Informal Support Networks: an investigation into Home Data Security Practices

Conference Paper · August 2018

Norbert Nthala
University of Oxford

Informal Support Networks: an investigation into Home Data Security Practices

Norbert Nthala and Ivan Flechais, *University of Oxford*

https://www.usenix.org/conference/soups2018/presentation/nthala

This paper is included in the Proceedings of the Fourteenth Symposium on Usable Privacy and Security.

August 12–14, 2018 • Baltimore, MD, USA

ISBN 978-1-931971-45-4

Informal Support Networks: an investigation into Home Data Security Practices

Norbert Nthala
Department of Computer Science
University of Oxford
norbert.nthala@cs.ox.ac.uk

Ivan Flechais
Department of Computer Science
University of Oxford
ivan.flechais@cs.ox.ac.uk

ABSTRACT

The widespread and rising adoption of information and communication technology in homes is happening at a time when data security breaches are commonplace. This has resulted in a wave of security awareness campaigns targeting the home computer user. Despite the prevalence of these campaigns, studies have shown poor adoption rates of security measures. This has resulted in proposals for securing data in the home built on interdisciplinary theories and models, but more empirical research needs to be done to understand the practical context, characteristics, and needs of home users in order to rigorously evaluate and inform solutions to home data security.

To address this, we employ a two-part study to explore issues that influence or affect security practices in the home. In the first part, we conduct a qualitative Grounded Theory analysis of 65 semi-structured interviews aimed at uncovering the key factors in home user security practices, and in the second part we conduct a quantitative survey of 1128 participants to validate and generalise our initial findings. We found evidence that security practices in the home are affected by survival/outcome bias; social relationships serve as informal support networks for security in the home; and that people look for continuity of care when they seek or accept security support.

1. INTRODUCTION

Securing home devices, services, and data is increasingly difficult and necessary. While home users are not as attractive a target as many organisations, they are both commonplace and vulnerable to several attacks. Initial work in exploring the security of home computer users [1, 22, 25] has highlighted the importance of this domain, and yet much more needs to be done to be able to address the scale and complexity of the security challenge.

According to the 2013 census, 74.4 percent of [U.S.] households use the Internet [42]. Similarly in 2015, 86 percent of households in Great Britain (22.5 million) had Internet access, up from 57 percent in 2006 [14]. Worldwide, Internet Live Stats reveals that over 46 percent of the world's population (3.4 billion) had Internet access in their homes by July 2016, up from 29 percent in 2010 [40]. And as the number of connected homes increases worldwide, so too do the threats.

In 2012, Rao and Pati [36] conducted a study in India revealing common threats and attacks facing home users: viruses, malware, identity theft and privacy violation, and phishing. Large organisations generally mitigate these types of threat well, however this is not the case for typical home computer users. Best practice in mitigating viruses in a home context seems to focus on running antivirus software, patching, and warnings to avoid untrusted or malicious websites (from web browsers and awareness campaigns). In contrast, in addition to antivirus software and patching solutions, larger organisations also have acceptable usage policies to manage risky behaviour from employees; segmented network architectures to avoid the spread of viruses; active firewalls, intrusion detection and prevention systems to identify problems before they cause significant damage; backup strategies to recover from incidents; and, perhaps most critically, an IT support function that can deal with problems should they arise. In comparison, home users have very few resources, capabilities, knowledge, skills, or tools to protect themselves from the multitude of threats that harm them directly.

But threats that directly harm the home are not the only concern. In today's highly interconnected world, the security of cyberspace depends on the security of all the different devices connected to the Internet. Ng and Rahim state that home users play a crucial role in securing cyberspace: if not well-protected, home systems can be compromised and used to attack critical infrastructure (such as telecommunication and banking) that heavily depends on the secure functioning of cyberspace [29]. While security breaches affecting organisations receive much attention, breaches involving home users usually come to light only when home devices or users themselves are involved in an attack affecting critical infrastructure. The October 2016 attack on Dyn, for instance, which is thought to have been enabled by insecure IoT devices in homes [5], triggered a number of reactions from different stakeholders, with some device manufacturers reportedly recalling their devices. Users at home face many different kinds of threats and mitigation requires interventions both within and outside the home.

A key strategy for improving home security practices so far has focussed on increasing awareness [33, 21, 24, 38, 30].

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.
August 12–14, 2018, Baltimore, MD, USA.

Despite the effort put in such approaches, studies [3, 33, 17, 27] and recent events [5, 12, 26] show that home users remain vulnerable as evidenced by insecure practices and choices to ignore security advice, leading the research community to explore alternatives to increasing awareness.

Dong et al. [10] propose an economics approach to designing security solutions for communities rather than individuals. They argue that incentivizing people to improve the security of a community (from which they benefit) through a shared venture would motivate personal security investment. While maintaining user-centeredness, Gutmann [20] proposes the application of problem structuring methods (PSMs), a technique from social planning, to help analyse security problems. The intent is to ensure the most appropriate solution is applied to a problem, and Gutmann claims to tackle a common problem where developers and service providers impose their favourite technology on people, without considering the environmental, social, political, and legal aspects of the overall problem. Wash and Rader [44] propose security story-sharing to help shape the mental models which inform home security decisions. Through sharing the right stories, and with expert involvement, the authors foresee changing home user security behaviour. Adding to the body of proposed approaches, Rowe et al. [39] put forward an approach modelled on public health systems for a shared secure cyberspace. They argue for a population-centred approach in dealing with cybersecurity issues. This is a departure from the typical practices in information security which take an individual focus in trying to understand how systems are compromised, and how they can be protected. The authors outline the technical requirements of a public cyber-health system, with specific focus on how the system would achieve monitoring, prevention, and incident response.

Building on this work, we believe that secure (and security) systems in the home need to be designed from an empirical and grounded understanding of home users, the context of use in which they operate, and how they make data security decisions. We report on the qualitative and quantitative research we have undertaken to explore the security practices of home computer users. We conducted 15 scoping semi-structured interviews, followed by a further 50 targeted semi-structured interviews lasting approximately 60 minutes each. We analysed the data systematically using Grounded Theory and used this to design and run a quantitative survey of 1128 home users to explore how widely shared the qualitative findings are. Our key findings are:

- *Social relationships* play a vital role in information security in the home. They serve as informal support networks of security practices.
- *Perceived competence* is an important factor in security decision-making in the home. It is used to assess the quality of a security source, and the support offered in the home. The participants use different metrics to evaluate competence, including the profession of the source, the educational standing of the source, the level of usage of technical devices of the source, and negative experiences of the source.
- *Continuity of care* is an important characteristic of security support in the home. Participants report seeking or accepting support from a source that is constantly available when needed.
- Participants look for *evidence of a security problem or need* for them to practice security. Typical evidence is direct harm to an individual, or their social relation, resulting from the individual's insecure behaviour.
- *Confidence* of the participants in an implemented *security control* can increase insecure practices.

The remainder of this paper will review the related work in this domain in section 2, describe our research methodology in section 3, and present our results in section 4. We finally discuss the implications of our findings and highlight areas of interest for future work in sections 5 and 6.

2. RELATED WORK

In this section, we review prior work investigating home user security practices, structuring the concept of security practices into: (i) security behaviours; and (ii) the factors that influence the security decisions that precede the behaviours.

2.1 Security Behaviours

Studies have been conducted to understand and improve security behaviours in the home. AOL and the National Cyber Security Alliance conducted a study of online safety of home computer users [2] where 329 home users were interviewed and their computers were analysed. Researchers asked and checked for the availability of virus and spyware protection software, firewalls, parental controls, and the use of encryption for wireless network users. The study concluded that the majority of those studied lacked core protection. Similarly, Furnell et. al assessed the security perceptions of UK home users [17]. They surveyed 415 home users about their awareness of security threats, usage of system safeguards (firewall, antivirus, anti-spyware, and anti-spam software), and their awareness and understanding of security-specific tools found in contexts such as operating systems and applications. The study found that both novice and advanced home users appeared vulnerable to security risks. The authors concluded with a call for the development of new models of engagement and awareness raising.

Rao and Pati surveyed home users in India to understand their levels of awareness of security threats and usage of security measures (password protection, antivirus, firewall, patching, data backup, and parental controls) [36]. The study revealed poor understanding of security threats, and low levels of adoption of recommended security controls. The authors concluded that the security in the home can be improved through awareness and user-friendly security controls. Similarly, Ng and Rahim studied factors that influence a home computer user's intention to practice computer security [29]. They surveyed 233 home computer users on the use of antivirus software, data backup, and personal firewall.

Ion et al. studied security practices that different experts and non-experts consider to be the most important in protecting their security online [23]. They conducted 40 semi-structured interviews with security experts, and used the results to design a survey. 231 security experts and 294 non-security experts were surveyed, and the practices of the two groups compared. The studied practices included installing software updates, using antivirus software, account security (using password managers, writing down passwords, changing passwords frequently, and using two-factor authentication), and mindfulness (visit only known websites, check if HTTPS, clear browser cookies, and email habits). The results showed discrepancies between the most important security practices of the two groups. The authors concluded that more work is needed to improve the practices of non-experts, and identified three key recommendations: install software updates, use password managers, and use two-factor authentication for online accounts.

Dourish et al. [11] investigated how users respond to security issues in their daily lives and found that people ask for assistance or delegate security activities to knowledgeable family members (similar to [15]), friends, or roommates. They also found a reliance on technology (e.g. SSL for data connections, ssh tunneling for email, or trust wired Ethernet to be more secure than a traditional wireless medium) for protection; others reported delegating security to institutions such as financial companies. Likewise, Nthala and Flechais [31] found that some home users turn to trusted others (colleagues, IT professionals, relations, and peers) for help with security issues.

2.2 What Influences Security Behaviours?

Research has been conducted to investigate and understand the factors that motivate different security behaviours. Several studies [38, 29, 31] have shown that social influence has an impact on the security behaviours of home users. Das et al. [8, 9] studied in more detail how this social influence plays a role in the security behaviours of home users. They found that social influence affected the security behaviours of those involved through social processes (observing and learning from friends, social sense-making, pranks and demonstrations, negative experience of others, and device sharing), and conversations about security (a finding similar to Rader et al. [35]).

Wash [43] carried out a qualitative study of iterative interviews to investigate the existence of folk models of security for home computer users, aiming to increase our understanding of mental models of security for home computer users. The study focussed on finding out how home computer users understand and think about potential threats. Wash identified eight folk models categorised into models of viruses and other malware, and models of hackers and break-ins.

Herley [21] argued that users perform an implicit cost-benefit analysis when making a security decision. The cost is the effort required to follow security advice, while the benefit is the avoidance of potential harm that a successful attack might cause. The harm includes monetary loss (if any) that victims endure, but also the time and effort they must spend resolving the situation. Similarly, [31] found that the cost of protection also influences the outcome of security decisions in the home.

In a study investigating why users accept or reject different advice about secure behaviours, Redmiles et al. [38] found that users reject advice due to too much marketing information, inconvenience and threatening users' privacy. In addition, the study reported that trust was a clear factor that influenced the choice of a source of security advice.

Other related work has focussed on understanding practices around home network security, highlighting the differences in responsibility between Internet Service Providers and home users [32].

3. METHODOLOGY

We started our study with a scoping study of 15 semi-structured interviews. The aim of the scoping study was to make an initial exploration of security practices (which we consider to consist of (i) security behaviours and (ii) the decisions that lead to such behaviours) in the home, from which we would identify a research gap for further exploration. Our research questions would then be refined based on the initial results. Respondents for this study were chosen from a snowball sample [7] of home users in the UK. Two research questions guided our interviews during the scoping study:

1. What influences security decision-making in the home?
2. What kinds of security behaviours exist in the home?

We analysed the data using Grounded Theory (see section 3.2.2) to identify all the key themes emerging from the data. Our analysis identified a number of factors that influence the outcome of security decisions in the home, all of which were consistent with previous studies discussed in section 2.2. These included inconvenience, trust, cost, and availability of too much marketing material. Analysis of the data on security behaviours revealed two separate categories of the behaviours which we categorised as: *security work* and *security support.*

Security work is highly contextual and specific to technology platforms, comprising behaviours such as installing and using firewalls, antivirus software, patching, data backup, and parental controls. As reviewed in section 2.1, our findings were consistent but much less comprehensive than previous surveys in this area.

