Yeah. Just a normal household. So it's like, you can see what's in the background here. There's not a lot to the level of private stuff there. That would be of concern.

Researcher 30:11
Yeah. All right. smartwatches. Do you have smartwatches or at all?

Participant E 30:15
I do have a smartwatch. Well I guess. I guess I call it a smartwatch. It's a Garmin one. It's not like your standard Apple, or

Researcher 30:25
is that and is that that's, that's your personal device that you use? I guess he linked to personal like mobile? Yeah. Yeah. Okay. All right. When he talks about trash he talked about he talked about your, your shopping and trusting some sites and not others. What do you think about apps in general, do you how do you think about trust in terms of would you trust something because it's bigger? That's like, you know, I don't know what the Facebook's Twitter or whatever. They're huge. Basically, would you trust them more? Or would you say, would you then say, well, actually, I trust them less because because they're big, they're more a bigger target for how do you think about that?

Participant E 31:14
I guess it's more based on reputation. Particularly I don't trust Facebook or Twitter. Because they haven't certainly have a reputation for allowing things on their sites which I guess I don't have a reputation for xxxx. I'd been good moderators of contact. more open. I would not trust a an Android device explicitly with with too much. So it's pretty much an Apple Apple person. In terms of buy prices, obviously the Garmin watch which is neither Android my apple isn't it? I do know that Apple tends to tends to, I guess, a lot of the apps before they go they go into the Apple Store, whereas on the androids side it's not quite so it's a bit more open. So there are trust something which is a bit more closed community as

opposed to an open community terms of terms of other other apps it's around it's around. Social media isn't the probably a really bad example because trust social media in general. But other apps, again, around the reputation that those that you know, offer that particular organization that produce the app, so like banking apps, then you know the the banks got to be pretty robust. They also have they also have I guess, if that compromised in that liable, that's good reason to trust them a little bit more experience with the site builds up more trust. So there's a whole whole range of things which sort of build into that trust model, but yeah, sizes probably sub teacher as particularly one of those things, but it's more the size of the organization and how they actually use your information or what they're actually doing for you. So the type of application as well.

Researcher 33:40
Yeah, yep. No. And so I'm just going back on your like, so you're in the transition of RC always going to work work from home. Was that was there a significant change? In terms of the your organization's policy around that or in terms of its training around that was a big focus on actually improving or educating or compliance around that increase in you know, awareness, compliance education.

Participant E 34:10
This probably was I'd have to say it's probably a bit more focused on the working from home aspects of I guess. Still only using word approved methods for connecting to the to the to the laptop never sending work information home because that's, you know, that's a big no, no. But there's probably a bit more of a focus on that. There's a focus, probably a focus internally about making sure that the pose methods were secure, but they had to be focused on that anyway, because there were a number of people working remotely anyway. So for work, it was more around the volume. Working from home is actually coping with the volume of people working from home rather than the actual security side, but also making sure that people were a safe and physically safe because health and safety regulations but a little bit more around around the I can see other concerns about sharing information was certainly came up in the compliance training and that sort of thing.

Researcher 35:17
Okay, and when you're working from home, and I don't know where to start, you got other people in the Harris tea whenever you leave your your laptop, do you screen lock it or stuff like that? Or do you just

Participant E 35:30
I mean, I've took me when I'm working for five years now but no one else here. A little bit. Screens aren't visible from from outside or anything so, but most of the time, I'm lucky to us trying to keep anteater work.

Researcher 35:48
Okay. All right. I think that's probably covered. covered, and I think so. So I just want one thing about one thing we talked about earlier about, you know, family and friends using your home network or whatever, that's good. That comes back to that trust trust aspect again, doesn't it in terms of accuracy? Yeah, concerned about that because our family and friends and the only giving you your network password to trusted individuals. Okay, nothing

Participant E 36:16

to be feared generally when they're around. It's either family and if it's during work time, we're time we're think potentially more compromisable. That's only family who are visiting during more personal time it's I guess, friends of family, whoever The tinkerer visiting the finish will have other things. If you know what I mean. Given given given that, my partner and I were the only ones living in the house now it's, it's pretty much less of the other people who might have access to Wi Fi.

Researcher 37:00
Yeah. Okay. All right. That's all that's all my question. Any any any any areas or any stuff that you can think that would, would, would be? You know, that you were expecting questions on our

Participant E 37:11
I'm glad you didn't ask me on passwords.

Researcher 37:18
There wasn't a there wasn't a test like that. No, sorry.

Participant E 37:23
Yeah. actually interesting. I guess the range of questions that came through throughout this around a comfortable I guess how comfortable I am with my attention to security and that sort of thing. Yeah.

Researcher 37:46
Okay. That's great. Thank you. I'm gonna stop. I'm going to stop the recording now. If I can work how to do that.

Participant F

SPEAKERS
Researcher, Participant F

Researcher 00:00
If it's working right, just testing, can you say something and I'll see what's

Participant F 00:07
12345

Researcher 00:09
The growing? That's correct. Yeah. Yep, seems to be working. Excellent. All right, so so I'm gonna start with questions regarding devices or use. So you know, and I want as many devices I mean laptops, home computers, mobiles or whatever. So do you have? Do you have distinct separate personal and work devices that you use?

Participant F 00:35
So I have a separate laptop to at home, I have a MacBook at home, and I have a tablet at work, or whatever they call a laptop tablet thing at work. And then actually my mobile phone is a dual SIM phone so I have one sensor personal and once for work.

Researcher 00:55
Okay, so your your your MacBook at home is your personal computer that you and your tablet is your work computer but you have one thing with two SIMs effectively. Yeah, I want to work on wonder. Yeah, okay. And do you also have Do you also have a fixed home home shared P home PC? I think I'll just

Participant F 01:19
know that it's xxxx's really not mine.

Researcher 01:21
Okay. All right. So in terms of your talk about your work, your work laptop or your work device D D, is that for doing any personal use? Do you do any kind of personal activities on it? Yep, so

Participant F 01:37
doing things like emails, internet surfing. It's because it's a tablet. It's got I actually I signed contracts on it as well. Because got a pen. It's got stylus, okay. Yep, sorry. So actually, yeah, I do. I do do a bit on my work one because it has that functionality.

Researcher 01:55
Okay. And do you do activities like say do you do social media on your website? Or? Yeah,

Participant F 02:04
yeah, I do. I do LinkedIn. On my work device yet but not Facebook. Okay, so my personal

Researcher 02:10

What about things like online banking?

Participant F 02:12
No, not on my work device.

Researcher 02:16
What about things like the kind of online shopping when you go and purchase something and you might be putting credit card information

Participant F 02:23
I might have done that once or twice on my work device, right? Yeah, possibly. Right. Yep.

Researcher 02:31
And presumably, obviously you do all those. Do you do those activities? Obviously on your, your your MacBook or your to do online banking.

Participant F 02:41
He can't do online banking or I need to get on my phone. Okay, my book but yeah, every everything else I do on my MacBook. Yeah.

Researcher 02:48
So all social media, any online shopping for the fact that you do on your own personal? Yeah. Cool. All right. Thank you. And do you go counter question do you do daily work activities on your MacBook your own MacBook? At all?

Participant F 03:09
I don't think so. No, I think the only time I did that was if my PC was down if my if my laptop my work my work one was down.

Researcher 03:23
Okay, that was an alternative as a backup you might go into your home. You had your personal that MacBook and use that for Yeah. Okay. Cool. So you don't generally you kind of have this separation of work laptop and home laptop. Where as you might have done some some activities like LinkedIn social media and maybe some shopping on your work well, but generally you're you you do work on your work device, then you do your personal stuff on your home device. Or your personal device. Yeah,

Participant F 03:54
generally. But I think actually what started to blur that line is because of the functionality I have on my work one, like I said, we're building a house at the moment. So we've had a lot of contracts and things like that to sign and like forms to mark apps. So I've actually been using the word one quite a bit for that. So yeah, generally in the past I probably would have been more separate but the reason it's less separate now is because of the functionality that my work device has.

Researcher 04:20
They got more functionality on your on that is that functionality, you can't get on your own device.

Participant F 04:25
That's right. That's not Yeah, my home devices not touch.

Researcher 04:29
Okay. Yeah, yep. All right. Um, and do you say sorry? So when you're at home your your So how often say how often do you work from home versus working? From an office?

Participant F 04:48
So I work from home half the time,

Researcher 04:51
right? So when you're when you're working from home, you're on your work device, your work laptop and your your that you want it over your home Wi Fi network? Yeah. Okay. And how's that work impairment that obviously, I guess we came back kind of during COVID So it wasn't so just one of the questions is whether that's changed as a result of COVID but I guess you would, you've obviously come back after COVID. So is it is it been always been 50% at home or

Participant F 05:24
so when we were in I mean member in the UK? I was still working? Yeah, when we're in the UK and locked down. Yeah, I did work from home obviously more than usual. But I have always had a component of working from home for about 10 years. Yeah.

Researcher 05:45
And on your so I say I say you wouldn't do psychotomimetic Do do you ever use your Would you ever use your personal laptop your MacBook and over a over the network at work or or no, just read? And Do do you run any antivirus software on your own device on your own laptop devices? Or?

Participant F 06:12
Actually, no, we don't on our Macbook because MacBooks meant to be invincible. Which I know is not true.

Researcher 06:19
I know I'm sitting on one notes as well. So

Participant F 06:24
yeah, we don't actually have any on my MacBook. And then at work we have Norton

Researcher 06:32
but I assume their work is controlled by the work policy on the IT policy. Okay. Okay, and in terms of so. So in terms of say in terms of use buddy with any scenario where you've stored personal data on work device on your work devices and vice versa? I've used taught worked work documents on your home device, or

Participant F 06:57
Yeah, that's an interesting one. Yeah, so yeah, big because I am using my work laptop for personal contracts and stuff. I am saving those, you know, on my work one I'm not saving any work material on my personal one though.

Researcher 07:17

And how and so when you're using your devices at home, I do you obviously, for both your work device and your home device. Do you have you know, auto locking mechanisms that lock because when it's not used for a period of time, you know, screen locket or

Participant F 07:32
Yeah, we actually just have a rule that we have to lock when we leave our desk at work so I don't think there's an auto lock on it actually.

Researcher 07:40
Right. So when you when you when you're at home, so when you're home then so you have a rule so you don't have an awful lot because as a rule that you have to lock it whenever you leave your desk at work when you're using at home is that the same there's no auto lock so therefore if you walked walk to the kitchen or whatever, or the living room

Participant F 07:55
or Yeah, yeah, if I walked away, it would still be functional. Right? But wouldn't wouldn't zone out. My phone has that. And obviously a lot of internet banking has a feature that when you toggle to another tab or something, it will lock you out. Yeah, yeah. Yeah, I haven't built any of my own settings on there. Yeah.

Researcher 08:18
Okay. In terms of the phone then you have one phone that has dual SIM. Is that and his advice? Is that your device without a work device? It's a work device, but you have a personal sim that you use to use it for personal use. Yeah. And how does that work in terms of so do you do do you only do work? Work tasks over the work sample and only personal tasks over the?

Participant F 08:45
No? So basically, I'm actually using my personal site depends with with a Joe so it depends what slot you put the SIM in, right? I've put because I because the majority of data that I use on my phone is probably for personal use. I've got my personal and slot one. So therefore, that means that any internet use on the phone will come from my personal cell, right? My personal cell plan and therefore anything and if anyone just phones or texts, my work number that's in slot two, so I'll receive in as well.

Researcher 09:27
Okay, so work to the work phone for work number perspective, but actually all your internet activity, whether it's personal or work is going over your personal

Participant F 09:35
thing. Yeah, just just just for the internet. It's about where or how it's set up like that. The actual mobile network is separated. Right? That you have to you have to draw your internet's from one source. I think that comes from my personal one. Yeah.

Researcher 09:52
Okay. And do you say you and obviously, when you're at home is that there is your internet is that then going over your home Wi Fi network? And when? When you go to the office with that phone does that does it then go on to the work, corporate Wi Fi network and so how do you I guess you're doing I guess you're doing I mean, you said you do I've never seen you doing online banking. Are you doing online banking, online shopping, social media all on on your phone? Yep. And that's all going over your personal? Yep.

Yeah. That would never actually go over. So I guess but would you do that? If you were there if you were then in the office and you were over the corporate Wi Fi network with that then go with that then go back? Yeah. And that would stop that or you'd like that would be online banking or or purchases or or social media and stuff like that? Yeah. Yeah. Good, thanks. Alright, that's covered devices just um, might get back onto some more questions than that. But terms of access mechanisms, how you access the the laptop or your phone? Do you have a preference in terms of things like password pin, you know, fingerprints, facial recognition, and if they want and is that the same for your work and home devices?

Participant F 11:14
Yeah, so I prefer fingerprint. However, it comes down to the functionality so fingerprint I have on my MacBook, which works really well. And the fingerprint on my phone is not good at all. So I rarely use it because it doesn't work properly. It doesn't seem to recognize my finger well. So therefore it would be PIN and here on my work one we don't have fingerprints, it's just log into the LAN thing. So it's password protected.

Researcher 11:47
Okay, so your work devices, basically, whatever the policy that works, so you've got a password to access to the corporate network, basically. Yeah, okay. And and for your, for your, for your personal activities where you are see, you have to make multiple different passwords depending on banking or online shopping or social media, whatever do you do? Do adopt policy have a more complex password for certain types of usage or on? So I don't want you to tell me anything about your past your past.

Participant F 12:25
I normally do an auto generated password, right? It's my preference. Yeah. Okay, sorry. There are some historical accounts where I have before auto generated password was available as a feature where I've memorized my own. But now I do auto generate, and then I save it under the password manager.

Researcher 12:46
Okay, so that you're using a password management device to actually generate your passwords and that's so in using that to that. Do you have to change those at all often or?

Participant F 12:54
Sometimes, but the idea of having the managers you don't have to change them. Always says, yeah, sorry, yeah, no, I as the manager is working properly and I'm using the right manager, then it's normally fine.

Researcher 13:09
So if you're using a password manager, then you don't that's that you don't have to worry about changing passwords for that. Yeah,

Participant F 13:15
I only I only I guess if you find out that the password could have been compromised.

Researcher 13:20
Yeah, for other for other devices where you do set passwords. Do you Do you readily change those?

Participant F 13:27

From No, I probably don't have many, many that have a password like that anymore. Might just be like my facebook or something. And so no, no, don't really change those regularly.

Researcher 13:40
And what about your work devices? Does work force you to change passwords every so often, or how does that work from my work?

Participant F 13:46
Very good question. Yeah, I've had that in every single job, but actually, I have not been asked to change my password yet. So I don't know that they do.

Researcher 13:53
Do they have rules about what the password needs to be or?

Participant F 13:57
No, I'm not. I don't think so.

Researcher 14:06
And if you do, is there anything that is there anything that you that would would? Is there any event or something that would trigger you to change your password or where you where you've got passwords that need changing?

Participant F 14:17
Yeah, I mean, sometimes you might be alerted from the provider that they're aware that your password has been compromised, you know, from the from the website or whatever it is that yeah, so I change it in that instance. One thing which I haven't really done, but I do see a pop up is actually in password manager in Chrome. I think it does tell you whether they think that the passwords are compromised or not. And you should change them. Right. Yeah, I haven't actually done that. I have seen that there.