Security support, on the other hand, comprises two subcategories; support seeking and support giving. The work of Dourish et al. on delegation [11], Nthala and Flechais [31] on security support, and Redmiles at al. [38] on advice seeking and giving, all fall under security support. We noted that little work has been done to explore security support that is required or available in the home in great detail.

This led us to focus our research on understanding security support in the home, and the reasoning behind it. We thus refined our main research questions to:

1. What influences security decision-making in the home?
2. What are the characteristics of security support in the home?
3. Where do home users get support?

To answer these questions, we adapted the research methodology proposed by the Productive Security research team of Beautement et. al. [6]. We conducted a two-part study aiming to increase our understanding of security support in the home, and the reasoning that surrounds it. In the first part, a detailed understanding of the problem domain arises out of studying a few individuals and exploring their perspectives in great depth. In the second, a more generalisable understanding of the issues identified in the first part can be gained from examining a large sample and assessing responses to a few variables.

Part 1 of our research consisted of 50 targeted semi-structured interviews with a broad range of individuals and families within the home context. As the interview data was being collected, it was qualitatively analysed using Grounded

Theory (see section 3.2.2) in order to identify the significant themes to answer our research questions. The themes were used to generate scenarios and questions from which a survey was developed and run in the second part of our study. By tailoring our survey to the home context, we ensured that the questions were relevant and recognisable to the participants.

Part 2 made use of *Unipark* to run an online survey and *Prolific Academic* to identify a representative sample (in terms of age, gender, and educational level) of 1128 participants. The survey results were analysed and aimed to validate the findings of the qualitative data analysis, and support the generalisability of these results to a wider home user population. This was meant to provide clear evidence on which future work can draw to improve education, technology, and practices for home data security.

The study was ethically reviewed and approved by the Social Sciences and Humanities Inter-divisional Research Ethics Committee at our institution.

3.1 Recruitment

We recruited for the interviews by advertising through community centres, newspapers (in print and online), and other social groupings, and by putting up posters at the National Museum of Computing. The recruitment was conducted in different locations in the UK. Before starting an interview, we collected demographic information including age, gender, highest educational level, ethnicity, marital status, and occupation from the respondents to ensure we cover a broad range of home users. Each participant was compensated with a £10 Amazon voucher for an approximately one-hour interview session.

Participants for the survey were recruited through Prolific Academic, and each participant was compensated with £1.70 for an approximately twenty-minute session.

3.2 Procedure

3.2.1 Semi-structured Interviews

We followed a semi-structured interview protocol utilising an interview guide to maintain direction while keeping the interview open for both depth and breadth topic exploration. Prior to the interview, participants were asked to complete a demographic form, which included questions regarding the devices and services they use. Our interview guide is appended in D.

3.2.2 Grounded Theory

The interview data was analysed using Grounded Theory [19]. Grounded theory allows researchers to examine topics and related behaviours from many different angles, leading to comprehensive explanations. It is used to uncover beliefs and meaning that underlie action, and to examine both rational and non-rational aspects of a behaviour [41]. This makes it the ideal choice for studying security support and any issues that surround it. Our approach was consistent with that described by Strauss and Corbin [41].

Three researchers were involved in the analysis. The primary researcher, who conducted the interviews, did the initial open coding of the interview transcripts. To ensure credibility of the codes, a second researcher cross-checked all the codes against the interview transcripts. At the same time, the third researcher reviewed the initial codes and all quotes supporting each code. Any differences and/or issues arising from the initial coding were discussed and resolved among the three researchers. A codebook consisting of 130 codes emerged from the initial coding. These codes were then applied across other interviews through constant comparison, while new codes were added as they emerged and were deemed necessary. In further analysis, the three researchers discussed and grouped the codes into themes (axial coding) and categories (selective coding), based on the properties and dimensions of each theme. Regular coding meetings were held to discuss any emerging codes and to group the codes into families.

3.2.3 Survey Development

The survey tool was developed from the Grounded Theory analysis of the interview data to test a number of significant themes. Scenarios used in the survey were developed from analysis of anecdotes from the interviews, and themes that emerged from the analysis. The aim was to ensure that the participants were presented with scenarios they are familiar with, hence reducing the effect of unknown personal preferences. We made sure that our options to the scenarios were testing the construct under study. Hence, options with factor loadings less than .30 were dropped.

Prior to running the full survey, the tool was piloted and tested with seven participants. To ensure we tested for both clarity and usability of the tool (face validity), we developed and tested it on the platform it would run on (Unipark). The questionnaire went through three iterations of testing, and modification with our participants (four non-experts and three experts – two in usable security research and one in human-centred computing studies).

Two non-experts tested the instrument online, followed by *cognitive interviews* [46]. The participants were asked how they understood and interpreted each question; how easy they found it to understand each question and respond; how easy it was to navigate through the whole questionnaire; and how they viewed the general outline of the questionnaire. This was followed by *expert interviews* as applied in [37], where each expert was asked to first test the survey online, and then review each item on the survey tool in terms of biases, question ordering, clarity, sensitivity of questions, and other issues; all in line with the aim of the study. After this phase, the last two non-experts tested the tool, followed by cognitive interviews.

During each of these phases, the tool was updated based on feedback from the interviews. Once a consensus was reached on all issues affecting different aspects of the tool, we published the study on Prolific Academic targeting 1128 UK only respondents. We asked participants about demographic information including age, gender, and educational level. Survey questions revolved around factors that influence security decision-making (survival/outcome bias, confidence in a security measure, and availability and quality of support), characteristics support (duty of care and continuity of care), and preference and sources of support.

To check the quality of responses, we applied three kinds of checks. First, we used Prolific's start and finish times to check for *speeders*. During testing of the questionnaire, the average completion time was fifteen minutes. After publishing the survey on Prolific, we applied demographic filters of the survey platform on the first set of fifty responses to get a representative sample of the demographics shown in Figure 2. The average completion time remained fifteen minutes, with a minimum of twelve minutes. We set our minimum acceptable response time at ten minutes. Responses below the limit were rejected. Second, we checked for and rejected *straight-liners* - responses that all have the same answers, and *pattern responses* - answers in a pattern. Third, we included a *binary red herring question* which read, ”I am randomly answering the questions” with a ”Yes” or ”No” answer. We placed one towards the middle of the questionnaire, and another towards the end. Responses bearing a ”Yes” to any of these questions were rejected.

Due to the ordinal nature of our data, we tested for reliability of different constructs - each measured by a scale of items - on the final questionnaire by computing their ordinal alpha coefficients (Ordinal α) [18]. The constructs had the following coefficients: survival/outcome bias, .75; confidence in a security measure, .74; duty of care - motivate others, .91; duty of care - be motivated by others, .83; and duty of care - social responsibility, .81. Since our test for continuity of care involved repeated measures, we tested for the reliability of the eight pairs of items using Spearman rank correlation coefficient (r_s). There were positive correlations between each of the eight pairs of items, all significant at $p < 0.05$. The Spearman coefficients for the pairs were, $r_s(1085) = .594, .672, .601, .583, 638, .564, .499, .530$ for pairs A through H discussed in section 4.3.2 respectively.

3.2.4 Survey Analysis

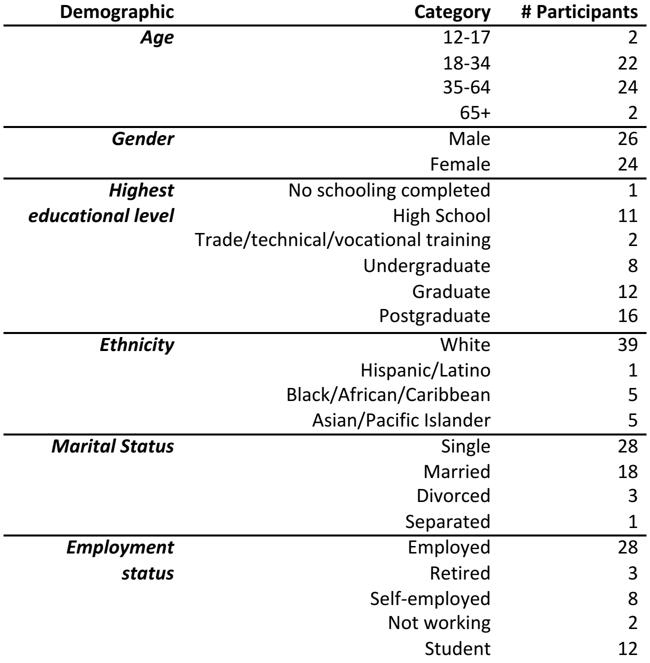
For the survey data, we present descriptive statistics for the different variables. We also run inferential tests on the data including Friedman [16] and Wilcoxon Signed-rank [45] tests for analysis of matched-pair data and rank-ordered data. These non-parametric tests were selected on the basis of the ordinal nature of our data, where the chances of getting valid results from parametric tests were minimal or unclear.

3.3 Limitations

Our study has some limitations. First, all are participants are residents of the UK. This might raise questions regarding generalisability of our results. However, we have documented the procedure we followed in this study, which makes it possible for other researchers to replicate it elsewhere.

Second, common to all qualitative studies, researcher bias is a concern. A single researcher, trained to conduct research interviews, conducted all the 65 interviews. The researcher avoided leading questions, and ensured participants felt comfortable to respond to questions. The researcher avoided interrupting participants, and probed for more information when required. To further mitigate bias, two other researchers reviewed and were part of the data analysis to enhance consistency in data coding. Our research design explicitly aims to mitigate potential bias by also running an extensive survey to test how generalisable the qualitative findings are.

Third, given that security is a sensitive topic, social desirability could bias some of the responses to the survey, specifically for the two scenarios developed to study survival/outcome bias and confidence in a security measure. To mitigate this, we took three measures: 1) we did not reveal at the onset that the main purpose of the survey was to study security practices of the participants. Instead, we stated that the aim was to understand decision-making in the daily use of technology. 2) We employed a self-administered questionnaire [28], hence no interviewer presence and a high degree of anonymity. 3) We used indirect (structured, projective) questioning [13] in those two scenarios, where respondents answered from the perspective of another person.



Demographic	Category	# Participants
Age	12-17	2
	18-34	22
	35-64	24
	65+	2
Gender	Male	26
	Female	24
Highest educational level	No schooling completed	1
	High School	11
	Trade/technical/vocational training	2
	Undergraduate	8
	Graduate	12
	Postgraduate	16
Ethnicity	White	39
	Hispanic/Latino	1
	Black/African/Caribbean	5
	Asian/Pacific Islander	5
Marital Status	Single	28
	Married	18
	Divorced	3
	Separated	1
Employment status	Employed	28
	Retired	3
	Self-employed	8
	Not working	2
	Student	12

Figure 1: Interview participant demographics

Lastly, our data consists of only what people say. This makes it hard to understand how our results translate into actual behaviour in the home. Future work would aim to employ relevant approaches to study these behaviours in context.

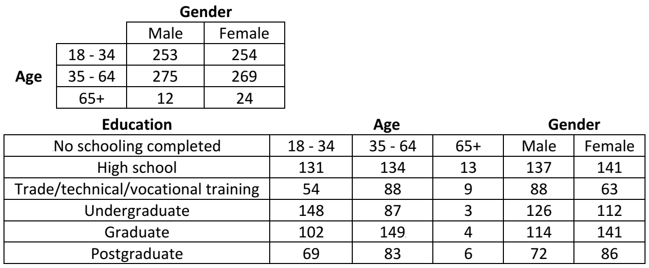
4. RESULTS

In this section, we detail the findings of our study. We start by presenting the demographics of our participants, and then discuss the key findings from our study organised according to the research questions. First, we discuss the factors that influence the outcome of security decisions in the home. Second, we explain the different factors that our participants reported using to evaluate the quality and source of security support. Finally, we detail the characteristics and sources of security support in the home.

4.1 Participants

Our scoping study comprised 9 male and 6 female participants, with ages ranging from 18 to 34, and an ethnicity of 4 Asians, 5 Whites, 4 Africans, and 2 Black Americans. For the targeted semi-structured interviews, we selected 60 people to interview, 50 of which attended. We kept a balance between male and female participants, as well as a diversity of age, ethnicity, education, and employment status.

Demographics for our 50 participants are shown in Figure 1. Two participants indicated being both students and em-



		Gender	
		Male	Female
Age	18 - 34	253	254
	35 - 64	275	269
	65+	12	24

Education	Age			Gender	
	18 - 34	35 - 64	65+	Male	Female
No schooling completed					
High school	131	134	13	137	141
Trade/technical/vocational training	54	88	9	88	63
Undergraduate	148	87	3	126	112
Graduate	102	149	4	114	141
Postgraduate	69	83	6	72	86

Figure 2: Survey participant demographics

ployed, while one indicated being both employed and self-employed. 52% of our participants were male, 48% were female. 44% belonged to the 18-34 age group, 48% belonged to the 35-64 age bracket. During the interviews, these two age groups were noted to be the ones responsible for making most of the security decisions in the home environment. The other two age groups, 12-17 and 65+, made up 4% of the participants each. 32% of the participants hold postgraduate degrees, 24% have graduate degrees, 16% completed undergraduate studies, 4% completed trade/technical/vocational training, 22% completed high school, and 2% did not complete any school level.

1128 respondents took part in the survey. After running quality checks on the data, 41 responses were excluded, leaving 1087 responses. Fifty percent of our participants were male, and fifty percent female. Forty seven percent were between the age range of 18 - 34, fifty percent between 35 and 64, while three percent were above 65 years old. Of all the participants, less than one percent had not completed any education, twenty six percent had completed high school, fourteen percent had done trade/ technical/ vocational training, twenty two percent had undergraduate degrees, twenty four percent had graduate degrees, and fifteen percent had postgraduate degrees. The demographics of our participants are summarised in Figure 2.

4.2 Security Decision-Making

We asked our interview participants questions regarding their security decision-making process in order to identify factors that influence the outcome of such decisions. In addition to other factors (knowledge and skill, inconvenience, cost, trust, and influence) that have been reported by other studies before (ref. Section 2), we identified three other areas that have not been explored yet. These include survival/outcome bias, other factors that induce or undermine one's confidence in a security measure, and the availability and quality of support. We discuss these in detail below.

4.2.1 Survival/Outcome Bias

Our analysis of the interviews reveals a tendency for participants to concentrate on practices that have survived security breaches, and to overlook those that have not. This was a reason some participants gave for not implementing recommended security measures. They believe that as long as something bad has not happened yet, they are safe: *"For me, until something happens, I will be safe"* - P4.

Even in the face of a security concern, some participants report not engaging in security action because *"I think it's probably the fact that as far as I'm aware of, I haven't had serious breaches of personal data, or data security breaches. Not that I'm aware of, no. I think if I was exposed to something which was quite serious, then I would probably change my look quite a lot"* - P6 or *"I don't think I have because I have not had any reason to. That's why personally I just feel like as long as it has not done anything that would cause direct harm to like my information or anything like that, [it is secure]. I haven't felt the need to do any other security check to keep up with any security information because I haven't experienced anything that would cause me to do that. So I feel like until I have that experience with maybe an application, then I might either delete the application, or look for some security measures that I might take"* - P1.

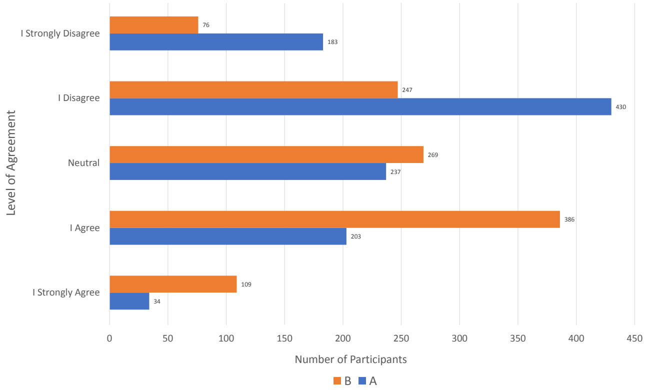


Figure 3: Survival/Outcome Bias

While realising that statistical validation of this factor requires some complex and detailed study design as shown in [4], we crafted a scenario to make a preliminary exploration of the availability of this factor. We presented the respondents with two options, both indicating survival/outcome bias. Shown below is the scenario:

> For the past 5 years, your friend John has been downloading free music, videos, and software from different websites including torrent sites without any problem. One day, he reads an article about the dangers of free downloads such as viruses, adware, Trojan horses, worms and spyware. For each of the following options, how much do you agree that it is a good choice for John?
> A - *Continue downloading free files from any website as usual. He has been doing it for 5 years without a problem, chances of being affected are very small.*
> B - *Restrict the downloads to those websites John has already used before. He has used them for 5 years without a problem, he trusts them to be secure.*

The options were evaluated on a 5-point Likert scale ranging from Strongly Disagree to Strongly Agree. The results showed that about 22% agreed with option A, while about 46% of the participants agreed with option B (cf. figure 3). While there was a statistically significant difference between options A and B ($Z = -18.058, p = 0.000$), our aim was to make an *initial exploration of the availability of survival/outcome bias*, and not to study types or levels of survival/outcome bias, or factors that affect the construct.

4.2.2 Other Factors That Induce or Undermine Confidence in a Security Measure

In our analysis of the interviews, we found that where a security measure was in place and the participants were confident in it's effectiveness, they would trust the service or action to be secure; *"With financial, there was one time when my credit card was charged to two transactions that I did not recognise. I immediately contacted the bank, and I was able to describe why I couldn't recognise them, and the bank believed me and refunded my money... That made me confident in using online shopping, and financial services"* - P7 ... and similarly *"I am less concerned about banking because I find that the banking services I use to be secure, and I am often reassured by the fact that if something were to go wrong, the bank is likely to compensate me for any fraud or any security breaches that would result in the loss of my money"* - P21. This confidence is not always to do with security measures implemented by a service provider however; *"If they have got work stuff on their laptop, or they are one of those people that have a word document with all their passwords on it, people do that, then I would probably advise them to think about high level security, or at least password-protecting files because I think it's very interesting that there has been an increase in people holding data hostage, and say pay us this, and you can have your files back. That for me would be like, ok you can keep it. I am not that bothered. Any photos I have got are uploaded to the cloud, there is nothing on my desktop that I need that can't be replaced. But for a lot of people, that obviously is not the case."* - P5.

To explore this factor, we crafted the following scenario:

> Your friend Felicity is a college student. She owns a laptop. She stores assignments and study materials on it. Felicity visits her friend, Laurel, whom she finds watching a very interesting movie. Felicity asks Laurel if she can share the movie with her, as well as some of the music Laurel downloaded. Laurel copies all the files to a USB stick, and hands it over to Felicity. On their way out, Laurel tells Felicity that she thinks her laptop might have a virus because she could not open one of her word documents to study, and this has happened to her a number of times. For each of the following options, how much do you agree that it is a good choice for Felicity?
> A - *Felicity could copy the movie and music to her laptop. Laurel probably got a corrupted file, there is nothing to fear.*
> B - *Felicity could copy the files to her laptop. She has an antivirus which will keep her data secure.*
> C - *Felicity could take and maintain a backup of her files in a USB stick, phone storage, cloud storage, external drive, another computer, etc. She could hence copy the movie and music to her laptop. She can always get the files from the backup when needed.*

We introduced option *A* to indicate taking no action, here serving the purpose of a control variable. The other two options, *B* and *C*, were used to test the participants' confidence in the implemented security measures and the subsequent behaviour following from their confidence. These options were also evaluated on a 5-point Likert scale ranging from Strongly Disagree to Strongly Agree. The results (cf. figure 4) showed that about 14% agreed with option A, about 26% agreed with option B, and about 46% agreed with option C.

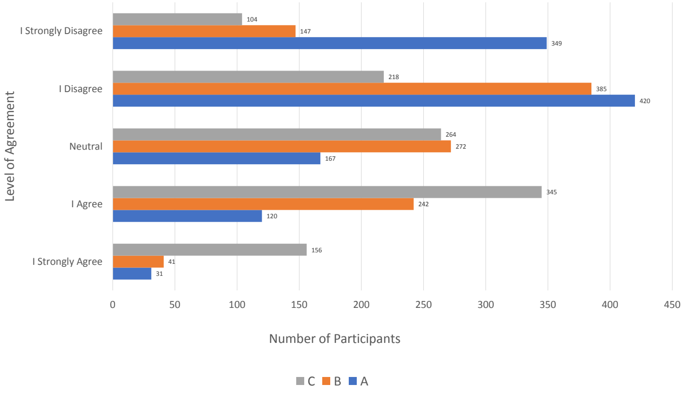


Figure 4: Confidence in a Security Measure

A Wilcoxon signed-rank test showed that the introduction of an antivirus in *B* resulted in a significant statistical difference between option A and B ($Z = -16.473, p = 0.000$). Similarly, the Wilcoxon signed-rank test showed a significant difference between options A and C ($Z = -21.855, p = 0.000$), where a backup was introduced as a security measure. While there was also a significant statistical difference ($Z = -14.497, p = 0.000$) between options B and C, it was not our aim to compare different security solutions, and we hypothesize that this might have occurred due to the participants' perceptions, preferences, needs and experiences.

4.2.3 Availability and Quality of Security Support

Our analysis of the interviews surrounding security decision-making in the home revealed that our participants constantly need support in their endeavour to be secure. Previous studies have explored support in terms of security advice or information [38, 37, 21, 34]. While this is a common trend, there is evidence [3, 33, 17, 27] of a low success rate of such form of support. We thus set out to first identify the kind of support that is needed or exists in the home regarding security. Our analysis revealed a number of different kinds of support currently present and/or needed in the home: *information, advice, and technical help.*

While there might be some differences between information and advice, we noted that participants treated the two as the same. This challenge is also seen in other studies [38, 34] that have been done on this topic, where they interchangeably refer to the two without any difference. To avoid introducing discrepancies in the results, we therefore treated these two as one, and referred to it broadly as security advice. Our analysis pointed out the following kinds of advice that our participants talked about:

- Advice on available security tools or controls
- Reviews about a particular security tool or control
- Information on the cost of protection
- Opinion or recommendation for a particular security-related action, e.g. permissions requested by applications
- Advice on privacy settings
- The risks for a specific environment, service, or tool
- Where they can get support with a particular problem

Technical support was reported to be common mostly among the social circles of the participants. This included some aspect of responsibility where someone, who is perceived to be more competent or feels responsible, assumed the responsibility of making security decisions on behalf of others (that is, decide and act on their behalf). Parents for example reported making decisions for or offer advice to their children; *"I give that [advice] as a concerned parent just as I would encourage them to look both ways when they cross the road. They don't ask me for that advice."* - P4, *"I don't think anyone is really responsible for the household. Myself and my wife will have some say in what the children can or can't do on their devices. But no one person is responsible for that."* - P30; friends on behalf of their friends, *"One of my friends is good with computers. He does all the security stuff for me when he comes."* - P48.