Researcher 14:49
Is that inside in and is that is that the apple Password Manager or is that

Participant F 14:54
when I think okay, yeah.

Researcher 14:58
Okay, all right. Um, okay, thanks. So I think the customer thinks sorry. Um so in your home network, that's is that shared with you know, with, with the you know, with your your partner, your kids, you know, obviously, we're not your kids, as I shared with your family.

Participant F 15:22
Yeah, yeah. So, so yeah, xxxx obviously uses it. He uses it for work as well, because he works from home permanently. And what else if people come over? Yeah, it's on the fridge.

Researcher 15:36
Okay. So your passwords on your home Wi Fi is on the fridge and if guests come they can log in. Does that pass whatever change at all?

Participant F 15:47

I really have not changed it recently.

Researcher 15:50
I never you never go in, delete somebody from it or kick somebody off. Or anything? Oh, no, I've not done that. And is that because obviously they're people you trust or people you know, you're?

Participant F 16:00
Yeah, I would only really be immediate family that would use it. I mean, it's pretty rare these days. People ask you for the Wi Fi password.

Researcher 16:06
Yeah, yeah. Okay. Okay, so So basically your password your home Wi Fi password is shared with guest family friends wherever they come from a visit basically. Yeah. So going back to your devices D that do you whether it be your work, your work, tablet or your MacBook Air or your phone, D D use those devices over other networks that might be you know, Wi Fi in a cafe or Wi Fi in a hotel or Wi Fi in an airport. Yeah. Yeah.

Participant F 16:45
I mean, I haven't been to an airport in a while. Yeah, I mean, certainly, when I used to travel for work, and that sort of thing would regularly use Wi Fi. But yeah, now I'd use Cubase Yeah. Or if I was going around to my parents or something I might use their Wi Fi. Or maybe Cafe cafes. I wouldn't probably use a Wi Fi hotspot in the city or anything like that.

Researcher 17:13
Okay, but if you're with our cafe and you really I don't know, what would you then do? Let's say the phone we would do then you log on to that cafe Wi Fi network would you then do things like online banking or purchases or or social media on that or is there

Participant F 17:28
any I don't think that I don't think we'd be doing internet banking on the network. Because we do but we do it internet banking on our phone and we wouldn't I wouldn't bother with connecting my phone to a cafe network would only be working for an hour on a laptop. So probably wouldn't do internet banking. I mean, maybe would do some shopping possibly,

Researcher 17:52
right? Generally you wouldn't bother connecting your phone because I guess you've got that because you have unlimited data anyway on your phone. Okay. And but you would potentially could do some shopping on your laptop if you're working there or you could do some social media network, okay. And do you differentiate between like a cafe Wi Fi network or a hotel network? Or is it just Are they just do consumers want public Wi Fi networks that you can connect to?

Participant F 18:27
So probably would be more likely to connect the phone to a hotel network because you'd be staying there for a longer period of time,

Researcher 18:35
right? Yeah, yeah. Yeah. Okay. So it's gonna be depending on depending on the context of if you're just there for an hour or whatever. Yeah, you might not but

Participant F 18:48
it's a short period of time. Isn't my last point. Yeah.

Researcher 18:52
Are there any activities that you you wouldn't carry out over a public Wi Fi network at all? Um, is there anything that you wouldn't do because

Participant F 19:02
do internet banking on a public Wi Fi network? And I probably wouldn't use something that required putting in my credit card details or anything like that. Yeah. Yeah, it would really the only reason I'd be connecting to something that's public Wi Fi would be to contact someone that I need to get ahold of or you know, yeah.

Researcher 19:30
I wanted what do you think about apps that you you you sign up to or you subscribe to or you know, things like, does does the size of that the I guess the the popularity or the size of that application influence you in any way because it would you would you sign up to something because it's more it's got lots of users is popular? Or do you sign up for something that's less popular because it's less likely to be subject to attacks because it's less?

Participant F 19:58
Yeah, so if I was looking for an app, and there was a number of different apps available to do the same thing. I would probably go based on the reviews as to which one I would choose, right? Yeah, that doesn't happen very often. I mean, normally an app has, you know, connected to a particular service that you might already be part of, or you're wanting to be part of. So

Researcher 20:20
yeah, you would think about an app having loads of millions of users will be more more time or a bigger target for somebody focus. cybercriminal because we would be that would concern you much or

Participant F 20:31
I wouldn't be thinking about that. Probably when I'm downloading an app. Okay.

Researcher 20:37
I'm on I'm a subject of cyber attacks. Have you ever been I've ever been the victim of a cyber attack?

Participant F 20:44
Um, no, not really. Not personally.

Researcher 20:48
No, no. Have you seen Have you seen attempts that you've spotted in? Not

Participant F 20:55
at all myself? Yeah. Yeah, yeah, definitely. I just got a phishing email last week actually, saying that they were the chairman when they weren't. xxxxx was on holiday. So that was lucky.

Researcher 21:09
And so So how, how would you do find those to spot those kind of phishing attacks?

Participant F 21:16
And what I've pretty lucky because you know, I worked for xxxxxxxx for years. So I am I have a pretty good litmus test as to what to look for.

Researcher 21:28
But you haven't yeah, there's been no you haven't had any have been had any attacks that have been successful or anything that's compromised you or stolen your data? Or?

Participant F 21:38
I mean, I'm sure that my my data has been, you know, my password from 10 years ago. I'm sure that that's out there on the internet somewhere. I mean, a bit pretty unusual if there wasn't something of mine that was out there, but I am not aware of it and it hasn't affected me.

Researcher 21:57
Right. Yeah. Okay. And that leads us on to the next topic total. How How concerned are you how, you know, how concerned are you about identity theft? Does that does that worry you? Does it does it? Does it affect how much information you make available online or?

Participant F 22:14
Yeah, that's also people ringing out to ask information. I think it's unusual if they need a lot of information to do something that's quite straightforward. So I wouldn't say that I'm worried about identity theft, but I'm very aware of it. And like, for example, if a company wants me to give them give the date, they want me to give me they want me to tell them what my date of birth is. Just to like into to sign up to their mailing list. You know, I'll put it I'll probably put a fake date of birth and so I wouldn't be sharing my personal information that would be associated with my identity, willy nilly unless I thought that it was actually necessary to identify myself.

Researcher 22:59
Okay, how about many thoughts about privacy? In terms of any concerns about privacy or?

Participant F 23:08
Not really? I mean, I don't think I have any real private things about me, I suppose. So. No, not really worried about that.

Researcher 23:18
So you're not Yeah, you're not worried about that. You know, what about your digital footprint and other than what you've just said in terms of when they're asking for information that might be more than what you think they need for the task and handle?

Participant F 23:30
Yeah, I mean, I am aware of that when I'm undergoing an activity or a conversation or an interaction with a company. It may be that I asked them to, to, like, demonstrate that they're the right person contacting me. Or it might be that I asked them where they need

certain information in order to process what I'm asking them to do or whatever. Yeah, so yeah, I'm definitely aware of it and I would be asking questions about it.

Researcher 23:59
Okay. What about device cameras? Do you? Are you concerned about device cameras being subject to hacking or people accessing them or?

Participant F 24:06
I mean, not really, because I don't think that, you know, again, I'm not really worried about privacy too much because not really sure what they're gonna see at the end. Of the camera anyway. Yeah. All right. Yeah, no, not really. Okay.

Researcher 24:24
Okay, I'll just say different topics. So in terms of training, in a work in your work environment, it could be kind of working from all previous work environments have you received Have you received training regarding cybersecurity? And has that been a one off training or is it ongoing training or?

Participant F 24:42
Yes, I haven't previous, like big companies. I haven't in my current role. Yeah. So that's probably a resource thing. You know, as companies scale, they can be able to do that. Okay. You definitely receive training many times.

Researcher 25:03
You receive training many times, but not necessarily in all jobs for all companies. Is that okay? Yeah.

Participant F 25:09
To be fair, it probably would be every single company I've worked for apart. From the one I work for now, because it's very small.

Researcher 25:16
And what about what about things like cybersecurity guidelines and policies? Although they've always been communicated and clear from organizations and

Participant F 25:28
so, so I think device guidelines and so far is what the rules are around using work kit. They've always been relatively clear. guidelines around the internet use. Yes. I wouldn't really say cybersecurity guidelines. No, I don't think I've probably maybe at my last company, but maybe it's age. But yeah, no, I don't think companies really have cybersecurity guidelines that they share with their staff,

Researcher 25:55
more usage, more device usage guidelines, or would you say, oh,

Participant F 26:00
yeah, well, it's more about like, what you can and can't use your device for which you know, might be you can take personal calls on it or can't leave your device in the car because if it gets stolen, that's not covered by insurance, you know, that kind of stuff, but not really about the principles and practices that employees should be doing to ensure that their cyber secure I don't think I've really seen that actually. And guidelines.

Researcher 26:26
Yeah, yeah. Okay. And

Participant F 26:29
process where they think they've done and delivered the training. You know, they don't actually have a policy or a guideline around it specifically, they've just done it. They've just made staff undertake the training. So it's kind of box ticked.

Researcher 26:41
So it might have been, so it might have been that the policy guidelines or it might have been covered in the training, but yeah, yeah. Okay. All right. And what about fun, any personal use non word use whatever. Any tea, are you aware of any guidance or training or guidance or guidelines or policies that you have to comply with from anything you use in terms of usage or, or is it is that really come from work? related to cybersecurity, I suppose. Yeah, yeah.

Participant F 27:17
Yeah. Do you mean Have I gone about to kind of create my own?

Researcher 27:22
No, no. Are you are you aware of any organizations that that are proactive in, in, you know, in, in preventing, you know, or giving guidelines and preventing cybersecurity attacks any any does? Are there any organizations you would highlight to say, Okay, well, they, they, they, they, they send out regular stuff, they give guidelines and stuff regarding regarding cybersecurity at all.

Participant F 27:50
I mean, the company that are the cybersecurity company I worked for was pretty good at it, but that's because they're in the industry. So, yeah. No, I mean, otherwise, I think it's sort of just an annual training thing.

Researcher 28:04
I mean, more and more more in personal usage outside of work, so nothing to do with work, right. Yeah.

Participant F 28:10
No, you know, I don't think that any company, is there any guidance around sort of personal principles? I think, I think they assume that you know, the same people would take learnings from a work sense and apply it to their personal life sort of thing.

Researcher 28:24
Right, but that would come from from something they did, they'd learn from work I guess. Yeah, that's right. Yeah. So isn't ads in somewhere else? So we there is somewhere else where you've gotten actually okay, well, that's, that's interesting. I apply that to other personal use, or it's generally come from work where they've, they've given you

Participant F 28:43
I see what you're saying. So is there any other any other like situations where I've taken learnings from? Yeah, um nah, I mean, maybe like, just awareness campaign like in the UK, they have NSPCC or like the, the, what's it called the National Cyber Security Unit in

Cu or whatever it's called. So you know, I'd see this stuff on social media and my you know, take learnings from the public campaigns, right? This is in New Zealand. We haven't really seen anything Nah, no, I haven't been looking for it. You know, it's different when you work in the industry. You see this stuff regularly? Yeah.

Researcher 29:36
Yeah. Alright. And then okay. And then. Okay, we've covered so the question regarding intentions versus action. So in terms of your your awareness of cybersecurity and your intentions, how, how well does your do actions match up?

Participant F 29:55
Yeah, probably not very well. I mean, knowing what I know, I should definitely have better practices. But yeah, it's just it's another administrative task, isn't it? So it's just something that ends up on the, you know, in the back of your mind that you could maybe do one day is if there's an order on from that from that point of view. And so yeah, I mean, I could definitely do better. But then it's also not something that you really talked about with people. I'm guessing that my practices are probably a little bit better than the average person. But again, don't really know because no one talks about it so

Researcher 30:31
not a good QB barbecue conversation about

Participant F 30:37
management going Yeah, yeah. So so yeah.

Researcher 30:46
That's fine. And you know, that kind of related question Has your has, how's your approach change? You know, pre K word where you weren't working from home so much to post COVID When you were when you are working from home much more has that has that had a change in terms of how you behaved from a cybersecurity perspective?

Participant F 31:08
I actually think it's probably going to negative impacts, because those work and personal lines are so much more blurred. And, yeah, because you kind of use any device for anything that needs to be done type thing. Whereas when personal and work lives were separated a bit more I think there was a bit more of a separation and device use. But also, I think, because during the pandemic, like nothing else that happened, there wasn't any big cyber attacks. There wasn't any terrorist attacks in the world, you know, because the world was just dealing with a pandemic. So I think it kind of made people forget about being prepared and preparing and securing yourself for those sorts of things. So yeah, I think it's probably made us quite complacent. And also because, you know, company training was probably put on hold during that time and much more hard to roll out. So again, there wasn't really those like natural moments in time, all those reminders each year when you had to undergo your training as to what you should actually be doing. So yeah, I think it probably on the whole has made people much more complacent.

Researcher 32:21
Yeah, okay. That's good. Um, and how much does? How much does trust influence your behavior and you know, trust in, in people trusting organizations trust in you to be working with those trusting other organizations? How does that affect how you behave? from Cyprus? Yeah.

Participant F 32:41
I think I'm definitely more likely to use a company services if I trust the company, and an extension of that would be using their apps, right. So it's a tricky one because I'm not really sure that when you think about trust, you actually necessarily think about how cyber secure as as company you're, you're probably more Yeah, I'm not sure that's really selling that sort of front of mind when you're thinking about trust, but it probably should be you know, it's just how well their marketing and comms departments done, I suppose in terms of making them look like a trusted and ethical brand. So yeah, definitely. I think it's much more important to myself into to buyers in general, but I'm not really sure that's associated with cybersecurity.

Researcher 33:32
Okay. And in terms of the organization you work for you would you say you typically trust the organization and work for or do you have, have you had scenarios where you'd say, well, I, I, I wouldn't trust it. I have I'd have concerns with the IT people in that organization accessing data, but

Participant F 33:49
I would actually have concerns in the company I work for at the moment. And previous rows, and no, I'm probably pretty, pretty confident and the expertise

Researcher 34:01
in the data related to any confidence in your expertise or comfort or, or concerns around maybe people being malicious or

Participant F 34:12
while there was concern when I worked at xxxxxx, the cybersecurity company, because we were the perfect target, you know, a security company. So, so yes, there was concern there that there was, you know, it to be careful from an inside point of view. Yeah. I wouldn't say that it was necessarily because I felt it myself. It was more because that was sort of the message from management.

Researcher 34:41
Yeah, okay. Okay, sounds good. Thanks. And then just in terms of, how would you have you got how would you classify your behavior regarding aspects that says forwarding emails or opening attachments or, or passing

Participant F 35:03
options that they actually so there was I imported this phishing email that I got on the other day to the chairman and identified four things that was wrong with it. So yeah, I'm I really would not open attachments unless I was absolutely certain it was from the, the sender. And see, I always check email addresses and things like that. You know, like, Isn't if the email address looks sketchy then, you know, it's probably not real. Yeah. Yeah. Okay. But also circumstantial things. So this email that I received from the chairman was at 8am on Tuesday morning, and it was Anzac Day. Right? So I was like, That's a bit weird. I don't sit and said, Can I speak to you? So I was I don't think he wants to speak to me on ANZAC Day. So yeah, you're playing

Researcher 35:56

fantastic. Yeah. And what about things like a you know, obviously, let's use the tape but USB drives, for example, do you do share documents via USB drives?

Participant F 36:05
I don't really do that anymore. I've done that for a long while. And I think that's because, well, I was very aware of the worry with USBs. But I think that was more a functionality thing that they just you know, there's no room for me to have USBs anymore.

Researcher 36:22
What about other smart devices? So you know, in your home smart TVs might work? watches what what had How do you think about those from a security perspective? Do you have concerns around those or, you know, in your home network with you have lots of network devices connected via Wi Fi?

Participant F 36:38
Probably the biggest thing that is concerning is Alexa Voice listening. And I pretty sure that's effect right like they are they are listening and so therefore they can affect what you see on your devices and, you know, follow your shopping behaviors and that sort of thing. So that's, that's, I don't really like the apps. I suppose I feel that the benefit of Alexa outweighs that risk or that concern. So that's probably the only real thing that I'm worried about, really, but we do have a lot of other connected stuff like we've got a Sonos and yes, smart TV and smartwatches and stuff like that. But probably the Alexa would be the one that I don't like, right?

Researcher 37:31
Okay, and it has a smartwatches like all fitness plans or whatever. Do you do you ever have concerns around them tracking your location and being used as a, you know, where you're tracking where you're at? Yeah,

Participant F 37:41
no, I've never thought about that. Thanks. For now. No, no, I've thought about the keys, they could have come to find out where you were. And to be fair, I don't actually really use my smart watch much. But I do have geolocation on my phone so it could be used to.

Researcher 38:00
Okay, all right. And probably one last question. So when you're on your on your online shopping, do you do have specific like debit or credit cards that use online shopping or just use ones that you normally use?

Participant F 38:15
I always use credit cards because normally they are covered for fraud, right? Yeah, I would I do specifically not use my debit card on this. I absolutely have to,

Researcher 38:24
but it'd be your normal credit card. You won't have a special one that you just Alright, I think that was that's all my questions. Is there anything anything you want to ask or anything that's springs to mind or that

Participant F 38:37
oh, what's, what's your study plan? What are you you're writing your thesis then?

Researcher 38:43
Yes, there's no reference thesis. Yes, basically. So it's basically interviewing a number of people like yourself and then and then analyzing the data and then and then writing the thesis based on it. So yeah, so yeah. So quite a lot of interesting stuff in there. So thanks. Thanks for that. Appreciate that.

Participant F 39:03
Are you finding this, your research is hopefully supporting what you had thought?

Researcher 39:09
It is in some aspects and sometimes it throws up something interesting. So I think from that perspective, it's like you know, you know, you learn you learn a little thing quite often, I've learned a little thing from each interview in terms of actually I haven't I haven't thought about that or, you know, that's kind of interesting approach to it.

Participant F 39:26
Yeah. Well, if you need any other cybersecurity, I mean, not that I'm an expert, so I shouldn't have said other at all, but I said, if you do need any sort of cybersecurity experts, I'm more than happy to connect you with my colleagues and the my ex colleagues in the UK. Yeah,

Researcher 39:45
that's great. I'm just going to stop the stop the recording now. Okay. Just bear with me a moment.

Participant G

SPEAKERS
Participant G, Researcher

Researcher 00:01
Alright, so just gonna say something to test that it's coming through. Okay?

Participant G 00:06
Maybe you want me to say something?

Researcher 00:09
If you can say something? Yes, please.

Participant G 00:11
Hello, Paul, how are you?

Researcher 00:14
I am good. Thank you. Okay, that's all looks to be working. Okay. These transcriptions are never 100% but they do a reasonably good job. Yeah, yeah. Okay, so first we're going to start with just returns of understanding the devices that you use both personal devices and work devices and that can be mobile phones and laptops or tablets and stuff like that. So what what devices do you have and what do you use?

Participant G 00:43
Okay, so I've got a work laptop and a work phone. And then there's a household we have two iPads. That are while we have two iPads that are shared. And then one of my children's got a Chromebook, and other ones got a Chromebook and a MacBook Air. We kind of all can have access to those and then my husband's got a work laptop. Which we all use. Everyone uses everyone's laptops to pop no one uses my work. laptop or phone. Right. I don't I don't have a separate phone. I just use the same. So yeah.

Researcher 01:24
So you just have a say just have a work phone. Yes. And you have a work laptop. Yeah. And then you have a number of shared devices that are used

Participant G 01:33
at home. Yeah, and even my husband's like, I'll go and watch Netflix or neon on my husband's work, laptop but no one uses my work laptop or phone for anything.

Researcher 01:44
Okay, so he has a working laptop, which he also use for him perhaps. Okay, yeah. All right. Any particular reason for that or just you just keep your your person your work laptop just purely for work?

Participant G 01:59
Yeah, fieldwork and all my security at work, or their passwords, everything. I just don't like anyone using mine whereas, yeah, yeah. Yeah. I just keep it work. Work based.

Researcher 02:14
Okay, that's cool. Um, so in terms of your work laptop, do you ever use that for doing personal use?

Participant G 02:23
Yes, I do for me. Yeah. Yeah.

Researcher 02:27
And what, what is any restrictions that you do you restrict? Do you don't do on the work laptop or would you do

Participant G 02:33
so I wouldn't. So, so I've used my work email for personal stuff. For example, there's my email for my school, the school children comes to my work one because my only other email I could Google a Google email over here. I've got a Google email, but I've got a Hotmail but I don't have access Hotmail or anything like that from my work, laptop. So because I need access, I get email stuff during the day important stuff on school, which I sometimes have respond to. That's why I use that kind of stuff for my my work email the same for my banking, I use my like, as general correspondence. I've just genuinely tend to use my work, email.

Researcher 03:15
Okay. So do you do do you do things like online banking on your work laptop?

Participant G 03:18
Yeah, I do. Um, yeah.

Researcher 03:22
Things like online shopping. We have to put in credit card details and stuff like that. Would he do that in your work laptop? I

Participant G 03:27
have done it on my rig. And my husband mainly does it from his but I have done it on mine. So yeah, I have used my credit card. On my laptop, but I never save any other passwords, which is interesting, because when the children step up, they always say they won't say passwords and I can't understand why I don't want to have my past word save I never save password.

Researcher 03:49
Right. Okay. And in terms of things that I also say Do you also do Do you do any social media on your work?

Participant G 03:57
Laptop? Um, I don't actually really post anything on social media to be honest, but I do have will face weirdly your Facebook is open on my work, email and we use messenger to message my parents from my work laptop, otherwise I use if I'm gonna post anything, it would be for my phone. Right.

Researcher 04:21
Okay, so now you mentioned the phone so the phone is a work phone so you use that for that you're gonna have a one on one phone which I work yeah, I work provided network

connection. Is that right? Yeah. Yeah. So again, do you use that for both personal and work use?

Participant G 04:39
Well, yes, I do, actually. Yeah, yeah. No, I mean, I don't have heaps, but I have my ASB bank app on there. Right. I have two bank on that. And I have Twitter and I have Instagram but i i Look I don't post

Researcher 04:57
and you would again do would you do like online shopping stuff

Participant G 05:00
on your phone? No, no, I don't really do online shopping on my phone.

Researcher 05:03
Okay, but you do online banking for example. And in terms of say, Sit at home, you've got kind of shared devices that you use at home that are non work devices. Do you ever use those for work? No.

Participant G 05:21
No, I'm just trying to think there if I have ever No.

Researcher 05:28
No, okay. And and the you so you don't do any you don't use your personal devices at home that are personal devices to carry out any work tasks or activities. No Okay. And we would never use this device. You would never bring this device into the office and use it over the work network. Okay, no. Okay. When you use all work devices, like your laptop and your phone when you when you're using those from home, presumably they're going over here are they going over your home Wi Fi network?

Participant G 05:59
Yes, they are. Yeah. Yeah.

Researcher 06:03
And, and since COVID, since the pandemic, are you doing more work from home or roughly or

Participant G 06:11
on this? So before several weeks, I was part time obviously, and I am still part time Well, they've just increased my hours and I was always doing a little bit of work from home occasionally, especially project specific so there's esprit project was near where I lived, so I probably would work more from home. Generally speaking, you know, relative to my hours when I worked on this xx job I probably had an average one day a week, working from home at the moment and I've just increased my hours to almost full time. So since the pandemic interestingly, I actually prefer working in the office.

Researcher 06:49
What do you what would you want less from home now because it's a pandemic? Yeah, do

Participant G 06:55

with less than home I do work from home to fit in with not lifestyle but for the children from time to time to be home for them one day a week. But generally my preference is to be in the office but I do like the flexibility of being able to work from home as needed.

Researcher 07:15
And as the the you know, the organization you work for as that, as that changed as a result of the pandemic and enabling you to work from home easier or

Participant G 07:24
Yeah, well, I think for me, because I was part time and being a project manager it was always quite flexible for me. So it was an understanding of an element of working from home or flexible working. But that was probably more on a ad hoc case by case where it's now taught in more policy around working from flexible hours working from home right, so I think it's definitely it's more across the board now.

Researcher 07:50
Yeah. Okay. Yeah. And in terms of your work intensive work devices, annual home devices, I do use any kind of antivirus software or anything like that, so

Participant G 08:01
we'll see what what if it's on my work laptop, it's all set up with whatever antivirus they have for that. And when we first got a laptop in New Zealand, we got a name of it. We actually paid for a antivirus software because our friend worked for the company. So we did have it but I would say we don't have anything now on any of our devices. No anti was the antivirus. Yeah, nothing. I assume my husband does on his work, but I definitely

Researcher 08:38
do is that depending on what the work policy what the work Yes.

Participant G 08:43
Turn on voice I don't know I'm assuming they would have some element but we haven't when we've put we've recently bought a new MacBook Air for our son and we haven't considered I don't even have it came up as an option. We just bought it in while we go. Same with his iPad that got people last year beginning last year. Yep, we just bought it and didn't even consider it to be honest. Yep.

Researcher 09:07
And do you so you said you use your work devices both phone and laptop for personal use? Do you ever store personal documents or information on those devices? at all on your phone or on yours?

Participant G 09:20
I do not on my time but on my desktop. I have got some now that you're saying that? Yep, I have got on my desktop. I have got the tabs on my passport, driver's license. Recent renumeration saved on there actually, because I've been needing that for documents for the bank.

Researcher 09:41
And in terms of your devices, both laptop and her phone and home devices, what's your preferred mechanism of access? Like do you prefer? A pin or password or biometrics like fingerprint or face recognition face recognition or? Yeah,

Participant G 09:57
so I'm about to get a new laptop with work in which that will be set out for your eye and fingerprint, my current one that's just the password and also it's probably not as as secure because I couldn't remember any of my answers to my security questions. So at the moment, I've just got a long password, which we had to change regularly. So when I set up on my new laptop, which I've gotten I just need to set it all up they're not gonna have will be i and fingerprint which I hope will be a lot easier with my phone, I've got a thumbprint and also code and then the children. They just all use their thumb prints, right? Okay, yeah.

Researcher 10:41
But your would do Do you have a preference if you had a choice or

Participant G 10:46
password be honest, right. Okay.

Researcher 10:50
I mean, in terms of password, do you do you use any kind of password management tools or or stuff like that?

Participant G 10:57
Or is this like that? So every so often I get something up saying Do you want me to save this here and a chain or whenever your key my keychain keychain? Yeah, I don't understand it. It's something like no, no. Okay, yeah. And I have to say what I have bought is I've got this little book that I bought from your sensei terrible I think I felt like I am an old not really with the time so heads up cuz I got so many different passwords with different things. I've got a little black book and it's actually a password book. Like a telephone book, right? And you put all the companies that you've got different passwords with but when I put the password and I don't put it out the fall, I do have like a little code to that but I that's where I keep it all. Okay, I guess Yeah.

Researcher 11:40
Yeah. And do you d so that book do you lock it away anywhere or was it

Participant G 11:47
Well, I used to but now we've gone using it so often to remember when when different things that I flipped around the house,

Researcher 11:55
okay. And do you do you have different like policies around the exercise more, more, more, more difficult, more difficulty, whatever for certain paths was another say would you have more difficult passwords for banking, for example, I'd say

Participant G 12:10
the same variety. I've got three kinds of standard passwords, which all have slightly different endings.

Researcher 12:17
Okay, but you use them for the for multiple different things.

Participant G 12:21
Yeah, yes, that's right. So I think if anyone wants to crack, crack anything, they probably could crack. A few.

Researcher 12:28
Thank you. And how often do you how often do you change passwords?

Participant G 12:35
Well, with work with laptop there we had they have to change them all the time with my phone. Never change it and with my banking. Never change it, right? Yep, yep, I would say it's only only my xxxx one which we have to

Researcher 12:56
set up basically on your on your work one on your work, where you're forced to change it by company policy or okay. So you never change banking or or social media or online websites or wherever we've locked on an account or whatever. Any times where you would have been prompted to change it or would have thought about changing it or

Participant G 13:18
only if I get any if I keep putting it in and it's says yeah, it wasn't and then I reset it and then I'll go in, put in the new password, which will be what I thought was the one before but they said it didn't exist. And I put it in like a you can't reuse the password. Well, I just said I couldn't use that. Plus, it didn't work. Yes, only if I think too many failed attempts, that sort of thing.

Researcher 13:42
Okay, all right. Okay, thanks. And so you said before you use both your laptop and your home on your work phone, when you're when you own your home, your work users over the home network. Yeah.

Participant G 13:56
It automatically just clicks over

Researcher 13:59
as our home Wi Fi network shared with all other people.

Participant G 14:02
Just just in whoever well definitely the people in our family and probably any other family, extended family or any my children's friends who will turn up to the house they probably already got it all on their phones now. To any

Researcher 14:15
friends guests or whatever. Visitors Do you share that around? Yeah. Is that fair? Is that like a freely available in house or is it

Participant G 14:24
well, we the children just go on to their phone and they just says share with them they share with someone else you have to have it shared. You can't just log on to it. It's not Yeah, it's not an open right. Yeah. You know, not only one because we when when we first moved here, our neighbors you can just join they're just join their internet. It's like yeah, we had to specifically stop ourselves from dialing in automatically to this.

Researcher 14:53
Because I had no password, no password on all I had no password. Yeah. Okay, that's fine. Thanks. Then presumably on your home Wi Fi setup you never do you ever change the password or was it just as it

Participant G 15:08
is the most complicated one that comes with comes with a

Researcher 15:11
device? Yeah, yeah. But uh, you would know you'd that would only be shared with with people you knew or family and you wouldn't be shared with anybody you didn't know. Okay, and would you say both for your personal devices and your work devices? When you go out and you go to the I don't know, hotel or cafe or airport or whatever? Would you would you use those over public? Wi Fi?

Participant G 15:41
Um, I don't tend to with my work. If I'm going with if I'm going on with work, it's with work, I might write you. But if it's not with work, um you get to the airport I wouldn't. And then if I'm, I felt often struggle on my phone anyway to hook into airport Wi Fi. So I genuinely do you know, he was that when you use your own data, however, yeah.