We were particularly interested in how participants choose where to seek this support and/or whether or not to accept any unsolicited support that is offered to them. In this regard, we identified five factors that are used to assess a source and/or the quality of support: perceived competence, trust, availability, cost, and closeness to a source.

i. Perceived Competence: The notion of *better than me* was common among the participants when talking about a source of security support. We understood this to mean the perceived competence of the source of support; and 91% of the survey participants agreed to consider competence in seeking or offering support. The participants reported making a comparison between their self efficacy and the perceived competence of a potential source.

We sought to identify the metrics that are used in this comparison, or in other words, how the different participants understand competence in security. Our interview results showed that for some it means someone who *works in data security*; 86% of the survey participants nodded to this. For others, it means someone who *works for a technical company*, regardless of whether their job is technical or not; 24% of the survey participants agreed to consider this metric. More than that, it also means someone *whose job is technical*; 24% of the survey participants agreed with this.

Another metric used in assessing someone's competence involves identifying someone with *more experience in using technical devices than the one seeking help*; 51% of our survey participants agreed with this. 27% consider someone who *has studied/studies* a technical course. 7% go for someone who is *more educated than the one seeking help.* 78% said they choose someone who *has studied/studies data security.* 39% seek help from those who have *experienced a data security incident before*; and only 4% said they do not consider any of these factors when choosing a source of support. The survey participants were asked to select more than one metric they consider, hence the percentages total more than 100.

In addition to selecting the metrics the participants consider in assessing the competence of a potential source of support, we also asked the participants to rank these metrics in order of preference. A Friedman Test on the metric rankings showed that there was a statistically significant difference ($X^2(7) = 3218.784, p < .05$). Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni correction applied, resulting in a significance level of $p = 0.002$. There were no significant differences between options A and D ($Z = -.339, p = 0.735$), or between A and H ($Z = -1.320, p = 0.187$), or between B and H ($Z = -1.744, p = 0.081$), or between D and H ($Z = -1.646, p = 0.100$); however, B was ranked higher than A ($Z = -4.662, p = 0.000$), and higher than D ($Z = -3.909, p = 0.000$). The overall ranking is:

1. F: He/she works in data security.
2. G: He/she studied or studies data security.
3. C: He/she has more experience than you in using or working with technical devices and services.
4. B: His/her job is technical.
5. A,D,H (A: He/she works for a technical company; D: He/she studied or studies a technical course; H: He/she has experienced a data security incident before.)
6. E: He/she is more educated than you.

ii. Trust: Previous studies [38, 37, 31] reported that trust plays a role when users choose a source of security advice. Similarly, our study found that trust influences the choice of a source of support among our participants. Characterising this in our study was the availability of a social relationship between those involved. This is also reflected in the preferences of a source of support, discussed in 4.3.1. When seeking advice for instance, *"because they are my closest friends and I kind of trust what they have to say. I know that they give me an honest opinion"* - P29; and *"they are my parents. So I am their closest relation. I think they trust me a lot"* - P2. 89% of the survey participants indicated considering trust when they seek or accept security advice or help.

iii. Cost: Our study confirmed what other researchers [21, 31] have reported about the importance of cost in security. We went further to identify two dimensions of cost among our participants that are considered in deciding when, and where to seek support. First, *cost to the one seeking help*, which includes money, favours, and gifts. Second, there is *cost to the source of support*, which is characterised by effort, and inconvenience. These dimensions were evident in reported (from interviews) security support sought and offered among the social relationships of the participants. In the survey, we asked the participants to choose which of the two they took into consideration when choosing a source of support. 49% indicated that they consider the cost to the one seeking support as an important factor, and 36% consider the cost to the source of support to be a significant factor.

iv. Closeness: When we tried to find out about the sources of security support in the home in our interviews, one thing that was not clear was whether the preference of the sources was determined by (constant) availability of the source, or how close one is to the source. Phrases such as "my friends", "my dad", and "my work colleague" could not explicitly clarify which of the two was in play. When asked why they chose such sources, the common responses were "because they are better than me", "they know me", or "I trust them". We hence separated the two, *closeness* and *availability*, and surveyed them as separate factors. 31% of the survey participants indicated that they consider closeness as a significant factor in selecting a source of and accepting support for their security.

v. Availability: Our analysis of the interviews indicates a common pattern in the sources of security support, be it advice or technical help. Such consistencies included friend-to-friend, parent-to-child, between couples or within a family, among work colleagues, and client-to-commercial IT Services Professional. In the survey, we asked the participants if constant availability of a potential source of support is an important factor. 31% of the participants indicated that they consider availability as a significant factor.

Only 1% of the survey participants indicated that they do not consider any of these factors when selecting a source of security support. We also asked the participants to rank these factors in order of preference. A Friedman Test on the ranked factors showed that there was a statistically significant difference ($X^2(5) = 2444.265, p<.05$). Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni correction applied, resulting in a significance level of $p = 0.003$. There was no significant difference between *availability* and *cost to you (money, favour, gifts, etc)* ($Z = -.835, p = 0.404$). The overall ranking therefore is as shown below:

1. Competence
2. Trust
3. Availability and Cost to you (money, favours, gifts)
4. Closeness
5. Cost to the source of advice/help (effort, inconvenience)

In the next section, we discuss what characterises security support in the home. We detail the how the evaluation of the five factors discussed in this section impact the sources of support, and the reasoning behind the choices and practices.

4.3 Characteristics of Security Support

Our analysis of the interviews reveals that participants mostly had the same sources for advice and technical help. These included family, friends, work colleagues, service providers, and IT repair shop professionals; with family and friends being the most common source. This corroborates other studies [38, 37, 11, 17]. Other sources include search engines (*"I searched online for people with the same problem and got many results. People gave many solutions and I tried several of them until I got one that seemed to work."* - P23), and specific websites (*"Sometimes you go to sites that you think are credible like stackoverflow... some credible sites or sites that look credible to me. I just read about what people have experienced and how they went about it."* - P11).

None of the sixty five interviewees cited any security awareness websites as a source of security advice. We did not expect our participants to recall details of websites they visit for security information, but this is consistent with the findings of Furnell et al. [17], who found that the majority of their respondents had not heard of public awareness websites (including Get Safe Online: https://www.getsafeonline.org/, and Webwise: http://www.bbc.co.uk/webwise).

Our analysis shows that the preference and choice of a source or recipient of security support in the home is characterised by two main attributes: duty of care and continuity of care.

4.3.1 Duty of Care

Participants consider security support in the home a moral obligation to ensure the safety or well-being of others. This duty of care is expressed through the following modalities.

i. Delegation: As explained in section 4.2.3, support for security in the home involves seeking or accepting advice, but also encompasses users taking security responsibility for others to ensure their well-being. We found that some people delegate the responsibility for security to competent, and trusted others; a result shared by Dourish et al. [11], who found that people *"delegate to another individual, such as a knowledgeable colleague, family member, or roommate"*. Some of our participants said; *"Me! Mum always. I guess because my husband thinks I'm more knowledgeable about computers and about settings for the internet"* - P7; and*"Oh! My husband, because he has always been keen on computers and adopting technology, and that is a big part of his work. So he is the one who does that [all security tasks]"* - P45. A similar finding is also presented in [31], *"There is a friend who usually comes here. Mostly he is the one. If the laptop has a virus, I give it to him."*

ii. Motivation: A second way in which duty of care is expressed is by motivating others to behave securely. This generally includes offering unsolicited support. Our interview data shows two aspects of unsolicited support: 1) when somebody notices a practice they believe to be insecure and they intervene (e.g. *"they just feel like they can send a young person like 'go and check my email', and they give you all the details to check the emails and I'm like, it's supposed to be private."* - P1); and 2) when there is nothing specifically wrong but support is offered (e.g. *"My parents, I do advise a lot about different security issues. They are just aware of it"*- P43). Unsolicited support without noticing a particular need was common in cases where there was delegation and participants felt responsible for the security of another.

We asked survey participants how likely they are to offer unsolicited advice and technical help to someone they believe to be less competent in security than them. Since the interviews show that this practice is common among relatives, friends, and colleagues, we sought to explore in our survey how widely held such behaviour is. Our survey shows that about 56% of the respondents are likely to offer unsolicited support to a relative; about 47% to a friend; about 27% to a work colleague; and about 12% to other sources.

We also asked the participants to rank who they would likely offer unsolicited support to, in order of preference. A Friedman Test on the ranked order of preference showed that there was a statistically significant difference ($X^2(3) = 2127.517, p<.05$). Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni correction applied, resulting in a significance level of $p = 0.008$. The overall ranking in order of preference is as shown below:

1. Relative
2. Friends
3. Work colleague
4. Others

But offering unsolicited support is only one side of the coin – to fully explore this, we also asked participants how likely they are to accept unsolicited advice or help with data security from different sources of support. About 63% of respondents reported being likely to accept it from a relative; 63% from a friend; 48% from a work colleague; 44% from a service provider/manufacturer help desk; 40% from an IT repair shop professional; and about 12% from other sources.

We asked the participants to rank these sources in order of preference. A Friedman Test on the ranked sources of support showed that there was a statistically significant difference ($X^2(5) = 1987.664$, p<.05). Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni correction applied, resulting in a significance level of $p = 0.003$. There were no significant differences between Relatives and Friends ($Z = -2.153, p = 0.31$), or between Work colleague and Service Provider/manufacturer help desk ($Z = -1.990, p = 0.047$). The overall ranking in order of preference is as shown below:

1. Relatives and Friends
2. Work colleagues and Service Provider/Manufacturer help desk
3. IT repair shop professional
4. Others

We sought to understand the extent of care and intervention in cases where the participants notice a practice they believe to be insecure, and crafted the following scenario:

> Assume you have a sister named Vanessa, and you believe her to be less competent than you in data security. One day you visit her, and while you use her laptop, you notice that her antivirus is not set to automatically scan removable media, such as USB sticks, when they are plugged in. For each of the following options, how much do you agree that it is a good choice?
> A - *Change the settings of the antivirus to enable auto-scan of removable media, and say nothing.*
> B - *Change the settings of the antivirus to enable auto-scan of removable media, and tell Vanessa what you have done.*
> C - *Leave the settings as they are. It is Vanessa's choice to disable auto-scan.*
> D - *Leave the settings as they are. It is not your responsibility.*
> E - *Ask Vanessa why auto-scan is disabled.*

The results showed that 27% of the participants agreed with option A; 68% with option B; 23% with C; 19% with D; and 90% with option E. A Friedman Test on the ranked order of preference showed that there was a statistically significant difference ($X^2(4) = 1634.910, p$<.05) in the choice of the options. Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni correction applied, resulting in a significance level of $p = 0.005$. The overall ranking in order of preference is:

1. E: Ask Vanessa why auto-scan is disabled.
2. B: Change the settings of the antivirus to enable auto-scan of removable media, and tell Vanessa what you have done.
3. C: Leave the settings as they are. It is Vanessa's choice to disable auto-scan.
4. A: Change the settings of the antivirus to enable auto-scan of removable media, and say nothing.
5. D: Leave the settings as they are. It is not your responsibility.

iii. Social Responsibility: As evidenced in the last scenario regarding responsibility towards the security of others, option D received the least agreement (19%), and was the lowest ranked. Our interviews reveal that participants consider security support in the home as an obligation to act for the benefit of *society*. What is more interesting is the scope of this society; who do the participants consider part of their *security/secure society*? "I give it [security advice] to a certain level... I am not an expert in security, but people ask me and I tell them my thoughts... *whoever* asks me... *anyone*.. I mean *colleagues at work, my friends, my relations*" - P40. "[I give advice] to help her... [and to] *everyone if I know them* and I am sympathetic to them" - P36.