Researcher 16:11
Use your data on the phone.

Participant G 16:14
hotspot, my phone to my laptop? Because I've always I've often struggled.

Researcher 16:18
Right? Right. Is there is there a reason why you'd like if you go to a cafe whatever without other you say you wouldn't necessarily use that cafe.

Participant G 16:27
Yeah, I wouldn't. If I was an account, I would be the only place I've ever considered doing is if I was in an airport, right with work. Otherwise, I would just use hotspot my phone if I needed to. I don't I don't like using Wi Fi in that situation.

Researcher 16:40
What about your way of business in a hotel would you then use the hotel Wi Fi? And when I say when you are at the airport or using that Wi Fi network at the airport or using hotel Wi Fi network? Is there any activities, personal activities that you wouldn't do over that network?

Participant G 17:01
You would only do it if it was for sport. Work for what

Researcher 17:05
you were doing. You didn't do any banking or any purchases online purchases or?

Participant G 17:11
No, no? No. Okay.

Researcher 17:18
And okay,

Participant G 17:22
actually having said that, though, I did try to download a book on you know, on the app that comes up on iPhone books you can download, right? I have purchased a book using an airport download using their data to download right.

Researcher 17:43
And the are you influenced by the size and popularity of apps in terms of what you use or as in? Do you go okay, well, that's widely used app so therefore is it Yeah, that's the use. Good or do I do on camera? I meant d go actually, well, I guess it's only a small staff was going to be less subject to

Participant G 18:05
I, in terms of my apps on my phone, my phone. I just don't know, we've never had too much data. So I've only got limited apps on my phone. So I've got Twitter, Instagram, banking to banking apps. Messenger. That's That's it. I've got nothing. So I actually don't like getting a one button podcast. But I don't really like having because I use my work phone. They don't really have apps where's my husband's got pages of apps and the children the same? And they don't seem to have any rigor in what they download. But I don't just have key ones.

Researcher 18:47
Yeah. Does that give you concern because you're effectively on the same network as home with them.

Participant G 18:53
No, we wouldn't think of it I wouldn't think it was because I don't I mean, I just don't do that thing anyway, and I just don't like being that connected. Yeah, I think and also because it's a work phone, so yeah, yeah. xxxx. xxxx has like they're on Instagram. It's north of the schools. They're on Instagram and Twitter. Right. So that's another way I need to keep in contact.

Researcher 19:22
Okay, so they're on your phone because it's because of work or

Participant G 19:26
work and children and children a way of being in contact and knowing what's going on here. Okay.

Researcher 19:33
And have you ever been, I guess the victim of a cyber attack?

Participant G 19:38
Well, at work, we sometimes get dodgy emails come through but we have we often have to do this anti cyber cybersecurity training. And we there's a you know, a fish. Everything is a fish is a fish. You click on this fish. Yeah. So then we if we think that's come out, then we report them, right. So they have I have had them come through but you just report them. And normally by the time they come through, we've been warned about them. My husband

actually had his sorry, this is my site. Sorry, one second my children. Okay, done Yeah, so my husband he got his Hotmail, Yahoo Hotmail hacked, right? Yeah. Does he Yes.

Researcher 21:08
Does he know how that happened or?

Participant G 21:10
No. It just obviously started that sending out weird emails to people and people said I think your Hotmail has been hacked. Okay.

Researcher 21:18
You've not experienced that?

Participant G 21:20
Know? Touchwood I've had plenty of friends that seem to have had their Facebook accounts. compromised, right? Yeah, but not me. The only time I've ever been victim to anything like that was when I was in Sydney and I had my credit card cloned. And you now how that happened. What caused that? Yeah. It was in a that was in a taxi. Right? They pinpointed it. Yeah, right. Yeah. And so that would have been with the device they used.

Researcher 21:50
Okay, so the device used in taxi basically to pay what was a would have cloned it. Or something like

Participant G 21:54
that, or? Yeah, yeah. So in the morning, I remember going into the morning I'd only spent $200 on my credit card because it was stacked up there. You know, the year that month, and then I for some reason, went down that later on that afternoon to then check and there was only $200 available and that taking the credit card and book flights and gone to the and gone to the fish markets. Interesting. In that instance, I did get all my money back. Yeah. Yeah, that would probably been about 2000. Or maybe I haven't.

Researcher 22:29
And in terms of when you do like online shopping, which they do more online shopping now as a result of COVID or

Participant G 22:36
so recently, I've just done a couple of purchases, helps get things for the house. And then we do online shopping for countdown, but I'm not really a big shopper and if I am by Judy shopping, I actually like to go into the store.

Researcher 22:55
And if you do online shopping do you use the same credit card or use or debit card that you use for anything else or

Participant G 23:02
Yeah, yeah, okay. I don't ever say my credit card details. Any credit card details we've saved are actually for countdown. And I think they're saved in in Air New Zealand. Okay, otherwise I input them all the time. And you would use a credit card versus a debit card or you don't have a debit card actually who's got the credit? Card? Because oh no sorry, like my credit card I can use but actually for the school so when I'm making payments for

Jordan on school I'll use the I never know what's what it comes up and he use credit card or you can go in and just basically a direct debit transfer. So I don't have a debit card but I the direct debit. Some of the providers have that facility where you can do it. Alright.

Researcher 23:49
And okay. So in terms of cyber attack, so How easy do you think it is to spot attacks? Like you know, you talked about cyber training at work do you find it easy to spot phishing attacks or, or go

Participant G 24:06
work we have these regular trainings, so they will come through and you're supposed to check the you know, the end of the email, because the start might be quite similar. The end might be a bit strange and then the one at the moment, is that the post, we're delivering a parcel, you need to click on here. So that one I need to be careful with because recently except for what a few things that are being delivered. And that would be why not keep an eye out and I did worry my parents in the UK because they had something that was delivered on and it was from the post office saying you need to go in and pay this credit card because these they haven't paid enough postage. So my dad actually did that. And we thought oh, no, you've been had. But as it turned out, it was actually one of his cousins who sent me a Christmas card and they forgot to put their stamp on so that was a legit case. But then interestingly, a month later, he received something else same thing and this time instead of just paying it their ticket into the post office and that was a scam, that there are pretty much identical. So at the moment, if something comes through I will without opening it trying to look at the end of their email if I think it's to a gene but I know somebody's really looking out for it to be honest. Any courier companies? So I spot it. I don't know. I'd like to think so. But they are quite clever.

Researcher 25:39
Yeah, yeah, definitely very clever. So you talked about training at work. So you get cybersecurity training at work?

Participant G 25:46
Yeah. So often there's like a lot of online module that we have to go through to.

Researcher 25:50
Okay, so it's regular regular training. I have to

Participant G 25:53
guess, based on the latest info, I guess coming out. Okay.

Researcher 25:57
All right. And so is that where you get most of your learnings from? Yeah, but presuming that training is focused on protecting the company, as opposed to protecting you individually? That's right. Yes. Do you get any learnings for any roles or any other companies or any anything else or in terms of well, I

Participant G 26:13
might get emails in the bank saying, We will never ask for your pin and and then there seems to be more attacks that I know of in the UK speaking to my parents like the phone call one I mean more so when I had before my grandma passed away because there was definitely targeting the elderly on that and will get text messages. You know, quite often I'll

get a text message and I just delete them. Whether or not that's text or WhatsApp or phone calls me just getting a no not to answer or donate them, right? Yep. Yep.

Researcher 26:47
And as well as the training do, do you have I guess, does the organization provide guidelines for how how to behave sub from a cybersecurity perspective or in terms of what you can and can't do or what you should or shouldn't do? Or is it more on the training that that's delivered through?

Participant G 27:02
Yeah, well, that's why when I'm away, I'm not quite sure what the policy is at the moment actually around dialing into a shared Wi Fi like, I think if you're in an airport, seems to be that I would use it there if I was on work. But other than that, I will tend not to go on to any any Wi Fi generally. And I don't know whether or not that's anything new is perhaps when I first started work and going and using laptops around the places just how not knowing how secure it was to go use other Wi Fi stuff. Yeah, I don't know. Not too much as

Researcher 27:48
too much. Yeah. Raining, would you would you so why would he use the airport or not another one.

Participant G 27:58
There's lots of business people sitting

Researcher 28:01
right so you think it was set up was set up to support the fact they would be used by business travelers?

Participant G 28:06
Yeah, yeah. It's just seems more renowned, renowned area to do it. Yeah. And I guess you're putting trust in them that they're reputable company that they'd be trying to offer a safe secure Wi Fi. But obviously there would be a limit to what I want to access. Right. I wouldn't begin if I was had anything extremely confidential. I wouldn't be doing I wouldn't be doing that. Like I would know I generally don't go on my laptop in an airport. But I'm just saying, when we went skiing last year, I had to get the names of minutes and set out. Meeting Notes. out before I went so I went on and said that but there was nothing I wouldn't be going in and accessing confidential information on a shared Wi Fi anyway.

Researcher 28:57
Okay, so you you you be conscious the fact that actually I'm on I'm on a public Wi Fi network. That's why I'm not I'm not going to do anything that's strictly confidential,

Participant G 29:05
or whatever. Yeah. Just like you wouldn't take a file and leave it you know, hard file with you and leave it anywhere.

Researcher 29:12
Okay. And cover that. In terms of, say we talked about you mentioned trust that in terms of trusting, so how does trust play get does trust player has an influence on other aspects of how you behave online or?

Participant G 29:33
Yeah, so our work. The second you could perhaps you might be searching for something and we have restrictions in terms of what we can or can't access. So it's quite a bit it's quite strict on that basis. And from a from a trust perspective as a worker, I've got a I've got a laptop, but I would just generally just use for work use other than, like, I might make a few purchases at all. Look, you know, read the news. And then you want to say reputable companies that well known companies that might have a sale I might buy something online, but I'm not buying from spirits places or accessing anything that's not well please i trustworthy just the normal known right news outlets or companies that I

Researcher 30:24
purchase from right so no, no known device known known organizations. Yeah, yeah. Yeah. Yeah. Okay. And you know, when he obviously you said he would do passive stuff over the work network for laptop. So do you trust the organization you work for? Yes. Do you trust the people who work you? Yeah, yep. Yeah. Okay.

Participant G 30:50
And actually, to be honest on that, like I wouldn't, I didn't really use my own work left. That message across, but with the younger people coming in, I look around on my Oh, they're looking. They seem to be a bit, I guess. Yeah, a bit more. They use and what they access just way more than I would.

Researcher 31:09
Yeah, yeah. Okay. And sort of just going back on a couple of things like privacy, identity theft. Do you are you concerned about identity theft? Yeah. Yep. And how does that how does that how does that impact how he behaved both in touch with your home devices or your work devices or your or your online intake activity across both those dimensions?

Participant G 31:32
Yeah, so the fact that I've got personal information sitting on my desktop, probably not the best thing, but it is on a work laptop, I guess. But I'm more worried about with the children and my husband giving their details willin willy nilly. Yeah, and I own any when they're setting things up. I don't like them to use their real birth dates. I don't know. Yeah. Yeah. Yeah. Okay, so yes. I mean, I don't know how it all works, but you have to provide details or a lot of stuff. So, it used to worry me a lot years ago, but they you can't get away from it on a lot of things. When you're sitting. Yeah. Yeah, they want everything they want. A lot of the time, even if you're just sitting up a credit card you know that when your passport driving license,

Researcher 32:29
okay. And how do you how do you think yeah, do you think that you do you think your digital footprint online would enable somebody to who had a mind to it to steal your identity or do you are you careful about what he what information is out there on that?

Participant G 32:44
I don't, I mean, I I, I will provide personal information to record companies when I'm setting things up that I need like for mortgages credit cards, banking, that kind of thing, that NZTA, Waka Kotahi, that kind of thing. So there's definitely a digital footprint there in terms of social media in general, things like that. I don't tend to give away much of my details, or as little as possible, and I tried to use the security settings so that not you know, it's not open to anyone so with Facebook and Twitter and Instagram, like I'd actually don't actually post

anything really ever and it's all limited to only people that know me can be the view stuff or they have to ask the invite they have to ask for me permission to have to give them permission to see my staff Yeah, so that so that they will be quite limited, but my information is definitely out there.

Researcher 33:54
Okay, that's fine. And do you ever worry about device cameras about

Participant G 34:00
stuff so because I like listening to podcasts, and if I'm watching tap, I will not home? To get a piece of tissue over the camera. Right?

Researcher 34:11
What about microphone about microphones?

Participant G 34:14
I don't actually know somebody sent my face but definitely my laptop and it is listening to me. Because there's so many things that pop up I don't know think about the microphone quite on my phone. Actually. I say they can't say for example, on Twitter or anything like that. It says they can't access my phone. There's like photos and they can't access my microphone. But then when I go to do something because I want to send something to my parents on Messenger quite often they'll say oh, we can't access your photos. So give me you need to give permission then I have to remember to go back in right. Okay. But my microphone must be on because often I get something pop up and I might although it's been listening to me.

Researcher 34:55
But you'll cover up the camera occasionally when you Yeah, yeah. Okay. Okay, and what about so how would you say that your your when your actions match your intentions in terms of cybersecurity. Doo doo doo doo doo act? Do you act exactly how you want to act or do you have intentions that you don't necessarily mean?

Participant G 35:21
I think I am quite paranoid about stuff. So I think I am cautious. Yeah, I think I am cautious that I cautiously I'm always making sure that everything's logged off or logged out. I don't access things that I don't think would be appropriate. I say, Yeah, I do think I try to blow your mind with how paranoid I am about people accessing data. But yeah, but But having said that, though, as I mentioned, I've still got my information with a lot of organizations.

Researcher 35:58
Okay, and do you think your approach to that has changed as a result of the pandemic and working from home or you said obviously, you work from home? Let's say it doesn't that's probably not a relevant question.

Participant G 36:13
Well, I consider my home the home environment digitally to be just as safe as my work rightly or wrongly, right? Yeah. So I don't do Yeah.

Researcher 36:27
And in your home environment, do you say when you go and work from home, does your do your work devices or do your home devices have like auto locking mechanisms where

they just lock after us and yeah, yeah. And you would automatically when you've you weren't sitting at your laptop or your phone to automatically have it locked?

Participant G 36:42
Oh, yeah. Yeah. There's nothing it's ever left open.

Researcher 36:46
On right even in the home.

Participant G 36:49
Yes, same settings.

Researcher 36:50
And is that is that because you choose to do that was that because work for the Web Devices work

Participant G 36:55
that's been set up.

Researcher 36:59
And and how do you you know, how do you think we How do you behave in terms of things like you know, forwarding emails or opening attachments or using USB sticks to transfer files between devices and

Participant G 37:13
yeah, I don't use USB sticks anymore. I do. I would forward emails with attachments. But the attachments will be work generally work related. Yeah, so I don't when you say attachments are within

Researcher 37:32
somebody, maybe it could be a work email. It could be. It could be a personal email. It could be you know, it could be any, any sort of attachments. What do you what do you think, you know, work, you might say, well, you know, there's work attachment. So therefore I know where it's coming from. And therefore

Participant G 37:48
I generally know where they come from, and we have quarantine. All our emails go through a quarantine and sometimes I will get stuck in quarantine you to go in and look to see whether it relates them. So in terms of attachments, I don't really send much around to be honest Yeah, if I'm gonna do a thing, I might send a link or my as text message to something if it was my personal note so like on Instagram, I might just link I wouldn't I don't really forward attachments, search

Researcher 38:21
and opening attachments. Will you be conscious of like, well, I know where that's I don't know where that's

Participant G 38:25
because yeah, I would only quite quite to the detachment so it's obviously hoping a lot of attachments with work but it coming through from you know, please find attached sheduled

or quantities please find a text drawings. It's it's clear what they are. And then in a normal format, appropriate format.

Researcher 38:46
Yeah. And and in terms of the home network talked about the home that we trust. So what about what about the fact that other devices are connected so like you got smart might have you might have smart TVs or smart personal assistants like Alexa or you know

Participant G 39:04
anything like this, we don't have Alexa. We don't have a smart TV. We, we we haven't set up for that yet. We've done a renovation but we have it so we've just got anything we might watch the laptop and hook up to the TV. It's it's quite nice with basic really,

Researcher 39:19
what about smartwatches and fitness bands and stuff like that? Was that sorry? Smartwatches or fitness bands or Old? Old traditional traditional one? Yeah,

Participant G 39:30
yeah. All right. No, I don't I don't want to tell me that. I'm not doing what I need to be doing. We, I mean, the children would, would be more into that kind of thing, but it's not really Yeah.

Researcher 39:46
Okay, so you're not concerned the fact that your house network is because you're not much connected to it. So therefore, you started using it, I suppose primarily for phones and laptops. personally.

Participant G 39:54
Yeah, I generally we use our home that work is generally used for me working from home, the children doing their homework, My husband working, doing some work at night, and then streaming they own or Netflix

Researcher 40:10
Alright, I think that's it, that's my question is actually. Yep, I think that's all. Thank you.

Participant G 40:20
Thank you. Well, if you haven't asked me one. Ask if you ask let me know.

Researcher 40:23
That's really interesting. Thank you. I'm just gonna, I'm just gonna stop the recording now.

Participant H

SPEAKERS
Participant H, Researcher

Researcher 00:00
We'll get into it okay, just testing seeing if that's recording when you say something, just Hello.

Participant H 00:08
My name is xxxx Good Alright, looks

Researcher 00:12
like it's working fine good. Okay, um so I'm gonna start with devices. So you know in your personal life and your work life do you have? Do you have both personal and work laptops and phones or do you have separate ones or do you combine ones or what what devices do you have that you use on the Internet?

Participant H 00:29
That's it combine but definitely with all of our all of our devices and make sure that they're pretty secure anyway. So without personal it's a work of or personal reasons. I secure them appropriately. Likewise, on my home network, any devices that I don't trust, segmented on a separate network with firewall protection between them as well.

Researcher 00:54
That's fantastic. I've found Do you have would you have a personal phone and a work phone or just just just combined? combined? Yeah. And is that what the work provided one, or personal one,

Participant H 01:05
that's the one where we're a be BYOD environment.

Researcher 01:08
Okay. And same with laptop is that you have a laptop or tablet is that I work device or a a personal device.

Participant H 01:16
That's a personal device, but I tend to use a laptop of mine specifically for work purposes right so and then I have my PC which I use for other purposes.

Researcher 01:29
So you have a separate laptop they use for work purposes. Yeah, yeah. All right. Sorry. Okay, and so that separate laptop that you use for work purposes. Do you do any personal activities on it or

Participant H 01:44
not? Really not other than maybe surfing the net but I've got more than enough devices to keep a good segmentation between work and, and, and personal use.

Researcher 01:55
Okay, so you tend to you in terms of a device use you tend to segment your personal use annual work use between the device even, is that the same for the phone or?

Participant H 02:04
No, I just have the one thing, right it really having said that it is protected with work, work level security.

Researcher 02:12
Right. Okay. Use that one phone to do work activities. Plus, also you might want to do online banking on that. Yeah. What about what about online shopping where you're extending or inputting credit card type details? What about social social media or stuff like that on

Participant H 02:33
LinkedIn, off other social forms of social media, so I only really use LinkedIn which is pretty much work related anyway.

Researcher 02:41
Okay. I'm sorry.

Participant H 02:45
Know tick tock.

Researcher 02:47
Tick tock. Yeah, I've personally never use tick tock.

Participant H 02:52
Something's not secure enough. Because I'm also the xxxx for the company I work for something's not really secure enough. for work purposes and don't use it for personal personal use. Okay. All right.

Researcher 03:06
And you said earlier, you've got a specific laptop you use for work that you don't say that laptop you didn't do any, any personal banking on it or any online shopping on it or anything like that. That would just be for work. stuff.

Participant H 03:18
There's probably nothing to stop me from using for personal use, but I just generally wouldn't,

Researcher 03:22
ya know, and it's more about it's not not a question of guess what wouldn't stop what would stop you and I was questioning whether you would or wouldn't it's kind of more behavior based in terms of actually, what I'm trying to understand is based on this research is actually how people behave in terms of you know, starting with the devices they use, and then moving on to the networks and the apps and stuff as to you know, you're you obviously work in the industry. So you're, you know, you've got a very clear view of actually where the risks are, but

Participant H 03:47

sort of make it a bit simple. Most of the personal use online shopping and that sort of thing tends to be via the phone,

Researcher 03:53
right? Yeah.

Participant H 03:54
Okay. All right.

Researcher 03:59
I guess but I guess they'll move on to networks I suppose. On your devices, I you. So with COVID and with a pandemic. Are you working more from home now than you were before?

Participant H 04:11
I work 100% from home, okay. Yes, occasionally, I might go in for a client meeting or something along those lines, but I refer to my home office here. It's been the xxxxxx office for four subsidiaries, which is wherever,

Researcher 04:22
right Okay, and so that's basically you're connecting into the company workforce network by or your home Wi Fi, your home network, basically,

Participant H 04:30
of sorts. company basically has a Cloud First policy and basically everything's on the cloud anyway. So Melbourne office is really just a landing pad with internet access for people there's there's no servers or infrastructure running Alright, so having said that, we take the home security, home network security very seriously. At least I do as the xxxx. So for people in what we call a control group, which I'm a part of, which is part of the company, we actually fund and provide prosumer grade networking infrastructure for the home. So, right, we don't trust the cheap $20 routers that your internet service provider gives you.

Researcher 05:19
Right? So so as soon as you start as a up in the site, so fair to use that minimum standards for people working from home that they have to have certain level of security or a certain level of routers or, or, um, yeah,

Participant H 05:33
so basically, when they start part of the control team, they fill out a survey detailing what the home network setup is, and then we'll determine pretty much what we would provide or what we didn't need to provide. So for members of the sub security team as an example, we tend to send them a prosumer grade, router access point. And everything else that way they've got a high degree of security at home than they would otherwise. Right.

Researcher 06:05
Do you think that he honestly, this is my viewpoint ready? Do you think that's, that's specific to the company you work for now? Or do you think other companies will will adopt similar?

Participant H 06:18

Most companies unless they might actually occasionally provide something but I think that it's something that a lot of organizations aren't really aware of, or or prepared to do something about. I think it's kind of in the too hard basket. Likewise, I think for a lot of companies, it's like crossing that boundary between your home life and the work life so those maybe shy away from it. But at the end of the day, in either routers you're going to buy at the local box stores or your internet service provider gives you that junk, that absolute junk. You know, a lot of people will buy them you know, they'll say on the box has got a firewall but they won't really understand that, you know, 12 months time, you're not going to get any updates for the fall. Because they'll just stop. Likewise, in mobile phones. I mean, you know, androids up to three years of buying them. You're not going to get security updates. Apple's a little bit better. So we we definitely because we tend to, you know, we're all over the country and we're all working from home pretty much. We actually take the home security more seriously. We also have a very different approach to cybersecurity awareness within xxxxxx. So he focus on personal Cybersecurity Awareness rather than protecting the kamberi and protecting clients. And we find that that's much more effective than developing a proper, secure mindset, because awareness training gets much more personal. And it gets people thinking about their own personal cybersecurity posture, which I think is more effective than we need to do this to get ISO accreditation or whatever.

Researcher 07:57
So So that's interesting, because I've so my question is come on to Okay, where you know, where have you gained awareness from or does the organization you work for providing cybersecurity training? You know, what you are, and one of the questions about that is actually well, in most cases that I've come across, actually, there are some companies providing cybersecurity training, not all of them, that cybersecurity training is focused on, on protecting the company data, you're saying you're the cybersecurity that you organiser to providers actually focus on the individual and therefore making it more real for the individual in terms of

Participant H 08:30
even have have tips like you know, if you've got a young kid don't have the name splashed over the back of their backpack, right? Yeah. A lot of it is about you know, I refer to a lot of the training that needs to be done is basically it came the workforce with 21st century life skills, right. So and we find it's much more effective to actually take it from that angle. Because you know, people come home and help you know, that router I got from my internet service providers. Crap, or, you know, I've got this vacuum cleaner that has a microphone on it for some reason, and it's made in China. Maybe I don't want that on the same network as you know, what I'm using to access my banking sort of thing. Yeah. And that way we're having them and equipping them for the right mindset, not because the line between home and work, particularly when you've got a workforce like ours that is working from home, it is blurred. It has to be blurred. Yeah, we went down the other road, and we find it's much more effective.

Researcher 09:29
Yeah, that's really interesting. I haven't really come across that much. Do you do you see other than your organization? Do you see other organizations not Not, not other organizations who work for DC either other bodies or retailers or companies are actually being proactive in providing that that personal cybersecurity awareness that you know bring making it real for the individual or or no

Participant H 09:54
unfortunately, not, I think a lot of Cybersecurity Awareness tends to be done by you know, sort of the IT directors and that sort of stuff. And, you know, that sort of level of thinking, you know, they've got their hands full, you know, with you know, just what they've got to manage. And unfortunately for a lot of organizations, their idea on cybersecurity awareness and cybersecurity training very much focuses just on fishing exercises, which you know, time and time again, I'm seeing over and over again, you've got 20 to 40% of people who are always failing the fishing exercises, no matter how much these crappy computer based training things are put on. And that's actually an area that we focus on quite heavily. We actually have a human centric cybersecurity capability looking for 60 which is very much about you know, taking much much more of a human centric approach or such socio sociological approach if you like, which is tackling things more at the root cause than the symptoms that we see time and time again, which are fat. Let's be quite clear about it. It's the approaches that a lot of organizations are taking

Researcher 11:08
our family are talking about, sorry.

Participant H 11:12
A lot of the approaches taken by organizations that we see are failing,

Researcher 11:16
right, and they're failing because

Participant H 11:20
they're failing because just like a lot of things in our industry, they're focusing on the symptoms rather than the root causes. If we look at the cybersecurity as situation that we have in the Western world, particularly here in Australia, because we are very much behind the rest of the world. The you know, having any one's looking at the root causes and the root causes are human factors and human behaviors. And the other one is to put it bluntly, crap software, and the insecure software development practices. In fact, we're in the process of building out a Software Assurance capability to tackle that second, start to tackle that second aspect as well. 80 To 90 Tonight, we're seeing organizations where 80 to 90% of their software isn't actually their code. Software development is becoming much more about integrating libraries and API's together than actually writing code. And they're not looking at the security of the code that might run a pin test at the end, which is looking for known problems. And you know, some of it's quite scary, some of it some, and I've made trains running around the airports to scare the birds. Yeah, yeah. And, yeah, that's a huge issue. Number two root causes. But unfortunately, when an incident happens, as I'm sure you're aware, most people don't. Most people struggle to get get down to a three levels of abstraction level and four or five. So that might come down to oh, there was a vulnerability that wasn't patched or there was a vulnerability that couldn't be patched. And that the controls that should have been in place failed, but they really get down to the fact of why did that vulnerability exist in the first place? Yeah.

Researcher 13:04
And when you mentioned you said, obviously, the root cause a lot of root causes are down to human behavior. Would you highlight any particularly human behavior that you that you would click to

Participant H 13:13

you just got to look at the People's propensity, propensity to click on links. Social engineering is, you know, obviously, quite effective these days. And it doesn't help that organizations are still using insecure mediums like email and in particularly SMS and multi factor authentication. Right, the SMS is never going to be a secure form of communication that never was designed to be so you know, those sorts of issues, but at the end of the day, you've got a lot of people who are not digital natives, who, who you know, view it as it is problem in fact, we even encounter quite a lot of boards that view cybersecurity as our that's the IT departments problem. That's a responsibility. We'll make it within when in reality, it is actually what the board

Researcher 14:06
well, and it's not just an IT issue.

Participant H 14:10
That's exactly that's the issue is actually it's not around ICT, firewalls and all that sort of thing. It's actually more than digital safety. So, if we look at it this way, you've got cybersecurity which is much more of a technical level wrapped around that. That's a subset of information security. So you know, standards, that sort of stuff. That is a subset of security and a lot of physical security based organizations are not necessarily the most cyber aware all of these are subsets of digital safety and something that I think New Zealand is doing a better job of than Australia at the moment where they've been quite clear that boards need to treat it treat cybersecurity as being at the same levels level as occupational health and safety.

Researcher 14:57
Yeah, yeah. Okay. You talked about the home network, and I'm getting a sense that some of these questions would be kind of a little bit irrelevant. You say you're because you've already said that you you've set up your home network with you know, cybersecurity grade or you set it up to be a secure network as as as secure or more secure than work. So you've not just taken the ISP router that's been provided to you and plugged into that and you know, you've probably not got the post it note on the on the fridge with the password. What about your

Participant H 15:29
sorry, not with the camera around that's for sure

Researcher 15:32
No, no. And the ID so in your home environment in your personal space with family and friends do you? Does that there's access get shared around with family and friends and what about kids and visits friends, kids and visitors and stuff?

Participant H 15:47
I have a guest portal for you know if I have guests around that want to access it, and I've got a nice mock up of an FBI warning thing to sort of freak them out when they join. And yeah, I can say that the device, all the devices on our network, if they're secured as they can be and for the ones that, you know, we can't secure effectively that are basically in the sunburn of a of a on their own sort of separate network, but they're not able to communicate with each other and maybe they might have some internet communication if they need, right.