We asked our survey participants how likely they are to seek advice or help from a source of support that they believe to be more competent than them. The sources included relative, friend, work colleague, service provider /manufacturer help desk, IT repair shop professional, and others. We found that about 80% are likely to seek advice or help from a relative; about 85% from a friend; about 71% from a work colleague; about 58% from a service provider/manufacturer help desk; about 51% from an IT repair shop professional; and about 16% would seek support from other sources.

We also asked the participants to rank these sources in order of preference. A Friedman Test on the ranked order of preference showed that there was a statistically significant difference ($X^2(5) = 2066.482, p$<.05). Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni correction applied, resulting in a significance level of $p = 0.003$. There was no significant difference between Relatives and Friends ($Z = -0.684, p = 0.494$). The overall ranking in order of preference is as shown below:

1. Relative and Friend
2. Service provider/Manufacturer help desk
3. Work colleague
4. IT repair shop professional
5. Others

There is a significant difference ($Z = -5.618, p = 0.000$) in the likelihood of seeking support from a work colleague (71%) and a Service Provider/manufacturer help desk (58%). However, the rankings indicate a significant difference in reverse; the Service provider/Manufacturer help desk was preferred over a work colleague. We hypothesize this might be because 1) some service providers or device manufacturers do not provide support with security, and 2) the range of services and devices available in homes is too broad, and expecting participants to go to many service providers and manufacturers for assistance is contrary to the finding in [11] where users expect a unitary solution to security problems.

Given the common trend during the interviews where most of the participants indicated that they seek support from friends, relatives, and work colleagues, we wanted to know how likely our participants are to offer support to those that approach them for help. Asked how likely they are to offer advice or technical help when asked by someone they believe to be less competent than them in data security, the results showed that about 80% would likely offer support to a relative; 78% are likely to help a friend; 67% are likely to assist a work colleague; and 41% are likely to offer support to any other people who seek it from them.

4.3.2 Continuity of care

The second characteristic of support in the home that we identified from the interviews is continuity of care. Our participants look for a continuous caring relationship with an identified competent and trusted individual. This is evidenced by the preference for availability (ranked third from competence and trust), as shown in section 4.2.3. From our analysis, two reasons explain this need: 1) In the case of delegation, one needs someone who will be constantly available, and as [11] also reports that people used to delegate to a "person who had helped them in a previous context, such as in discussing what to get, helping them set up the computer, etc.", and similarly *"I was involved in helping them set up in the first place... I helped a lady buy a computer, I helped her to get it online. So she comes to me all the time for information and she keeps asking me questions. I consult and then go back to her"* - P36; and 2) If something goes wrong as a result of the support someone offered, the victim can easily go back and seek further assistance.

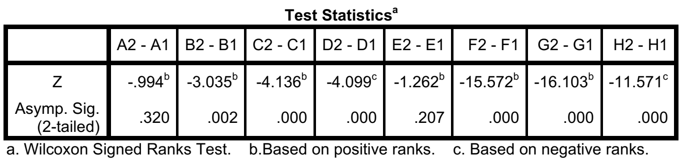
Our study showed that participants are likely to take responsibility for consequences resulting from support they offered; *"I may help to solve the problem"* - P28, *"I would consider that as my responsibility, if it was compromised"* - P47. To verify how widely shared this belief and practice is, we crafted two scenarios: one without indicating that a compromise was due to advice that the participant might have given; the second indicating that the compromise was due to advice that they had offered beforehand. We presented the participants with the same answers to both scenario so that we could test the significance of the difference in taking or accepting responsibility. The first scenario read:

> Assume you have a friend, Catherine, who you believe to be less competent than you in data security. She comes to you for help because she had corrupted files on her computer and thinks she has a virus. What would you do?
> A - *Do nothing.*
> B - *Fix it, if you feel you can.*
> C - *Tell Catherine what to do to fix the problem herself, if you know the solution.*
> D - *Tell Catherine to look for help elsewhere if you feel/find that you cannot fix it.*
> E - *Arrange for a trusted contact to fix it, if you feel/find that you cannot.*
> F - *Arrange for a third party to fix it. You offer to pay.*
> G - *Arrange for a third party to fix it. You offer to help pay (share the cost).*
> H - *Arrange for a third party to fix it. You expect Catherine to pay.*

The results showed that 3% of the participants agreed with option A; 87% agreed with B; 70% agreed with C; 81% agreed with D; 73% agreed with E; 7% agreed with F; 7% agreed with G; and 56% agreed with option H.

While maintaining options A - H, we then presented respondents with an updated scenario as follows:

> Assume you have a friend, Catherine, who you believe to be less competent than you in data security. She comes to you for help because she had corrupted files on her computer and thinks she has a virus. You recall that three months ago, Catherine was trying to install a piece of software, but was failing. She asked for your help. You were busy and told her the antivirus was the problem, and to try turning it off. You now notice the antivirus is off. What would you do?



Test Statistics[a]

	A2 - A1	B2 - B1	C2 - C1	D2 - D1	E2 - E1	F2 - F1	G2 - G1	H2 - H1
Z	-.994[b]	-3.035[b]	-4.136[b]	-4.099[c]	-1.262[b]	-15.572[b]	-16.103[b]	-11.571[c]
Asymp. Sig. (2-tailed)	.320	.002	.000	.000	.207	.000	.000	.000

a. Wilcoxon Signed Ranks Test. b.Based on positive ranks. c. Based on negative ranks.

Figure 5: Test for continuity of care

The results showed that 4% agreed with option A; 90% agreed with option B; 74% agreed with option C; 79% agreed with option D; 77% agreed with option E; 21% agreed with option F; 28% agreed with option G; and 40% agreed with option H.

We ran a Wilcoxon signed-rank test against respective pairs of options to check if the changes in the responses were significant. The test showed significant changes in options B, C, D, F, G, and H. These results are summarised in figure 5, where the options are presented as $x1$ for options from the first scenario, and $x2$ for options from the second scenario; where x represents the respective letter for a given option.

5. DISCUSSION

5.1 Evaluating Security Decisions and Support

Our study has uncovered that participants look for evidence, specifically impact, of security problems for them to feel motivated to practice security. The perceived absence of harm (to themselves or their social circles) is seen as evidence of good security decisions. However, harm arises only when an attack is attempted and then successful: a perceived lack of harm is not sufficient evidence to validate a good security decision for the following reasons.

First is the case where harm occurred but was not perceived by the home user: for instance a user might download malware that steals information in the background without their knowledge. Another instance where the perception of harm can fail is in the situation where a successful attack harms a third party outside the notice of the home user: publicised examples of this are the DDoS attack on DyN DNS servers [5] through compromised IoT devices and the 2014 Lizard Squad attack on XBox live and the Playstation Network [26] through compromised home routers.

Second is the case where harm genuinely did not happen, however this is not always evidence of a good security decision either. In the case where no attack was attempted, a lack of harm is no evidence of effectiveness: vulnerabilities might still be exploitable or countermeasures ineffective. Another situation is where an attack was attempted, but was stopped by a third party before material harm occurred. For instance, a home users' credit card details might have been stolen while shopping on an illegitimate website, but the bank stopped the attacker from using the details.

Only in the third case, where attempted attacks are genuinely mitigated down to no harm, does the perceived absence of harm actually demonstrate evidence of a good security decision. We believe that this is strong evidence that survival/outcome bias is a key element in poor security decisions, and that the wider challenge of evaluating a good security decision is a difficult problem for home computer users (and arguably the wider security community).

Related to the difficulties of evaluating good security decisions is the challenge that home users face when evaluating the competence of those they seek support from. For example, participants reported that the ability to use technical devices better than them was used to support the assessment of competence, however this is not clear evidence of security competence. This problem is somewhat mitigated when home users seek support from people within their social circles, where trust and remedial help may be available in the case where problems arise. However, outside of established relationships and remediation, the challenge remains difficult for home users in telling the difference between a genuinely competent individual, an incompetent individual (who may or may not be aware of the fact), and in the worse case a malicious attacker seeking to take advantage by masquerading as a helpful individual.

Home users need to be able to evaluate the quality of a security decision or source of support. In the absence of clear indicators of quality, a variety of different practices have emerged, yet their effectiveness is questionable. A key challenge remains to uncover the means of making quality more evident to non-experts both for security products/practices, and for the skills, knowledge, and characteristics of those who offer support. This is a hard challenge, particularly where such indicators might then be spoofed by malicious actors, however we believe it is still important to work at making good security evident to non-experts considering the wide variety of non-malicious situations where they may need to make a decision or seek support.

5.2 The Role of Social Networks in Home Security

We have explored the role that social relationships play in security practice in the home. While the need for continuity of care may seem odd, it also reflects common security practices in organisational settings. Even though employees are offered security training and awareness, there are usually support people to whom they can turn to when they have issues. In addition to resolving problems, security support is also responsible for carrying out proactive security activities such as firewall configuration, system patching, network monitoring, and many more. In contrast to this, every home is considered to be responsible for its own security, whether it is competent to do so or not. As a result, a wide variety of different practices exist around seeking and giving support for security in the home context. As Dourish et al. [11] observe, the knowledge and skill of a trusted and competent person is one element of a person's defense against potential threats. In this paper, we have discussed social relationships in the context of informal support networks that exist in the home environment. We postulate that these existing networks can be leveraged to provide appropriate and relevant support to home users.

Prior work has investigated how the security behaviour of home users can be changed. Different improvements to security awareness techniques have been proposed and tested, yet evidence [17] shows that despite claims of being aware, home users still do not practice security. One reason for this is that while awareness might impart knowledge, it does not cover skills; a very essential aspect of security practice. Based on our findings, we argue that the *security posture* of the home is more likely to improve by targeting the support network rather than the user directly for two reasons:

First by targeting the support network, change is introduced at the point where security work is more likely to occur. We believe that by providing tools, training, education, and incentives to those who provide help to others, there is a better chance of achieving a measurable beneficial change to the security of homes.

Second, given the importance of social relationships and the trust placed in the support networks of home computer users, we believe that leveraging these is also a promising approach for transferring both security knowledge and skills to home computer users. Owing to the cost of building a support infrastructure that meets all the requirements discussed in this paper, we believe a fruitful approach is to investigate how social relationships could be leveraged through collaborative technology, social media, and training that focuses on building independent competent communities.

6. CONCLUSIONS

Our research has focussed on the key role of social relationships in home data security, and the reasons behind these informal support networks. We have also uncovered two important factors that explain why some home users do not behave securely: *outcome bias* and *confidence in security measures*. Based on our findings, we put forward the following recommendations:

Leverage existing social relationships: While awareness is important, current practice has focussed on improving the security awareness of individuals or end-users. We suggest focussing on finding ways of targeting existing informal networks of support: building competence, targeting tools, and fostering a sense of trust and recognition. This leverages two characteristics of support currently sought in the home – duty of care and continuity of care.

Simple and useful tools: We need more tools targeted at home users. First, tools that non-experts (especially the existing informal support workers) can use to manage security configurations for different devices and services in the home. Currently, the proliferation of networked devices and services in the home makes the task of managing security complex, and security configurations need to be done on each and every device and service separately. As Dourish et al [11] state, people expect a unitary solution to a number of security problems. Developing tools to manage security configurations of a number of devices and/or services centrally would motivate home users and simplify this task.

Second, tools need to be developed to help the informal support workers that currently assist home users. This might include remote assistance, network monitoring, or incident management tools. It is important to note that this also raises a wide variety of different challenges pertaining to consent, privacy, and standards of care, in addition to fundamental security considerations.

Evidence-based security: Finally, our work has shown that home users look for evidence of harm to evaluate the quality of their security decisions, and to be motivated to make changes. We hypothesise that this might be due to current mechanisms failing to effectively convey knowledge of an attempted or successful incident. This suggests that there is a need to find ways of detecting and communicating (in a simple, concise, and understandable manner) any attempted, successful, and failed attacks.

7. ACKNOWLEDGMENTS

This work was supported by the Research Institute in Science of Cyber Security (RISCS) under grant No. BLR01330, and grant No. BLR01790. Recruitment of participants was done in collaboration with the National Museum of Computing, and Community Centres in Oxford. Norbert is funded by the Rhodes Scholarship (Malawi & Linacre, 2015) and the Oxford-Linacre African Scholarship (2015/16).

8. REFERENCES

[1] C. L. Anderson and R. Agarwal. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *Mis Quarterly*, 34(3):613–643, 2010.

[2] AOL/NCSA. Online safety study. https://library.educause.edu/resources/2004/1/aolncsa-online-safety-study, 2017. Online; accessed on 25-August-2017.

[3] K. Aytes and T. Connolly. Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing (JOEUC)*, 16(3):22–40, 2004.

[4] J. Baron and J. C. Hershey. Outcome bias in decision evaluation. *Journal of personality and social psychology*, 54(4):569, 1988.

[5] BBC. Smart home devices used as weapons in website attack. http://www.bbc.co.uk/news/technology-37738823, 2016. Online; accessed on 03-April-2017.

[6] A. Beautement, I. Becker, S. Parkin, K. Krol, and A. Sasse. Productive security: A scalable methodology for analysing employee security behaviours. In *12th Symposium on Usable Privacy and Security (SOUPS)*, 2016.

[7] P. Biernacki and D. Waldorf. Snowball sampling: Problems and techniques of chain referral sampling. *Sociological methods & research*, 10(2):141–163, 1981.

[8] S. Das, T. H.-J. Kim, L. A. Dabbish, and J. I. Hong. The effect of social influence on security sensitivity. In *Proc. SOUPS*, volume 14, 2014.

[9] S. Das, A. D. Kramer, L. A. Dabbish, and J. I. Hong. Increasing security sensitivity with social proof: A large-scale experimental confirmation. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pages 739–749. ACM, 2014.

[10] Z. Dong, V. Garg, L. J. Camp, and A. Kapadia. Pools, clubs and security: designing for a party not a person. In *Proceedings of the 2012 workshop on New security paradigms*, pages 77–86. ACM, 2012.

[11] P. Dourish, R. E. Grinter, J. D. De La Flor, and M. Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6):391–401, 2004.

[12] ENISA. Mirai malware, attacks home routers. https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers, 2016. Online; accessed on 03-April-2017.

[13] R. J. Fisher. Social desirability bias and the validity of indirect questioning. *Journal of consumer research*, 20(2):303–315, 1993.

[14] O. for National Statistics. Internet access - households and individuals 2015. http://www.ons.gov.uk/ons/dcp171778412758.pdf, 2017. Online; accessed on 01-April-2017.

[15] A. Forget, S. Pearman, J. Thomas, A. Acquisti, N. Christin, L. F. Cranor, S. Egelman, M. Harbach, and R. Telang. Do or do not, there is no try: user engagement may not improve security outcomes. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 97–111, 2016.

[16] M. Friedman. A comparison of alternative tests of significance for the problem of m rankings. *The Annals of Mathematical Statistics*, 11(1):86–92, 1940.

[17] S. Furnell, P. Bryant, and A. D. Phippen. Assessing the security perceptions of personal internet users. *Computers & Security*, 26(5):410–417, 2007.

[18] A. M. Gadermann, M. Guhn, and B. D. Zumbo. Estimating ordinal reliability for likert-type and ordinal item response data: A conceptual, empirical, and practical guide. *Practical Assessment, Research & Evaluation*, 17(3), 2012.

[19] B. G. Glaser and A. L. Strauss. *The discovery of grounded theory: Strategies for qualitative research.* Transaction publishers, 2009.

[20] P. Gutmann. Applying problem-structuring methods to problems in computer security. In *Proceedings of the 2011 workshop on New security paradigms workshop*, pages 37–44. ACM, 2011.

[21] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, pages 133–144. ACM, 2009.

[22] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne. The psychology of security for the home computer user. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 209–223. IEEE, 2012.

[23] I. Ion, R. Reeder, and S. Consolvo. "... no one can hack my mind": Comparing expert and non-expert security practices. In *SOUPS*, pages 327–346, 2015.

[24] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. Teaching johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, 10(2):7, 2010.

[25] Y. Li and M. T. Siponen. A call for research on home users' information security behaviour. In *PACIS*, page 112, 2011.

[26] P. Lunsford and M. C. Boahn. How the lizard squad took down two of the biggest networks in the world. 2015.

[27] M. S. Mendes, E. Furtado, G. Militao, and M. F. de Castro. Hey, i have a problem in the system: Who can help me? an investigation of facebook users interaction when facing privacy problems. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 391–403. Springer, 2015.

[28] A. J. Nederhof. Methods of coping with social desirability bias: A review. *European journal of social psychology*, 15(3):263–280, 1985.

[29] B.-Y. Ng and M. Rahim. A socio-behavioral study of home computer users' intention to practice security. *PACIS 2005 Proceedings*, page 20, 2005.

[30] M. Nouh, A. Almaatouq, A. Alabdulkareem, V. K.

Singh, E. Shmueli, M. Alsaleh, A. Alarifi, A. Alfaris, et al. Social information leakage: Effects of awareness and peer pressure on user behavior. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 352–360. Springer, 2014.

[31] N. Nthala and I. Flechais. "if it's urgent or it is stopping me from doing something, then i might just go straight at it": A study into home data security decisions. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 123–142. Springer, 2017.

[32] N. Nthala and I. Flechais. Rethinking home network security. In *European Workshop on Usable Security (EuroUSEC)*, 2018.

[33] B. P., F. S.M., and P. A.D. Improving protection and security awareness among home users. *Advances in Networks, Computing and Communications 4*, 2008.

[34] E. Rader and R. Wash. Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, 1(1):121–144, 2015.

[35] E. Rader, R. Wash, and B. Brooks. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, page 6. ACM, 2012.

[36] U. H. Rao and B. P. Pati. Study of internet security threats among home users. In *Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on*, pages 217–221. IEEE, 2012.

[37] E. M. Redmiles, S. Kross, and M. L. Mazurek. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 666–677. ACM, 2016.

[38] E. M. Redmiles, A. R. Malone, and M. L. Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *Security and Privacy (SP), 2016 IEEE Symposium on*, pages 272–288. IEEE, 2016.

[39] J. Rowe, K. Levitt, and M. Hogarth. Towards the realization of a public health system for shared secure cyber-space. In *Proceedings of the 2013 workshop on New security paradigms workshop*, pages 11–18. ACM, 2013.

[40] I. L. Stats. Internet users. http://www.internetlivestats.com/internet-users/, 2017. Online; accessed on 25-August-2017.

[41] A. Strauss and J. Corbin. Basics of qualitative research: Procedures and techniques for developing grounded theory, 1998.

[42] E. U.S. Department of Commerce and S. Administration. Computer and internet use in the united states: 2013. www.census.gov/, 2017. Online; accessed on 01-April-2017.

[43] R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, page 11. ACM, 2010.

[44] R. Wash and E. Rader. Influencing mental models of security: a research agenda. In *Proceedings of the 2011 workshop on New security paradigms workshop*, pages 57–66. ACM, 2011.

[45] F. Wilcoxon and R. A. Wilcox. *Some rapid approximate statistical procedures.* Lederle Laboratories, 1964.

[46] G. B. Willis. *Cognitive interviewing: A tool for improving questionnaire design.* Sage Publications, 2004.

APPENDIX

A. INTERVIEW DEMOGRAPHIC FORM

1. *Age*: a) 12 - 17, b) 18 - 34, c) 35 - 64, d) 65+
2. *Gender:* a) Male, b) Female
3. *Location:* a) Rural, b) Suburban, c) Urban
4. *What is the highest level of school you have completed?*
a) No schooling completed, b) Nursery, c) High School, d) Trade/technical/vocational training, e) Undergraduate, f) Graduate, g) Postgraduate
5. *Choose one option that best describes your ethnic group or background:*
a) White, b) Hispanic/Latino, c) Black/African/Caribbean, d) Asian/Pacific Islander, e)Other:
6. *Choose the technology devices you own/use in your home:*
a) Mobile Phone, b) Telephone, c) Tablet/iPad, d) Laptop, e) PC, f) Game Console, g)TV, h) Camera, i) Wearable device, j) Other:
7. *Choose the services you use:*
a) Online/Mobile banking, b) Online shopping, c) Social networking, d) Communication, e) Education, f) Entertainment, g) Work, h) Home security, i) TV streaming, j) Health services, k) Other:
8. *How would you rate your general skills in using technology devices, services, and applications?*
a) Novice, b) Competent, c) Expert
9. *How would you rate your general skills in computer security and privacy (e.g. understanding threats, vulnerabilities, and countermeasures)?*
a) Novice, b) Competent, c) Expert
10. *Would you briefly describe the composition of your household?*
A. Marital status: a) Single, b) Married, c) Widowed, d) Divorced, e) Separated
B. Number of people in your household:
C. Relationship with other residents:
D. Age ranges of other residents:
E. Employment status: a) Student, b) Employed, c) Retired, d) Self-employed, e) Not working

B. INTERVIEW GUIDE

B.1 Introductory questions

1. Can you rank these services in order of importance, from the most important to the least important?

B.2 Data Security Concerns and Breaches

2. Do you have any data security concerns with these devices/services/applications?
3. Have you or people you know experienced any data security breaches in the past?

B.3 Security Controls/Tasks

4. What was done to address the data security concerns, and breaches? Who did this?
5. Do you think this was enough to keep your data secure? If not, why?

Open problems in security decision making	Data security concerns	Factors influencing security decisions	Home responsibility
Evaluating the effectiveness or quality of security solution	Loss	Convenience	Source of Support
Unable to have a relevant solution	Loss of control	Cost	Relative
Good Security Practices	Loss of money	Ease of use	Friend
Guidelines and rules for security decision making	Loss of Privacy	Experience	Service provider
Ask the more knowledgeable	Nuisance	Experience in using a security measure	IT shop
Disconnect from the internet when not needed	Uncertainty	Experienced a security breach	Work colleague
Follow advice from a service provider	Security practice	Professional experience	Online forum
Use a tier system of passwords	Insecure practices	Knowledge and skill	Search engine
Don’t give out personal details to someone you don’t know	Secure Practices	Professional - education	Technical help
Responsibility	Non-security-technology practices	Professional job-related experience	Awareness
Attitude - Giving advice and post breach reaction	Pre-emptive practices	Obligation	Identifying risks
Attitude - Problems arising from well-intended individuals	Pro-active Damage Limitation	Survival/Outcome bias	News
Attitude - Responsible stakeholders	Reactive practices	Perceived Competence	Devices
Boundaries of responsibility	Security-technology practices	experience in using or working with technical devices and services	Services
Understanding responsibility	Reactive - Incident Management	Level of education	Anecdotes
Abrogate responsibility	Noticing a breach	Personal negative experience	Incident reporting behaviour
Noticing responsibility	Risk attitude	Studied or studies a technical course	Security evaluation
Taking responsibility	It’s not a risk	Studied or studies data security	Cost of protection
Stakeholders	Not understanding the risk	Technicality of a job	Where to get support
Support	Risk evaluation	Works for a technical company	Reviews
Characteristics of Support	Perceived value of impact	Works in data security	Available security tools or measures to a problem
Continuity of Care	Perceived gain for attacker	Significance	Unsolicited support
Duty of Care	Security incidents experienced	Time pressure (Urgency)	Solicited support
Delegation	Identifying incidents	Trust	Trust evaluating practices
Motivation	Harm	Sharing devices, services and passwords	Relationship with others
Social Responsibility	Security alert	Extent of sharing	Knowledge and skill level
Types of support	Security warning	Purpose of sharing	Closeness to source
Advice	Intuition	Trust cues	Visual cues
Types of advice	Support giving	Availability heuristic	Kinds of information
Opinion	Support seeking	Brand recognition	Confidence in security measure
Recommendation	Availability of support	Interaction	Reviews about a security tool
Information	Quality of support		

Table 1: Grounded Theory Codebook

6. Did you face any problems with the solution?
7. Have you ever adopted or avoided a device/service/application for data security reasons? What prompted you to do this?
8. Have you ever changed settings or abandoned/uninstalled a device/service/application for data security reasons? What prompted you to do this?
9. Is there a particular time when you had data security concerns with a device/service/application but you chose to continue using the device/service/application? Why did you do so?
10. Who is generally responsible for making data security decisions in your home? Why?
11. In the particular scenarios you have mentioned, who made these data security decisions? Why? Were there any difficulties in deciding what to do?
12. If you were to make these decisions for your friend, what would you do? Why?