Researcher 16:22

What about typical home devices? So you know, you know, some of the questions are asked in terms of some of these discussions around Okay, well, you know, you're in the old world he had yet you haven't PC that's connected via modem into your telephone line. And it was very simple. Now you got a home network if you've gone and bought this router, or you've got one provided by your network provider, you've basically connected to your Smart TV, your Alexa you know digital assistant, you've got your smartwatch or whatever you've got, you know, got all these devices all connect to the same network. How do you think about that from a security and behavior perspective are you know, are these

Participant H 16:56
completely insecure setup? You know, if you've got TV that's probably not getting updates more than a year after you've purchased that you've got your you know, your cheap Chinese blimmin Fitbit thing or something along those lines or even you know, we've got a Chinese robot vacuum that for some reason has got a microphone on it. I can't see the purpose, robot vacuum and you know, having everything on the same network is just insane to me. It's just basically increasing your attack surface exponentially. So you know, we have an my home network aside from the guest network. We have three three networks right and purchased red, green and blue. Sorry, red, green and orange. Red. It's basically they can communicate to anything on the network other than access to the internet. And that's trouble. They can't even access, communicate with other devices. On that red network. Orange, you know, fast Internet access, maybe a couple of holes of printing also firewall rules for printing or something along those lines, and then the green network, which is, you know, basically for work purposes. And when we're for prosumer grade devices that we get, which actually aren't they're much more expensive than, you know, a lot of the routers you can buy, you know, so all software defined networking. So once you know what you're doing, it's actually quite easy to set up and configure and you know, it's it's still pro semigroup but as as I explained to customers all the time, and even internally you know, a lot of this stuff is like being chased by zombies. You don't have to be the fastest runner but you don't want to be the slowest so by having process integrator still a hell of a lot better off than what most people are. Yeah, yeah.

Researcher 18:52
And what about say, say your home environment and your work environment are you know, equally secure in terms of how you set out what about do you wish probably stupid question but do you ever go and you take your either your personal devices or your work devices do you go and do activities from a you know Wi Fi in a cafe or at the airport or in a hotel or had

Participant H 19:17
only with a VPN and only use going from my mobile phone?

Researcher 19:21
Okay, so you you don't you don't go you don't get connect to the Wi Fi that you'll connect your connect to your your hotspot on your phone and do it that way. You wouldn't have to connect to a

Participant H 19:33
Wi Fi in that way. So McDonald's Wi Fi guys

Researcher 19:37

Wi Fi Yeah, what does what Starbucks Wi Fi or whatever or you know, you get you take your work computer, you go and sit down and get a coffee you're gonna do an hour's work you you know, I'm gonna show a lot of people do this. They just connect their work device to the McDonald's Wi Fi and and then they're sending stuff over, over that over the network.

Participant H 19:53
And we actually covered that and our cyber security awareness training with people as well, because man in the middle attacks are too damn easy to do. I mean, I could do it with the Raspberry Pi and see, yeah.

Researcher 20:05
How do you have a view as to how successful that that training is in getting those messages across?

Participant H 20:11
It's hard to measure. We've we had to sort of pick this the slot off as part of a major cybersecurity overhaul when I started there wasn't actually much in place at all. And served over the last 12 months we've we've sort of rolled it out. But definitely, you know, we've got with we seem to have quite a good culture here. So, you know, it's an example a couple of months ago, one of one of our guys stumbled into a watering hole and so, the first thing he did was get in contact with us and disable us network access run. So one of the key challenges most organizations have is even when they do have near misses or even breaches they don't know about until it's too late. Because people are afraid, you know, they'll get in trouble or they'll be ridiculed or whatever. We're very much showing the much more realistic lines of let's face it, there's not a person on the face of the planet if someone wanted to get me even just with a phishing scam, they would get me right. The reality is on the dark web, and this is as of seven years ago. So it's probably cheaper now, for 10 grand, you could pay some hackers who will within 24 to 48 hours they'll have they'll provide you with all the information on an individual anywhere in the world. They will know that you're receiving an Amazon package and what the contents are and you're expecting it tomorrow. And this is a tracking number and you know, when people have got that sort of intel on you, spear phishing and that sort of thing becomes absolutely lethal. So the reality is, it's everyone's going to get done. But, you know, we're quite clear if he if you get down and we make a mistake. You need to get in contact with us straight away so we can actually manage the outcome because that's what it's all about. It's not about attributing blame or anything along those lines. It's about making sure that that mistake doesn't become a huge crisis.

Researcher 22:15
So it's not a say what I'm saying is that your your practice will come into practice. And it's not a compliance exercise or a a consequences punishment exercise in terms of you know, you've done something wrong. It's more a question of actually, these risks. exist. Please be open about it if you if you happen to get stung. You know, because yeah, because there are people out there doing this. You know, you could be the smartest person in the room and you can start miss, you can miss you know when when

Participant H 22:44
HCCs guys are doing some phishing tests on me they got me. Yeah, and I'm quite open with that, even with our clients, and that's the end of the day is if one of our systems safe, none of us are safe. And but in order to do that, it one has to have take responsibility. And

you know, as I like to say put the ego down. Help help us focus on the outcome because I don't care if someone makes a mistake, you know, the hope that they've learned from it, but someone makes a mistake. It's like, well, welcome to the human race.

Researcher 23:16
Yeah, yeah, no, absolutely. Do you like they do say that we learn more from our mistakes and we learn from? Yeah, yeah, absolutely. Yeah. And so talked about attacks. Have you have you been Have you been the victim of a cyber attack? Have you

Participant H 23:32
know, we have had a few near misses. And we are actually interestingly, quite a lucrative target because we're, again, it's something we explain in our subsidiary awareness training. We're a small organization, you know, got 45 permies and what 150 contractors, but we're dealing with some very sensitive clients, including defense so that makes us a very lucrative target from a threat actors perspective, their business cases, yeah. Okay, well, these guys potentially have access to some really good stuff that they would want. But they're also too small to be able to afford, you know, to spend, you know, hundreds of millions of dollars on cybersecurity, which makes us quite a big target. And that's one of the reasons why you know, a lot of our focus is on the human behaviors, because that is a first and last line of defense. Yeah. All the technology is there to support that.

Researcher 24:24
Yep. Yep. You You said you'd been you've been caught up by a phishing test or whatever, are you? Yeah. How did say what what caught your eye out? What what what did you learn from that? What was it very,

Participant H 24:38
it just sort of reinforced what I already knew. And that was a spear phishing test from people who already knew me, right? That and you know, our guys are pretty smart, right? But there's actually a very, very credible case that any graduates in psychology or sociology we need to make sure they're gainfully employed because if they end up with some of these three letters, we are all stuffed. They've got to write down to find out you know, even the time of day, you know, later in the day, when your cortisone levels are dropping, you know, all that sort of stuff. There are just so many variables and really professional spear phishing attack that make it very, very difficult for people not to get sucked in. Yeah, and it's very good at that.

Researcher 25:30
And you'd have to have your your personal behavior in terms of cybersecurity. Are you more worried about you know, financial aspects in terms of your banking or your credit card type details being compromised? Are you more worried about your identity or both? What drives what drives your behavior in terms of

Participant H 25:46
if your identity is gone all of those other things go and go with it

Researcher 25:48
Exactly. Yeah.

Participant H 25:50

So you know, identity theft would be a big one. Having said that, I'm also aware that if if the signs were actually there, and due to the context that we actually have, we would be able to get on top of it, not just for me, but anyone else within the company pretty quickly and effectively. You know, I'm fortunate enough to have an understanding, because I'm in the industry and that sort of thing. But to be honest, one of my big fears is actually more along the lines of, you know, a relative getting done or something along those lines. So some of you know, right,

Researcher 26:23
right. Yeah, yeah. But But personally, the way you say you say, I guess personally where you behave, honestly, and probably the identity theft, yeah. So do you know how do you do that? Do you like do you limit the domain? You said, you don't really use much social media than LinkedIn? Do you kind of limit your digital footprint or do you try to live it is quite hard to live your digital footprint these days. But in terms of what's out there, or

Participant H 26:48
I access the internet, therefore, I have no privacy. Yeah, my stance on it, but it's just like anything else. Just sort of try and reduce my exposure as much as possible. For anything financial, you know, a year YubiKey. You notice I've got it's very hard for an external threat actor to you know, push that button and plug it in. And so I tend to rely on that very good, good level of multi factor authentication. That are used for anything that's particularly sensitive. Yeah, okay. Apart from someone in Russia to you know, fly over here and grab this and push the button at the right. Right. Yeah. Yeah,

Researcher 27:28
that's what the physical become. Yeah, yeah. Well, it's

Participant H 27:32
interesting Riley, you know, even the same. Don't write down your passwords, you know, family friend set up on a farm in the middle of nowhere. They have a notebook and write all their passwords in their notebook. You know, the reality is, is it's probably quite secure. Government in the, you know, someone done already so Russia and North Korea, what are they going to do drive out there and steal and notebook?

Researcher 27:56
Yeah, yeah. What about so got it had a train of thought then I'd lost now. What about, say old mecanismo? You talked about stuff being out of date. Do you do you bother with antivirus software at all these days on on most

Participant H 28:16
all work devices within our company, we actually focus and recognize that, you know, with us being a cloud, only sort of organization, the biggest and being BYOD our biggest threats being the endpoints we have enterprise grade vulnerability scanning and we use BlackBerry silence with saw capabilities on the on the endpoints for our control team members. And definitely you know, sciences you know, clobbered quite a few things I've done. And it's good because it doesn't automatically then we investigate.

Researcher 28:55
And that's all kept up to date. And that's and that's what I needed for any device. Any device is connecting to your network to the company's network, because that personal because you have BYOD devices. So is that personal and work devices or

Participant H 29:07
that's that's work devices for the personal devices within the home? Basically, yeah, we have just consumer grade antivirus running on on all the devices that can happen. And for the other thing, other devices that don't, yes, we have a fair, fair Linux or something like that we have them automatically updating to keep them current. For the other devices. It's pretty much left up to the vendors sort of upgrade upgrade cycle. But, you know, for those sort of IoT type devices that we're talking about there that tend to be on the red network anyway. So you know, the exposure, the blast damage from that.

Researcher 29:48
Yeah. Okay. And you also mentioned earlier in the call, you mentioned cameras, do you? Are you concerned about cameras on devices on laptops?

Participant H 29:56
Oh, yeah. And, in fact, made sure everyone in the company actually has just a physical slider to put over their camera on their laptop. You know, I don't have Amazon Alexis running or, or anything along those lines, or they, in fact, I have forgotten to turn off the microphone on my phone here. I think wouldn't come as any surprise that mobile phone phones are listening in on us all the time. So, in fact, that's probably something I need to do with the refresher training course to help people that you know, turn off the microphone on your on your cell phone, or you might find priorities dropping a concern my biggest, biggest bugbear at

Researcher 30:38
a much more concern about microphones or cameras, or is it equal or

Participant H 30:43
equal. I mean cameras, you know, that you're visually you know where they are, right? So it's easier to, you know, make sure that like in this room, there's only one here and one on the phone right? For me, actually, it should the microphone listening and there have been far too many times. I've had conversations on something quite obscure, and then finding the advertising fee on my on my phone and starting to talk to those sorts of issues. Said regardless of what the manufacturers are actually saying, I do believe these phones are listening. Right? Okay. Yeah.

Researcher 31:21
Okay, we talked about D in terms of apps, D does that does the terms of the apps you know, you've already talked about but you don't do much on on social media. So but in terms of the app, see, would you where you would use Are you influenced by the size and popularity of apps or or as in would you not without the

Participant H 31:42
heart of part of what it is? And you know when I'm talking about apps on phones, a semi many on phones. Yeah, I'd look at the popularity rating but I'd also look at the Security Security side of things as far as you know, doesn't really need camera access or access to my file system.

Researcher 32:02
I mean, would you would you would you choose like I guess there's a good there's a there's a couple of couple of dichotomies here. One is actually some might say, well,

actually, I won't use the very popular app because it's, it's popular, that's what's more likely to be a target and attack versus I'll use a smaller app, but then they set their security model what the security might be weaker. For example, it's a bit of a catch. 22 doing your damned if you don't, right, yeah.

Participant H 32:29
But what we actually recommend to all of our employees again, as part of the training is your phone and your laptop and everything else. If they're outside of the control group, they have admin rights. On the machine, which is, you know, every couple of months. Just have a reminder in your calendar to go through and start uninstalling things that you no longer need or will use on your phone and on your on your PC. Right. If you don't need it, get rid of it.

Researcher 32:58
Yeah, okay. And how does how does? How does trust play into how you, I guess how you act or how you behave from a cybersecurity perspective? You know, do you if you trust somebody or you trust an organization to that, does that affect how you behave or are there other Do you categorize things as like, they're trustworthy, they're they're high level of trust or medium level of trust, for example, or

Participant H 33:21
In order for business to happen. There has to be a degree of trust, right? And definitely, when we're talking with clients, we're open and transparent and honest, and you know, we trust them. Having said that, we don't give them access to we have to share artifacts or something along those lines, have preferences to work, live off the land and utilize their systems. And that may mean that they provide a laptop, which you know, often happens, but we don't actually, you know, provide customers with access to controlled environments, in any way, shape or form. And, in fact, we've got safeguards to prevent that from happening at all. And for you know, the sort of gray area of you know, you need to transfer files between customers or something like that. We just have a, basically a zone that can be used for that. So I think provides your from a technology perspective provides your catering for the scenarios without creating too much friction, there's no problems as far as trusting people are concerned, you know, at the end of the day, trust, but verify, right, so And part of that we have to have to be part of that. Display level accreditation, you know, new new people waiting in the control team, if they're not already security cleared, we have to do the full background checks and get them through the clearance process and that sort of stuff. So So yeah, trust but verify.

Researcher 34:49
Yeah, yeah. And yeah, when he talks about exchanging files, presumably, you know, what, what mechanisms either Is that Is that done within the network or that's

Participant H 35:02
basically using you know, in our case, it's actually using a G Suite, Google Drive, and we just have a special google google drive that we can use to transfer data from customers rather than mailing

Researcher 35:16
so rather than say, you, you rather than you don't, your approach is not to email attachments, not to not to use

Participant H 35:22
my my possession or something that I'm encouraging others to adopt as well.

Researcher 35:28
Yeah. What about what about the old you know the the USB sticks that's been around for for a few years and

Participant H 35:34
silence and jumpcloud, which we use for identity and access management, we've got them set up to just clobber them that they're allowed by exception, right. But by default, you plug in a USB drive. It's not going to work. What you get, you can get read access, but you wonder why she know you're in a controlled environment. It's not going to work at all. Yeah, yeah.

Researcher 36:03
Okay, I think that's probably the areas that you'd highlight about not covered or not mentioned, or

Participant H 36:19
I mean, you know, even for smaller organizations, there are some really good options out there that are free that they can adopt. So I just mentioned jumpcloud, which which you use for identity and access management that's free for your first 10 users unlimited number of devices, right. So, you know, there are options out there, but part of the challenge that we have is there aren't enough skilled people, even in the ICT area, all right, for this sort of stuff. From a personal perspective, one of my biggest concerns as particularly small small businesses, you know, in Australia, New Zealand, you know, they've got, I've got an idea, and they're very, very vulnerable to ransomware. So that's one of the angles that we, you know, I have at the moment and others that I work with have which is more needs to be done to properly equip and enable the smaller businesses because they're sitting ducks. And you know, all this talk about, you know, make it illegal to pay ransom ransom. Well, you try and tell it to a sole trader, Trader photographer who their entire livelihoods gone. Right. And, you know, they're gonna be bankrupt. You're trying to tell them not to pay a $500 ransom. It's just unrealistic. Right? Yeah. And that's where I think collectively as a society, we need much more education. And, you know, real education for the population because we're not living in the 19 year round of 99. This is what I mean, your internet into the home and no one was even. I remember I was asking the question, but hardly anyone was like, Well, what impact is it having this much right and wrong information and behind going ahead, right. And everyone was just like, oh, yeah, let's get it done. This is cool, right? Well, yeah. Now we've got cyber bullying and all that sort of stuff. And these issues come up, but what was reactive biggest criticism I have of cybersecurity as it's predominantly reactive, not proactive. And the people who do work on the proactive stuff, so many levels of abstraction removed from what's visible. That struggle. Yeah. You talked about talk to you know, there's a application security credit bumping dealing with leftist Yeah, really good tackling things at the root cause. And yet they had a large client who course because they've been doing a good job. They were like, Oh, why are we spending all this money? Money with you? Yeah, how do you prove the security breaches? That never happened? Because of the work that you did? Practice?