B.4 Capability and Support

13. Are there any guidelines or rules you follow when making data security decisions? Where do these come from? In the scenarios you mentioned, did you follow these? If not, why?
14. What kind of information/resources do you need when you want to make a data security decision?
15. Where or from who do you seek such information/resources?
16. If you needed advice or technical assistance with data security, where would you seek it?

B.5 Delegation

17. Have you ever given advice/recommendation about data security to other people? Who were they? What kind of advice/recommendation did they want? How much effort did you put in (what did you do)?
18. Why do you think they chose to seek advice/recommendation from you? Why did you give advice/recommendation?
19. Have you made data security decisions and acted on them on behalf of someone? For who was this done? What kind of decisions were these? Why did you do it?
20. If you have given bad advice/recommendation or wrongly decided and acted on behalf of someone and something happened, what would you do? Has this ever happened to you?

B.6 Attitude towards data security

21. Can you give me examples of what you consider good and bad data security (measures/practices)?
22. Who do you think is responsible for implementing this kind of data security in the different devices/services/applications you use?
23. Do you personally follow these measures? If not, why?
24. Do you think any of your actions in using the devices/services/applications could expose other people to data security risks? What are some of these actions and how do you think they might affect others? What do you do about it?

C. SURVEY TOOL

C.1 Demographics

1. Please select your age range: a) 18 - 34, b) 35 - 64, c) 65+
2. Please select your gender: a) Male, b) Female
3. What is the highest educational level you have completed?
a) No schooling completed, b) High school,
c) Trade/technical/vocational training, d) Undergraduate,
e) Graduate, f) Postgraduate

C.2 Survial/Outcome Bias

For the past 5 years, your friend John has been downloading free music, videos, and software from different websites including torrent sites without any problem. One day, he reads an article about the dangers of free downloads such as viruses, adware, Trojan horses, worms and spyware. For each of the following options, how much do you agree that it is a good choice for John?
(Responses: I strongly agree, I agree, Neutral, I disagree, I strongly disagree)
A. Continue downloading free files from any website as usual. He has been doing it for 5 years without a problem, chances of being affected are very small.
B. Restrict the downloads to those websites John has already used before. He has used them for 5 years without a problem, he trusts them to be secure.

How would you rank the options from the scenario above in order of preference?

C.3 Assessing Other's Security Competence

How do you assess if someone is more competent than you in data security? (Please select all that apply.)
A. He/she works for a technical company.
B. His/her job is technical.
C. He/she has more experience than you in using or working with technical devices and services.
D. He/she studied or studies a technical course.
E. He/she is more educated than you.
F. He/she works in data security.
G. He/she studied or studies data security.
H. He/she has experienced a data security incident before.
I. None of the above.

How would you rank the options selected in the question above in order of preference?

C.4 Seeking Support

Assuming you believe each of the following to be more competent than you in data security, how likely are you to seek advice or help with data security from him/her?
(Responses: Very Likely, Likely, Neutral, Unlikely, Very Unlikely)
A. Relative
B. Friend
C. Work colleague
D. Service provider/Manufacturer help desk
E. IT repair shop professional
F. Others

How would you rank the options in the question above in order of preference?

C.5 Accepting Unsolicited Support

Assuming you believe each of the following to be more competent than you in data security, how likely are you to accept unsolicited (not asked for) advice or help with data security from him/her?
(Responses: Very Likely, Likely, Neutral, Unlikely, Very Unlikely)
A. Relative
B. Friend
C. Work colleague
D. Service provider/Manufacturer help desk
E. IT repair shop professional
F. Others

How would you rank the options in the question above in order of preference?

C.6 Giving Solicited Support

Assuming you believe each of the following to be less competent than you in data security, if they ask you for advice or help with data security, how likely are you to offer it?
(Responses: Very Likely, Likely, Neutral, Unlikely, Very Unlikely)
A. Relative B. Friend
C. Work colleague D. Others

C.7 Quality Check

I am randomly answering the questions.
A. Yes B. No

C.8 Giving Unsolicited Support

Assuming you believe each of the following to be less competent than you in data security, how likely are you to offer unsolicited (not asked for) advice or help with data security to him/her?
(Responses: Very Likely, Likely, Neutral, Unlikely, Very Unlikely)
A. Relative B. Friend
C. Work colleague D. Others

How would you rank the options in the question above in order of preference?

C.9 Assessing the Quality and Source of Support

Which of the following do you take into consideration when seeking data security advice or help from someone? (Please select all that apply)
A. Competence
B. Availability
C. Trust
D. Closeness to you
E. Cost to you (money, favours, gifts, etc)
F. Cost to the source of advice/help (effort, inconvenience, etc)
G. None of the above

How would you rank the options in the question above in order of preference?

C.10 Confidence in a Security Measure

Your friend Felicity is a college student. She owns a laptop. She stores assignments and study materials on it. Felicity visits her friend, Laurel, whom she finds watching a very interesting movie. Felicity asks Laurel if she can share the movie with her, as well as some of the music Laurel downloaded. Laurel copies all the files to a USB stick, and hands it over to Felicity. On their way out, Laurel tells Felicity that she thinks her laptop might have a virus because she could not open one of her word documents to study, and this has happened to her a number of times. For each of the following options, how much do you agree that it is a good

choice for Felicity?
(Responses: I strongly agree, I agree, Neutral, I disagree, I strongly disagree)
A. Felicity could copy the movie and music to her laptop. Laurel probably got a corrupted file, there is nothing to fear.
B. Felicity could copy the files to her laptop. She has an antivirus which will keep her data secure.
C. Felicity could take and maintain a backup of her files in a USB stick, phone storage, cloud storage, external hard drive, another computer, etc. She could hence copy the movie and music to her laptop. She can always get the files from the backup when needed.

How would you rank the options in the question above in order of preference?

C.11 Duty of Care

Assume you have a sister named Vanessa, and you believe her to be less competent than you in data security. One day you visit her, and while you use her laptop, you notice that her antivirus is not set to automatically scan removable media, such as USB sticks, when they are plugged in. For each of the following options, how much do you agree that it is a good choice?
(Responses: I strongly agree, I agree, Neutral, I disagree, I strongly disagree)
A. Change the settings of the antivirus to enable auto-scan of removable media, and say nothing.
B. Change the settings of the antivirus to enable auto-scan of removable media, and tell Vanessa what you have done.
C. Leave the settings as they are. It is Vanessa's choice to disable auto-scan.
D. Leave the settings as they are. It is not your responsibility.
E. Ask Vanessa why auto-scan is disabled.

How would you rank the options in the question above in order of preference?

C.12 Quality Check

I am randomly answering the questions.
A. Yes B. No

C.13 Continuity of Care - Scenario 1

Assume you have a friend, Catherine, who you believe to be less competent than you in data security. She comes to you for help because she had corrupted files on her computer and thinks she has a virus. What would you do?
(Responses: I strongly agree, I agree, Neutral, I disagree, I strongly disagree)
A. Do nothing.
B. Fix it, if you feel you can.
C. Tell Catherine what to do to fix the problem herself, if you know the solution.
D. Tell Catherine to look for help elsewhere if you feel/find that you cannot fix it.
E. Arrange for a trusted contact to fix it, if you feel/find that you cannot.
F. Arrange for a third party to fix it. You offer to pay.
G. Arrange for a third party to fix it. You offer to help pay (share the cost).
H. Arrange for a third party to fix it. You expect Catherine to pay.

C.14 Continuity of Care - Scenario 2

Assume you have a friend, Catherine, who you believe to be less competent than you in data security. She comes to you for help because she had corrupted files on her computer and thinks she has a virus. You recall that three months ago, Catherine was trying to install a piece of software, but was failing. She asked for your help. You were busy and told her the antivirus was the problem, and to try turning it off. You now notice the antivirus is off. What would you do?
(Responses: I strongly agree, I agree, Neutral, I disagree, I strongly disagree)
A. Do nothing.
B. Fix it, if you feel you can.
C. Tell Catherine what to do to fix the problem herself, if you know the solution.
D. Tell Catherine to look for help elsewhere if you feel/find that you cannot fix it.
E. Arrange for a trusted contact to fix it, if you feel/find that you cannot.
F. Arrange for a third party to fix it. You offer to pay.
G. Arrange for a third party to fix it. You offer to help pay (share the cost).
H. Arrange for a third party to fix it. You expect Catherine to pay.

D. SUMMARY STATISTICS

Survival/Outcome Bias:

	Strongly Agree	*Agree*	*Neutral*	*Disagree*	*Strongly Disagree*
A.	34 (3.1%)	203 (18.7%)	237 (21.8%)	430 (39.6%)	183 (16.8%)
B.	109 (10%)	386 (35.5%)	269 (24.7%)	247 (22.7%)	76 (7%)

Confidence in a Security Measure:

	Strongly Agree	*Agree*	*Neutral*	*Disagree*	*Strongly Disagree*
A.	31 (2.9%)	120 (11%)	167 (15.4%)	420 (38.6%)	349 (32.1%)
B.	41 (3.8%)	242 (22.3%)	272 (25%)	385 (35.4%)	147 (13.5%)
C.	156 (14.4%)	345 (31.7%)	264 (24.3%)	218 (20.1%)	104 (9.6%)

Assessing the Quality and Source of Support:

Which of the following do you take into consideration when seeking data security advice or help from someone? (Please select all that apply)

A. Competence	993 (91.4%)	E. Cost to you (money, favours, gifts, etc)	530 (48.8%)
B. Availability	334 (30.7%)	F. Cost to the source of advice/help (effort, inconvenience, etc)	394 (36.2%)
C. Trust	971 (89.3%)	G. None of the above	11 (1%)
D. Closeness to you	339 (31.2%)		

How would you rank the options in the question above in order of preference?

	0 (No rank)	*1*	*2*	*3*	*4*	*5*	*6*
A.	6 (.6%)	660 (60.7%)	273 (25.1%)	79 (7.3%)	39 (3.6%)	17 (1.6%)	13 (1.2%)
B.	22 (2%)	21 (1.9%)	77 (7.1%)	293 (27%)	283 (26%)	232 (21.3%)	159 (14.6%)
C.	4 (.4%)	321 (29.5%)	541 (49.8%)	118 (10.9%)	62 (5.7%)	32 (2.9%)	9 (.8%)
D.	28 (2.6%)	20 (1.8%)	71 (6.5%)	212 (19.5%)	195 (17.9%)	224 (20.6%)	337 (31%)
E.	21 (1.9%)	50 (4.6%)	82 (7.5%)	234 (21.5%)	252 (23.2%)	248 (22.8%)	200 (18.4%)
F.	24 (2.2%)	14 (1.3%)	38 (3.5%)	140 (12.9%)	232 (21.3%)	304 (28%)	335 (30.8%)

Assessing Other People's Security Competence:

How do you assess if someone is more competent than you in data security? (Please select all that apply.)

A. He/she works for a technical company	255 (23.5%)	F. He/she works in data security	938 (86.3%)
B. His/her job is technical	255 (23.5%)	G. He/she studied or studies data security	846 (77.8%)
C. He/she has more experience than you in using or working with technical devices and services	559 (51.4%)	H. He/she has experienced a data security incident before	428 (39.4%)
D. He/she studied or studies a technical course	289 (26.6%)	I. None of the above	47 (4.3%)
E. He/she is more educated than you	75 (6.9%)		

How would you rank the options in the question above in order of preference?

	0 (No rank)	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*
A.	36 (3.3%)	38 (3.5%)	47 (4.3%)	106 (9.8%)	176 (16.2%)	180 (16.6%)	233 (21.4%)	188 (17.3%)	83 (7.6%)
B.	32 (2.9%))	38 (3.5%)	41 (3.8%)	116 (10.7%)	201 (18.5%)	269 (24.7%)	229 (21.1%)	131 (12.1%)	30 (2.8%)
C.	21 (1.9%)	96 (8.8%)	73 (6.7%)	231 (21.3%)	252 (23.2%)	164 (15.1%)	140 (12.9%)	96 (8.8%)	14 (1.3%)
D.	32 (2.9%)	16 (1.5%)	38 (3.5%)	103 (9.5%)	173 (15.9%)	254 (23.4%)	249 (22.9%)	190 (17.5%)	32 (2.9%)
E.	39 (3.6%)	11 (1%)	15 (1.4%)	24 (2.2%)	41 (3.8%)	36 (3.3%)	65 (6%)	188 (17.3%)	668 (61.5%)
F.	8 (.7%)	730 (67.2%)	163 (15%)	71 (6.5%)	38 (3.5%)	33 (3%)	20 (1.8%)	18 (1.7%)	6 (.6%)
G.	18 (1.7%)	115 (10.6%)	634 (58.3%)	138 (12.7%)	55 (5.1%)	45 (4.1%)	32 (2.9%)	25 (2.3%)	25 (2.3%)
H.	22 (2%)	42 (3.9%)	68 (6.3%)	284 (26.1%)	124 (11.4%)	74 (6.8%)	84 (7.7%)	208 (19.1%)	181 (16.7%)

Duty of Care: Motivation - Offer Unsolicited Support:

	Very Likely	*Likely*	*Neutral*	*Unlikely*	*Very Unlikely*
A. Relative	209 (19.2%)	396 (36.4%)	180 (16.6%)	209 (19.2%)	93 (8.6%)
B. Friend	137 (12.6%)	376 (34.6%)	223 (20.5%)	250 (23%)	101 (9.3%)
C. Work colleague	55 (5.1%)	236 (21.7%)	268 (24.7%)	351 (32.3%)	177 (16.3%)
D. Others	24 (2.2%)	107 (9.8%)	275 (25.3%)	350 (32.2%)	331 (30.5%)

How would you rank the options in the question above in order of preference?

	0 (No rank)	*1*	*2*	*3*	*4*
A.	4 (.4%)	756 (69.5%)	196 (18%)	97 (8.9%)	34 (3.1%)
B.	5 (.5%)	216 (19.9%)	746 (68.6%)	113 (10.4%)	7 (.6%)
C.	5 (.5%)	96 (8.8%)	123 (11.3%)	812 (74.7%)	51 (4.7%)
D.	12 (1.1%)	18 (1.7%)	17 (1.6%)	58 (5.3%)	982 (90.3%)

Duty of Care: Motivation - Accept Unsolicited Support:

	Very Likely	*Likely*	*Neutral*	*Unlikely*	*Very Unlikely*
A. Relative	195 (17.9%)	485 (44.6%)	232 (21.3%)	134 (12.3%)	41 (3.8%)
B. Friend	174 (16%)	514 (47.3%)	253 (23.3%)	117 (10.8%)	29 (2.7%)
C. Work colleague	103 (9.5%)	424 (39%)	331 (30.5%)	172 (15.8%)	57 (5.2%)
D. Service provider/ Manufacturer help desk	135 (12.4%)	347 (31.9%)	266 (24.5%)	222 (20.4%)	117 (10.8%)
E. IT repair shop professional	118 (10.9%)	322 (29.6%)	253 (23.3%)	242 (22.3%)	152 (14%)
F. Others	26 (2.4%)	109 (10%)	424 (39%)	283 (26%)	245 (22.5%)

How would you rank the options in the question above in order of preference?

	0 (No rank)	*1*	*2*	*3*	*4*	*5*	*6*
A.	7 (.6%)	405 (37.3%)	192 (17.7%)	211 (19.4%)	119 (10.9%)	119 (10.9%)	34 (3.1%)
B.	8 (.7%)	220 (20.2%)	403 (37.1%)	167 (15.4%)	203 (18.7%)	76 (7%)	10 (.9%)
C.	9 (.8%)	95 (8.7%)	134 (12.3%)	456 (42%)	127 (11.7%)	235 (21.6%)	31 (2.9%)
D.	10 (.9%)	232 (21.3%)	149 (13.7%)	129 (11.9%)	332 (30.5%)	186 (17.1%)	49 (4.5%)
E.	8 (.7%)	123 (11.3%)	191 (17.6%)	93 (8.6%)	227 (20.9%)	378 (34.8%)	67 (6.2%)
F.	12 (1.1%)	11 (1%)	13 (1.2%)	22 (2%)	67 (6.2%)	81 (7.5%)	881 (81%)

Duty of Care: Motivation:

	Strongly Agree	*Agree*	*Neutral*	*Disagree*	*Strongly Disagree*
A.	61 (5.6%)	233 (21.4%)	239 (22%)	397 (36.5%)	157 (14.4%)
B.	350 (32.2%)	393 (36.2%)	171 (15.7%)	134 (12.3%)	39 (3.6%)
C.	56 (5.2%)	189 (17.4%)	319 (29.3%)	402 (37%)	121 (11.1%)
D.	48 (4.4%)	160 (14.7%)	269 (24.7%)	414 (38.1%)	196 (18%)
E.	539 (49.6%)	436 (40.1%)	63 (5.8%)	36 (3.3%)	13 (1.2%)

How would you rank the options in the question above in order of preference?

	0 (No rank)	*1*	*2*	*3*	*4*	*5*
A.	9 (.8%)	56 (5.2%)	131 (12.1%)	413 (38%)	118 (10.9%)	360 (33.1%)
B.	5 (.5%)	255 (23.5%)	509 (46.8%)	96 (8.8%)	191 (17.6%)	31 (2.9%)
C.	9 (.8%)	54 (5%)	160 (14.7%)	268 (24.7%)	503 (46.3%)	93 (8.6%)
D.	10 (.9%)	26 (2.4%)	108 (9.9%)	163 (15%)	237 (21.8%)	543 (50%)
E.	2 (.2%)	695 (63.9%)	174 (16%)	140 (12.9%)	28 (2.6%)	48 (4.4%)

Duty of Care: Social Responsibility - Seek Support:

	Very Likely	*Likely*	*Neutral*	*Unlikely*	*Very Unlikely*
A. Relative	383 (35.2%)	485 (44.6%)	128 (11.8%)	71 (6.5%)	20 (1.8%)
B. Friend	362 (33.3%)	561 (51.6%)	124 (11.4%)	29 (2.7%)	11 (1%)
C. Work colleague	207 (19%)	562 (51.7%)	214 (19.7%)	79 (7.3%)	25 (2.3%)
D. Service provider/ Manufacturer help desk	224 (20.6%)	402 (37%)	279 (25.7%)	150 (13.8%)	32 (2.9%)
E. IT repair shop professional	186 (17.1%)	367 (33.8%)	262 (24.1%)	206 (19%)	66 (6.1%)
F. Others	46 (4.2%)	123 (11.3%)	561 (51.6%)	239 (22%)	118 (10.9%)

How would you rank the options in the question above in order of preference?

	0 (No rank)	*1*	*2*	*3*	*4*	*5*	*6*
A.	10 (.9%)	361 (33.2%)	205 (18.9%)	229 (21.1%)	119 (10.9%)	132 (12.1%)	31 (2.9%)
B.	8 (.7%)	243 (22.4%)	393 (36.2%)	173 (15.9%)	198 (18.2%)	62 (5.7%)	10 (.9%)
C.	10 (.9%)	98 (9%)	138 (12.7%)	410 (37.7%)	166 (15.3%)	236 (21.7%)	29 (2.7%)
D.	11 (1%)	232 (21.3%)	159 (14.6%)	151 (13.9%)	305 (28.1%)	196 (18%)	33 (3%)
E.	9 (.8%)	145 (13.3%)	176 (16.2%)	97 (8.9%)	235 (21.6%)	357 (32.8%)	68 (6.3%)
F.	14 (1.3%)	6 (.6%)	9 (.8%)	17 (1.6%)	52 (4.8%)	90 (8.3%)	899 (82.7%)

Duty of Care: Social Responsibility - Seek Support:

	Very Likely	*Likely*	*Neutral*	*Unlikely*	*Very Unlikely*
A. Relative	479 (44.1%)	388 (35.7%)	80 (7.4%)	95 (8.7%)	45 (4.1%)
B. Friend	454 (41.8%)	398 (36.6%)	86 (7.9%)	102 (9.4%)	47 (4.3%)
C. Work colleague	286 (26.3%)	439 (40.4%)	161 (14.8%)	136 (12.5%)	65 (6%)
D. Others	147 (13.5%)	302 (27.8%)	307 (28.2%)	215 (19.8%)	116 (10.7%)

Continuity of Care - Scenario 1:

	Strongly Agree	*Agree*	*Neutral*	*Disagree*	*Strongly Disagree*
A.	12 (1.1%)	24 (2.2%)	116 (10.7%)	452 (41.6%)	483 (44.4%)
B.	389 (35.8%)	561 (51.6%)	80 (7.4%)	42 (3.9%)	15 (1.4%)
C.	146 (13.4%)	613 (56.4%)	188 (17.3%)	114 (10.5%)	26 (2.4%)
D.	327 (30.1%)	556 (51.1%)	100 (9.2%)	77 (7.1%)	27 (2.5%)
E.	263 (24.2%)	535 (49.2%)	192 (17.7%)	81 (7.5%)	16 (1.5%)
F.	11 (1%)	66 (6.1%)	131 (12.1%)	464 (42.7%)	415 (38.2%)
G.	20 (1.8%)	72 (6.6%)	148 (13.6%)	442 (40.7%)	405 (37.3%)
H.	153 (14.1%)	459 (42.2%)	281 (25.9%)	130 (12%)	64 (5.9%)

Continuity of Care - Scenario 2:

	Strongly Agree	*Agree*	*Neutral*	*Disagree*	*Strongly Disagree*
A.	14 (1.3%)	29 (2.7%)	98 (9%)	491 (45.2%)	455 (41.9%)
B.	424 (39%)	549 (50.5%)	62 (5.7%)	37 (3.4%)	15 (1.4%)
C.	200 (18.4%)	604 (55.6%)	160 (14.7%)	98 (9%)	25 (2.3%)
D.	240 (22.1%)	615 (56.6%)	131 (12.1%)	69 (6.3%)	32 (2.9%)
E.	252 (32.3%)	584 (53.7%)	161 (14.8%)	61 (5.6%)	29 (2.7%)
F.	63 (5.8%)	168 (15.5%)	219 (20.1%)	367 (33.8%)	270 (24.8%)
G.	65 (6%)	235 (21.6%)	211 (19.4%)	331 (30.5%)	245 (22.5%)
H.	90 (8.3%)	347 (31.9%)	315 (29%)	241 (22.2%)	94 (8.6%)