Researcher 39:03
Yeah, no, exactly. Yeah. Yeah. Just one request. I want areas and tons of devices like your laptops or your ID in terms of access mechanisms. Now, do you have a preference

sort of, you know, are you mandated to use either biometrics or like facial or fingerprints or do you stop passwords or pins or what's what's the

Participant H 39:23
with with our control teams? We took it further than what the the DIS accreditation, the defense industry supply program mandated. So we've got the highest level you can have for a BYOD environment for that approval. So we have have control team members hooked into jumpcloud. They login is through multi factor authentication, either pushed to the phone, or if they don't have access to the internet. Using the YubiKey. And basically, none of them have admin rights to the machine if something needs to be installed or something along those lines. So log requests were private, given that admin rights to do what they want to do, or what they, you know, required to do. And yeah, I would say that for BYOD environment we're about as secure as we can be.

Researcher 40:13
Yeah. Will you pass me in terms of you know, how you how you log in like, is that do you property is your preference, like biometrics or passwords or pins not not for work for personal stuff that you do online or

Participant H 40:26
username? Password with multi factor authentication, since there's physical or mobile push current trusted app,

Researcher 40:34
right. Okay. And in terms of how do you your passwords, how do you use do you how do you do you use password management apps like keychain or stuff like that or,

Participant H 40:43
and in fact, as part of our program we've just rolled out the junk that password manager tool that control team members as well. It's actually quite good.

Researcher 40:54
So you basically would manage your passwords to that and therefore, as opposed to having a

Participant H 40:58
password manager for my personal use, but then we also have the jumpcloud one for IPS right. Okay. When somebody leaves we can disable that.

Researcher 41:08
Okay, so all your how your how you manage your passwords and how their updates that's all managed for your personal stuff. That's your your through your password management app that you have. Just for personal stuff. Yeah.

Participant H 41:18
Yep. Okay. And now Yeah, separate password management app for work purposes.

Researcher 41:26
So, you know, you don't have you don't have a particular preference for fingerprints, or biometrics or

Participant H 41:31
I hate biometrics. You know, if the data stored about my fingerprint gets breached, I've got nine other digits I can use. Yeah. It's the problem with biometrics, right? Yes. Yeah. If one of them is compromised, you can never use that finger again, right? Yeah. Yeah. Okay.

Researcher 41:52
All right. All right. Let's see some interesting insights. Agia. Just one more question. Sorry. One more question. Sorry. How do you for you I mean, I just obviously, you work in in Tibet. Do you think your your action is related to cyber Kareem match your intentions? Do you think you're obviously very aware of of the rest of you think you've you do all that you can in terms of of what's needed or?

Participant H 42:18
Yeah, and look, let's be honest, you know, not everyone practices, what they preach but having said that, I'm never along the lines of everybody must always do something. I totally recognize that people are human and there are always going to be some sort of exceptions. And that's why making sure that people's intentions are correct. And if they're informed and they're aware, they will do the best they can and to be honest, that's all you can really ask people. So So yeah, the main thing for me is, you know, if we take a scenario where somebody you know, does get breached, or you no clicks on something they shouldn't have, if they really want to get on my bad side, they try and bury it and don't don't bring our attention to it, then I'll get angry at them. Right. Because at the end of the day, I don't I don't care about their ego. I don't care about mine. Trying to minimize the impact on everyone, in fact, with our clients. You know, one of the things we do to try and pierce that bubble of diffusion of accountability, where people a lot of people in an organization be like oh, you know if there's cyber breach i t 10. B and under the pump, you know, that'll be their problem. You know, it's that they've got no understanding what they're talking about, because if you're on call center, you're going to be the one that's been going to be copying abuse from some customers have their private details breached it affects everybody. And people have to break out of this mindset, that it's an IT issue. It's a societal issue. It's everything.

Researcher 43:54
Absolutely. Absolutely. Yeah. Yeah, totally. As we said earlier, it's not you know, it's not the it's not the it's not the it is not the IT function, it's it's across the organization effectively

Participant H 44:06
Absolutely. And then you look at software development practices, which are just completely separate from the rest has been able to do what they want. Yeah. And that's a you end up sort of situations. I think it was up to us. Probably have to turn off the recording before this.

Researcher 44:20
Yeah. And I'll, I'll I'll actually stop the recording now. Actually. I think it's been very useful. Thanks, xxxx. I'll just pause it and now stop that

Participant I

SPEAKERS
Researcher, Participant I

Researcher 00:00
Right now recording Can you say something just to see if it's picking you up?

Participant I 00:08
If it didn't help you out where I can

Researcher 00:15
say something about something else, sorry.

Participant I 00:19
Um, look, what have you see how long has it been in probably the last week together with a telecom also good lord that is gonna be about three years ago. So it's been quite a while from that point

Researcher 00:30
to Thursday. Well, I left I left there in 2013.

Participant I 00:34
Yeah, Majid the same Yeah.

Researcher 00:36
So that's 10 years ago. Yeah.

Participant I 00:38
Sorry. Longer than that, because you've been here coming up through the year. So yeah, it's a long time ago. Everybody's gone their own different ways. I haven't had to catch up with anybody from the old Q.

Researcher 00:49
Does a grip on there's a grip on Facebook actually, that I can

Participant I 00:53
Yeah. A lot of friends of fives Facebook, so stay with right away.

Researcher 00:57
Okay, there you go. I think actually Kim students organized a catch up probably in June, I think sometime

Participant I 01:05
next week, right.

Researcher 01:09
And it's recording Yeah. I mean, it's a that kind of kind of sometimes misses some stuff, but generally does doesn't need to be okay. So if you just met just make sure you speak.

Alright, I'm gonna cut into the questions now. I think the first first I'm keen to understand is you know, do you have separate, separate personal and work mobile devices? And do you have separate personal unware either laptops or tablets or computers?

Participant I 01:35
Certainly separate PC laptops from home to work, but my mobile is my work mobile as well as my personal mobile. So we're at work they give you actually a work mobile. I've chosen to use my own personal mobile but then use work over that as well.

Researcher 01:54
Okay, so you your your mobile device, but it's working over when you're on your phone to work and over the the

Participant I 02:00
company? Wi Fi? Yes.

Researcher 02:02
Okay. All right. And so you have one mobile phone that you use for personal work use and you have like separate laptops or computers or,

Participant I 02:12
yes, separate laptops. from home to work. What's this work laptop does for work only, and nothing else? Anything else in terms of home life is on separate devices, whether it be a MacBook or whether it be an iPad,

Researcher 02:27
okay? And do you have audio or have at home have still have a fixed fixed home PC at all or

Participant I 02:35
not? It's it's basically all over things over Wi Fi. Okay.

Researcher 02:40
So so in terms of terms of the phone, so use that for both work and personal use, and yes, that's correct. Okay. And your work laptop? Do you only just do and use that for work use is that

Participant I 02:55
you said? Just consider it. Yep. Completely for work. Yeah.

Researcher 02:58
Do you do any personal stuff on it at all?

Participant I 03:01
Well, if I may, Oh, okay. At work on my go into my personal email, my Yahoo account. Yeah. But the bulk of it is actually for work purposes only. And that's how it should be. Yeah. Right. So we've got quite strict a corporate rules given that we also provide cyber security. So yeah, we're quite banal when it comes to stuff like that. Yeah.

Researcher 03:20

So would you do would you do anything on your work computer like online banking, or, or like online shopping

Participant I 03:28
or not shopping but certainly online banking? Yes, I would.

Researcher 03:31
Okay, and would you do any anything like social media at all? No, no, not even business focus. Things like LinkedIn are

Participant I 03:40
well, social. Well, so yeah. Breaking it down certainly, LinkedIn if it's worth it, because generally I'm using LinkedIn for work purposes. So I see the relation there will correlate Is there anything else in terms of Twitter, Facebook, which I'm not on, or even Instagram, I know they're similar. Use of my own device. Okay.

Researcher 04:02
All right. And so, say you do work baby work, you might go into your personal emails at work. On your work computer, you might go and do online banking at work. But you wouldn't use it necessarily for anything.

Participant I 04:13
good description of this and

Researcher 04:17
got our personal laptop at home. Yes. Would you use that for? Do you use that for user obviously? Personal stuff? Do you use it for home? Do you use it for work stuff at all? No. You don't have a you're not able to log into it from into the world. Okay. Okay, but you would on that personal laptop, you would do things like online banking and personal shopping shopping. Yeah, yeah. Yep. All right. And do you do you work? Do you predominately work from the office or home or is it a mixture?

Participant I 04:49
It's a mixture. So probably 60% of work and 40%. And that's,

Researcher 04:55
and I thought that that like if that increased or changed or decreased since COVID, or

Participant I 05:00
it's increased? Predominantly, I was in the office five days a week, right? Yeah. And you're the concept of weaken the line was be the one off that was writing proposal, but otherwise, no, definitely. There's now a next model. Okay, now we know opera.

Researcher 05:15
But you could you could work from home previously and the systems were set up for you to be able to work from home if you need to. Okay, okay. Um, presumably on your phone, so on your phone, which is a work and personal device, but you bought it personally. So is that that using like a company what was that got? a BYOD policy or Is that Is that what that is? Or is it just a one off

Participant I 05:46

work? Predominantly it is they will supply a device but we do have a BYOD policy. So on that I have a token that I can access my Microsoft products and to if a syndication if I'm trying to access a document or whatever, whether it be SharePoint or whatever, right so they basically dog got stuck reached out my credentials if I'm doing that via if I'm outside of the office.

Researcher 06:12
Yeah. Okay. And so when you're when you're using mobile phone, do you you honestly, do you did that automatically? You've got it set up to automatic switch on your corporate Wi Fi network, go when you're in the office to your home network when you're at home? Is that right? Same with your is that the same with your work laptop, it'll work over the office network when it's on? That's great. And then same setup, same setup, and what would you would you ever take your personal laptop into the office at all or does it have a

Participant I 06:38
no don't because it can reach up from their point of view in terms of Wi Fi or anything like a tethered to my phone but otherwise no, no need to bring personal iPad into into the office at all. City from my work laptop and taking her home and using my home Wi Fi. If I'm accessing work applications, I think to actually go in for a token and authenticate myself. I have my mobile say who I am. So we've got security which is set up that way.

Researcher 07:13
Okay, is that is that using a VPN network? Is it and then using something like a Microsoft authenticator or?

Participant I 07:19
Yes, okay. Similar to what I uses, yeah. So this secure from that point of view and yeah, yeah. So again, they're designed to keep your personal life and your work life, private from their point of view, I should say,

Researcher 07:31
yeah. Okay. So and do you do you ever desire any, have you ever would you, would you store any personal data on your work devices? Or

Participant I 07:46
is that as I looked at you that probably isn't that's probably more around. Say if I had a receipts into my in my work address, that was personal, I probably saved it that way and just kept it on a shared drive. And then, after a while, I'd go through and just delete it. All

Researcher 08:04
right. Okay. All right. And but you don't use your, your personal laptop for any work. So there wouldn't be any work documents on that. And for your work devices, when you're using Wi Fi for your work device, when isn't it how do they that has got auto locking devices, often auto locking mechanisms to force you to log in or not leaving them unattended or

Participant I 08:29
it's absolutely yeah. So corporate policy for us, we walk away you lock it again, it will turn itself out after I think that's got two minute window that will sell themselves on that. Yep,

Researcher 08:41

okay. And I'm in terms of the corporate policies or any, any policing of that or it's just, there's just a policy that you're expected to adhere to.

Participant I 08:49
So within our work environment, we like given certain modules around cyber and security and work assets that we've got to go through and retrain ourselves or keep on refreshing, so to speak, to make sure that we're actually following corporate policy.

Researcher 09:06
So that's, that's training, that's training you have to do and you have to do that on a regular basis. Is that

Participant I 09:11
correct? Once once every year, once every year, okay, yeah. And if there's something new then that gets pushed up for a rookie. Yeah. To complete.

Researcher 09:20
And in terms of that train, I mean, I got obviously got, I guess you've got the worst kind of policy that you need to hear to. And obviously get the training or whatever is a it's a, it's a culture that, you know, for example, let's say you did something wrong, or you made a mistake, or what if there's a culture that to encourage you to do report that immediately or is it more of a punishment focused culture or No, it's

Participant I 09:45
true toward the middle. It's no blame policy that we have actually in the culture of xxxxx, but also in terms of certain things are saying or detected. There bounce open to discussing tension between it or the IT team and the person individually from that point. So clearly, if we're doing things that we shouldn't be doing, but the questions arise, but if we repeat offenders or either again as therefore a little bit more stringent in terms of taking the next step, if a person is doing a procedure to be doing something fortunate, or whatever the case may be.

Researcher 10:21
And the training that you get work is that is that focused primarily on protecting the work, work environment. It's not focused on you personally.

Participant I 10:31
That's work environment and how you access work applications or customer information or the applications to enable you to take your time

Researcher 10:40
and your and your personal life in terms of your personal cybersecurity when you using your home PC or your laptop or your your mobile phone for personal use. Have you seen or IV come across any training or guidelines or you know organizations giving you tips or guidelines or

Participant I 11:01
illustrate from the bank and joke or something else around phishing scams that sort of thing. So this really comes to light. The another thing that I use, I have a password manager. And it's really just based on how I operate. So again, anything SUNY financial

relationships, investments or whatever it is or under MFA or in terms of you know, how I will access those, that information,

Researcher 11:26
right. So, so, so I lost my train of thought and so it was I, what was my last questions? Right? Well, I'll

Participant I 11:38
use your personal information or any training or training.

Researcher 11:43
Yeah, sorry, training. So, so so the only the only guidance you received or kind of, I guess, yeah. Awareness. Other than then what you've got gained from your work training is from the banks in terms of fishing, whether it

Participant I 12:00
be grep was able to bust some scam or whatever the case may be

Researcher 12:04
correct. Yeah. Okay. Okay, that's great. Thanks. What about do you use? Well, on your work computers, and also you personally use antivirus software? Right. Is that is that workwise? That's obviously managed by the IT department, I guess, or

Participant I 12:19
that is totally seamless to move at home. What am I running? No, I can't think of what I'm running. But yeah, I definitely have any virus running on my laptop from their point of view.

Researcher 12:33
Okay, and so they talked about your passwords or your preferred so when for your own device. So obviously password access to your your work device, and I don't know when the phone is do they? Does it work determine that you have to have a password on your phone or cococozy using it for work or

Participant I 12:49
it was recommended about corporate policy that yes, we do. Okay, so you're getting a four digit code or face recognition at least?

Researcher 12:56
what's your what's your personal preference? Is it pins or passwords or face recognition or fingerprints or

Participant I 13:03
pins basically, right? Yeah. Okay.

Researcher 13:06
And what why is that doesn't have interest.

Participant I 13:08
Oh, this is so nobody will guess at all. This is really obvious. But yeah, for the dependents basically for my iPhone, at least in terms of on mobile to access that. It's a standard from their point of view.

Researcher 13:22
Okay. And so you you manage your passwords and pins via a password management app.

Participant I 13:31 YEAH. Generally, I've got one pin. And that is for my mobile PDA on this on this personal stuff. It's a joint pin between myself and my spouse.

Researcher 13:46
Right? Yeah. Okay. And in terms of so because it's for your password to use a password management tool, then that deals with all how often you change passwords does that? Does that manage all of that or

Participant I 14:05
it does mention as well or as they can randomly see, because we have as long as I'm in the Password Manager application, I can open up whatever. I need to open up that way as well. Okay.

Researcher 14:20
I'm not really used it does it? Does it force you to change passwords or time or does it just match that in the background? Well,

Participant I 14:25
it what it does is it scans basically all sites that you've got a password with, they check with what's similar or if you've got passwords, and then it gives you recommendations to either change or let the password manager and sheet to an arbitrary complex passwords. You don't actually know yourself because you can you didn't remember it as long as you're using Password Manager where you go, right.

Researcher 14:52
Okay, but you manage pins yourself. You choose the pins yourself.

Participant I 14:57
I've only got really got two sets of pins, one for the mobile and one for joint.

Researcher 15:02
Yeah. And you never You never change those at all. Okay. Okay. Okay, that's cool. Thank you. And I guess one of the questions around do you apply different, more complex security for things like financial stuff, but you manage all that way your password management app, so that's all Okay, so your home network when you know working more from home, since COVID was only requirements to change that in terms of security or or setup of that or

Participant I 15:37
it was really what's been set up for work. And again, if we're using using or accessing applications, we had to go through a VPN to actually get that information, anything that was web web browser. related. Sorry about the big word noise. So it was given the birthday. But it's all a whole thing about it was corporate roles. And as long as I access the VPN military advantage which is being possible or a modified to authenticate myself away, which so yeah,

Researcher 16:13
okay, but your home network, as you've got, obviously a home router and you've got obviously a password to connect to your devices. Does that does that ever change or is that just

Participant I 16:22
I would have probably the time where we change that password three times over the last seven years.

Researcher 16:33
What's caused you to change?

Participant I 16:35
Upgrading the router

Researcher 16:37
and upgrading router and

Participant I 16:40
if I've done that, then if I do give the router away or sell it, then that the possibility of them or should have gleaned a password. It won't apply to one on one my current setup is from that point. Okay.

Researcher 16:54
And and that password for that router is is used by a family.

Participant I 17:03
Yeah, yes.

Researcher 17:05
And is it shared with weird like friends and guests and stuff like that when they come or

Participant I 17:10
separate guest Wi Fi password separately or together? So there'll be anybody that comes into the house and they want access to the Wi Fi when they go they share that password.

Researcher 17:23
What's that? What's the benefit of that? Does that allow you to do different things or is that just

Participant I 17:27
different parts of separation just in case? Right? Just being extra vigilant monitoring else? Yeah.

Researcher 17:32
Okay. But basically it's giving you access to the router but there's no there's no you're not putting restrictions on what they can access from that. Okay, and like, did your family share the password out to friends stuff or

Participant I 17:50

coming into the house? Yeah. So hidden, super mature. The guest password that they will use appropriate stored on their phones. Yeah, it was it was just straight.

Researcher 18:00
But it's not startup posted on the fridge anywhere and you'd be surprised.

Participant I 18:10
Exactly. People do strange things. Yeah. Yeah.

Researcher 18:13
Okay. And is there any special level of security on your home network or any?

Participant I 18:21
I rely on LastPass Password Manager for them to get through that. Well, if you've got chased away by that city from two regions need access everything's encrypted. From my point of view is yet unless you're running the password manager, you should, in theory, never be able to make economic access that can

Researcher 18:45
come back to your devices. And let's say you go out or go on a trip or a holiday or business trip or you go to the local cafe or whatever do you do you use either your home your own devices or your work devices over public Wi Fi networks?

Participant I 19:00
So could you repeat it so when I go work go

Researcher 19:04
when again when you go when you're when you're away from home and away from the office and you maybe you're gone to maybe you want to go to a cafe or whatever or you've gone to an airport or you're going to a hotel Do you do you do you use your either your work laptop or your mobile device or personal laptop ever public Wi Fi networks?

Participant I 19:20
No. So what I'll do is with the iPad, I've got a SIM card. And that's it. I use that set up using and also tethered to my phone in terms of generally don't use public Wi Fi setups within like a restaurant or cafe, knowing that basically the potential there is Yeah.

Researcher 19:44
What about what about what about airports or hotels?

Participant I 19:48
If you're away on business, for example, koru lounger wallet and then the credential different use the public Wi Fi. But otherwise, yeah, that was probably the only circumstance.

Researcher 19:58
If you're on a if you're on a public Wi Fi in the koru lounge, would you is there any restrictions you put on the activities you'd count out? We do do an email or banking on there for example.

Participant I 20:09

needed to check out my bank account near Sydney on my mobile using their Wi Fi they are different to that

Researcher 20:16
particular niche

Participant I 20:17
I need to access via using my password manager as well. Yeah, so I filled it with some level of protection that way as well.

Researcher 20:24
What about purchases online shopping over the network?

Participant I 20:27
Yes. Okay.

Researcher 20:31
Are there any activities that you would definitely not do over a public Wi Fi network? You're just thinking

Participant I 20:43
for it's a public Wi Fi network. It's just more like chicken the hair or stuff or news on varied if it's making a purchase. Manage their fire using the SIM card approach. Rather than Wi Fi approach because it just weary of everything from their point of view but yeah, no chimneys just informational. You can probably describe it that way. Okay. folders using a public Wi Fi network. Yeah.

Researcher 21:10
Any any social media or public Wi Fi or

Participant I 21:13
Instagram. I probably would. Yes. Yeah.

Researcher 21:18
Okay, do you? Do you what do you what do you choose to use apps or you may choose to use sign up for apps or use apps like I know, some of them might be Facebook, Twitter, Instagram, or they might be smaller ones just does a size and popularity of that effect. You do think that's a well that's It's big. It's big. And as popular therefore it's going to be more secure. Or do you say actually, I'd rather go for a smaller niche type app because it's going to be less popular less of a target

Participant I 21:43
isn't sort of, I guess what I've done as well iPhone or Apple have got your app store you'd like to clear the ration about it. If something I hadn't heard of, or do some research, or a Google or whatever to go out as what's the feedback or reaction of the application. And then I do from time to time I actually think go through and just check my email addresses whether or not it's been poned or not. And just see if anything else from there. Nothing's changed really over the last five years since I've been a LinkedIn issue, but otherwise, yeah, it will come straight for from that point. Yeah. Okay. Yeah.

Researcher 22:25

And have you have you ever been a victim of a cyber attack? No. Not at all. Any any attempts that you've picked up? Uh, well, it

Participant I 22:35
seems there's been more people phoning me saying the representative company that they're not really Yeah, and it's been certainly not an online scam or anything like that. No.

Researcher 22:45
Okay, and how how easy to find it to detect, you know, potential attacks like phishing attempts or, you know, stuff like that.

Participant I 22:54
So there's sort of there are modeling related into my details there and I go, Well, hold on that doesn't seem right. Or, to us there's a foreign person calling from let's say spark saying they wants this there's an issue with my internet account over my account number and details are kind of go I'll call you roll NEW CALL ME. Especially here just just common sense approach from that point.

Researcher 23:19
Okay. Any any any exposure to ransomware attacks? Okay, how concerned are you about identity theft?

Participant I 23:31
Usually, it is very aware of what I do, how I how I transact, but also the cases what I access from that point of view as well. And it's more probably more around my visa or bank cards rather than anything else in terms of where is that information going?

Researcher 23:48
Around the visa and bank cards. What about what about information on various social media platforms or stuff they absolutely use?

Participant I 23:58
Because I'm not I don't I'm not on Facebook and I'm not on Twitter if anything on Insta It was either commenting on a friend's picture or commentary or posting something random but no, not too concerned about that at all. Okay, yeah.

Researcher 24:15
So you're concern around identity theft is around his banking details and stuff like that. In terms of the cameras on your device, so are you concerned about those watching or people watching to those cameras or,

Participant I 24:29
generally, if it's any thing that I'm not happy about, I just switch the camera off or cover the camera sitting on the capability or on my laptop? Let's just do this. You're in also Monday, as well.

Researcher 24:43
Okay, and what about what about what about microphones? Are you concerned about microphones listening in on on those devices at all?

Participant I 24:51

Haven't really thought about it. anything like it's just you know, where you got alexa et cetera as we'll soon what? What's being listened to in terms of home conversations? Is the the delivery of a content that comes in appears in your email or whatever the case may be, but yeah, I'm not. Yeah, just we're in terms of confidential information that you shouldn't be talking about. Yeah. What's the I don't really think about it like far more paranoid having some time ago and the kind of silence type of approach.

Researcher 25:26
Do you take any particular precautions for that? Camera you might turn your camera off because he didn't know and what would cause you to turn your camera off or what would trigger you to do that?

Participant I 25:36
Well, if I'm at home and my family is there or because they just didn't know keep, keep it. Not because they want to steal so why doesn't it sit there and listen to me on the other side of the camera, but again? Yeah, okay.

Researcher 25:52
All right. Um, okay. So we've talked about cybersecurity training that's covered that guidance and policies we talked about that I would cover that I think it talked about that how often you work from home. How would you say for you, how would you say your your site's intentions regarding cybersecurity, match your actions, how your actions match your intentions, like so? You know, do you do think actually, well, I do you know, I'm aware of cybersecurity and I do all the actions I need to I do think there are stuff that you don't

Participant I 26:30
there's probably stuff I take for granted but overall it's anything that I'm sharing around personal information, or identity, banking financial I'm extra vigilant around what am I doing, who's on the recipient, and making sure am I accessing the right channel, just share that information. That's probably the best way to describe that. So since you've been away rather than going you know, sharing willy nilly information, whether you join with us and my example, although it's financial, asking the the shop Okay, or the florist, Hey, what are you doing with my credit card? Information, that type of thing? Yeah. Because more than anything else, but yeah, it's just like enough, where I'll pay electronically, they'll make sure that I'm to a pay wave or a on or ecommerce payment system rather than vocally. share that information on the phone or device. Yeah. Okay.

Researcher 27:38
And how how has your approach to cybersecurity changed as a result of COVID and working more from home on

Participant I 27:47
Possibly no, it hasn''t. It's probably the work that I'm that I'm aware of in terms of cyber cyber attacks ransomware, etc, etc. Businesses. So again, while people are well, it's only my business personally, along with comments my personal contents are what I how I treat, information report the severity or sensitive information from their point of view.

Researcher 28:13
Okay. How do you how do you behave regarding things like forwarding emails or opening attachments or, or stuff like that?

Participant I 28:23
I always check an attachment of the phone know the person. Yeah, I don't have a problem but if anything's come left field that I'm not sure. Yeah, a lot of bad stuff gets tripped in spam. And I just delete it straightaway don't even bother opening that. Doesn't seem right well. Go near a

Researcher 28:44
captain span for home and work I guess or or

Participant I 28:47
or home and work. Absolutely. So you got we got email rule set at work and also a rule set up at home in terms of your NFS not genuine spam and just delete don't even bother opening up.

Researcher 29:01
What about things like bit old school but USB drives to ever use? How does how does trust influence how you think about cybersecurity?

Participant I 29:13
Does reputational brands and okay, if I've been relationship with lets say my bank Well yeah, I trust that they are basically I've got my protection all my assets protected in the right in the right mindset, but I would expect them to be again there are a lot of dodgy activity out there is usually discretion or using just common sense. Don't go they also don't share any information. Yeah, yeah.

Researcher 29:43
Which they generate trust. You obviously trust us obviously trust obviously family and friends trust trust. Trust your employer Okay.

Participant I 29:58
All right. If in doubt, philosophy doesn't seem right. Well, I'll just pick up the phone last call on doing the signals to me or what do you want from me to answer? What do you want me from there? willy nilly. Just go and buy you want us where you go.

Researcher 30:15
Just going back to the home again. So our home network now obviously we were a long way from the fixed time PC connected to our modem onto a copper line. Have you got other devices like you know, Alexa or Sonos sort of smart TVs? Or

Participant I 30:33
Smart TV? Stream stream TV traditionally, otherwise it's iPads that will be for streaming music. And basically, therefore it's just the mobile phones that we would access the Wi Fi on and just the MacBook in terms of doing something else.

Researcher 30:53
What about things like wearables, like smartwatches or fitness trackers and stuff like that? Like that? Okay. So in terms of a smart TV, for example, I have any concerns around that being connected to your home Wi Fi network and how that might affect security of either your personal

Participant I 31:10

accesses, and also password enabled as well. So anything that I'm accessing or inches of application on my smart TV, I've got to have a pre pre decent password associated with it and anything I do watch each channel so to speak, it's got a separate password that way as well. Okay, yeah.

Researcher 31:32
When you do online stuff, do you generally store your credit card details or just enter them each time?

Participant I 31:37
Like generally enter them each time keeping things stored? Privacy Policy I'll call myself into Yeah,

Researcher 31:46
yeah. No, it's fine. I think that's covered most of what I wanted to cover any, any, any Have you got anything? Anything that you think missing from that or in terms of

Participant I 31:58
speak really comprehensive? Again, it's because I live and breathe it. It's kind of like it comes naturally. The word to me it's more or less reinforcements for the friends family. I don't do this. If you don't start. Get yourself password managers. My first point of call in Sydney. At least it gives you a level of protection rather than zero case. You lose your credentials to try and get the pay or whatever the case may be. That's when the fun begins. And I think the other side of it is also say for example, you get the credit card does get smashed. Well, okay. All banks or insurance companies gonna be asking about the banks, or what What measures do you take yourself to protect your identity? If you've done nothing about that, well, may come as a result, so we're not covering you because you've failed to do something yourself. We'll take responsibility. Yeah, that's probably not showing our fault. I think we should come back to me if you've got any further questions.

Researcher 33:01
No, absolutely. I think thanks for that. Carrie. I'm just gonna stop the recording now. Because it's been really useful. Thank you. So that was me. How many of you interview

SPEAKERS
Participant I1, Researcher

Researcher 00:00
When you do your online When you do online stuff do you do you have a do you use your normal credit card, debit card? or do you do have a special one for doing online stuff?

Participant I1 00:14
In terms of online training,

Researcher 00:15
online, online, online purchases or whatever online shopping for example,

Participant I1 00:19
I use a debit card that's separate to buy a normal credit card.

Researcher 00:24
Just one day use just for online shopping.

Participant I1 00:26
okay, So effectively what I can manage, okay, if it does get hacked, The only thing we'll do is hopefully only a couple of dollars will get taken rather than launch affiliate vigilant when it comes to credit card because I'm looking at it probably once every second day to make sure you get the transaction as

Researcher 00:49
Missed that question so thanks.