OLDER ADULTS' PERCEPTIONS OF ONLINE RISK

by
Vanessa Boothroyd

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

MASTER OF ARTS

Human Computer Interaction

at

CARLETON UNIVERSITY

Ottawa, Ontario
May, 2014

Abstract

Older adults are a growing group of Internet users, but they are also among the most vulnerable for attack. We examine how older adults perceive risks involved in email and Facebook and compare their perceptions to those of younger adults. We interviewed sixteen younger adults and fifteen older adults and found that older adults had roughly the same perceptions of email risks, however notably different perceptions of Facebook risks than the younger users. Further, older adults' understanding of available security and privacy tools in both email and Facebook was more limited than that of younger adults. We also determined that family and the media are the most prevalent sources of information regarding computer security for participants in both age groups. This study provides recommendations on communication of Internet security and outlines elements of email and Facebook that need further clarification for older users, such as Facebook's privacy settings.

Acknowledgements

This project took a lot of hard work and dedication and I would like to recognize and share my gratitude towards those who made it possible.

I would like to thank NSERC ISSNet for funding this research.

I would like to thank my supervisor, Sonia, without whom this project never could have happened. Her unending patience, generosity, open-mindedness, teaching, resources, cat stories, thoughtfulness, nurturance, and painstaking editing of awkward, and run on sentences, and excessive commas, made this thesis, what it is, today.

My wife deserves more thanks than I will ever be able to give. She acted as a mentor, an editor, and as a sounding board for all of my crazy ideas. She patiently listened to and empathized with my struggles, and supported and enabled me as I surpassed them during the whole process. Thank you. It is finally the end of the "ssh"!"..sorry!!" in the evenings now, for which I'm sure we are both grateful.

I benefited greatly from academic support from my co-supervisor Andrew, who regularly took time out of his busy schedule to go over project design and planning, results analysis and draft editing with me. His meaningful insights regarding thesis organization, writing, and defense also influenced this project greatly.

Thanks also go to my participants whose willingness to share their understanding, strategies, and experiences made this thesis not only possible, but fascinating and fruitful. Extra thanks go to my pilot participants whose thoughtful insights and suggestions set the stage for this successful project.

I am also thankful to Judith who provided me with great feedback, brainstorming and insights throughout my project design and mixed methods research.

Finally thanks go to family and friends for their consistent support of me in all of my endeavours. Thanks especially to my parents and extended family who have given up their time with me during Christmas and summer visits so I could continue work on this project. Extra thanks go to my parents who provided me with valuable insights and resources, and especially to my dad who proof-read some chapters at the last minute and to whom I owe one of the best sentences in this thesis.

To the guilt I felt for taking so long - good riddance.

Table of Contents

List of Tables

Chapter 1

Introduction

1.1 Motivation

Older adults are the fastest growing population segment on the Internet [71]. Online services such as email and Facebook are seeing this influx of older adults reflected in their user base [71]. Access to online services enables this population to keep in touch with family and friends and continue to be active members of their respective communities [25]. However, as online threats continue to advance and multiply [21], the potential for falling victim to attacks increases. Older adults, in particular, must be cautious as they are the most vulnerable and most targeted demographic for a number of online attacks [11]. Older adults may be vulnerable due to inexperience with newer technologies and for health-related reasons such as Alzheimer's [11].

In order for older users to safely interact online, Internet risk and safety information needs to be designed and disseminated with their communication needs in mind. We conducted a mixed methods study combining qualitative and quantitative analyses exploring older adults' perceptions of online risk to determine what, if any, gaps in understanding are leaving them at risk. We also wanted to determine where older users had learned about computing security. As Rader et al. explains, "Ideally, the (security) information {...} would come from security experts in formal training sessions, however it is likely that this is not the case" [57]. Therefore, our study also aimed to identify the source of older adults' Internet security information, as that may help us interpret their understanding and behaviour with respect to online security.

The results of our study allow us to make recommendations regarding areas of Internet security which should be further expounded for these users, and to suggest education and communication strategies to increase older adults' understanding of risk, and therefore, their online safety.

1.2 Research questions

We investigated three aspects of older adults' (aged 65+) Internet risk perception: their awareness of Internet hazards, the strategies they use to stay safe from these hazards, as well as their sources of security-related information. We explored these topics with younger adult Internet users as well, to act as a frame of reference for the older adults' results. Younger adults between the ages of 18 and 29 use the Internet more than any other age group [71], and are among the most frequent users of social media and email [71]. This high level of engagement makes younger adults an interesting and relevant group of users to compare against.

The interviews originally asked users about risks and safety strategies in the context of a number of online services; however, analysis and reporting of all of the interview data was beyond the scope of an MA thesis. We therefore interpreted only a subset of the data: perceptions of risk and strategies in the context of two online activities (email and social networking), as well as users' sources of Internet-security information. Accordingly, our research questions are the following:

R1: What are older adults' perceptions of risk in email and Facebook and how do these differ from younger adults'?

R2: What safety strategies do older adults use to stay "safe" from risks in these online activities and how are these different from younger adults'?

R3: What are older adults' sources of security-related information and how do they differ from younger adults'?

For the present study, we define the term "perception" as "the use of previous knowledge to gather and interpret the stimuli registered by the sense" [52].

To find out what older and younger users knew about online risk without providing a list of risks (which might bias their responses), we conducted semi-structured interviews. These enabled us to ask a variety of questions and base follow-up questions on participant responses. We analyzed participants' responses using thematic analysis – a flexible qualitative data analysis method that allows for exploratory research without the constant goal of theory building [9]. We quantified results of

the thematic analysis to focus on differences between groups and contextualize users' responses.

1.3 Contributions

This thesis offers the following main contributions:

1. This was the first study designed to compare older and younger adults' perceptions of online risks, safety strategies, and instruction. The research contributes to the sparse usable security literature on older adults.

2. Recommendations are offered regarding those online elements that need further clarification for older users, such as the use of privacy settings. Recommendations are also made for improving communication around Internet security. We suggest leveraging media and using stories as a format of teaching. Finally, we suggest that online services consider older adults in the design of their systems and security features.

1.4 Thesis outline

This thesis is organized into seven chapters. In Chapter 2, we explore concepts and previous work in the areas of usable security, computer threats, perception and mental models of risk, and differences between older and younger adults as they relate to this topic. In Chapter 3, we describe the method used to obtain and analyze the data, including information on our recruitment process and participants. In Chapter 4, we describe the most frequently reported themes regarding participants' perceptions of risk involved in using email and social networking. Chapter 5 discusses the strategies participants reported for staying safe when using email and social networking. In Chapter 6, we describe where participants learned about computer security. Finally, in Chapter 7, we discuss the implications of these findings, the strengths and limitations of the study, and offer suggestions for future research. We also make recommendations for communicating about Internet security, identify areas of security that remain poorly understood by older adults, and make suggestions regarding how to fill gaps in understanding.

Chapter 2

Background

In this chapter we describe concepts and previous research related to the topics explored in this thesis.

2.1 Usable security

Usable security is an area of research that combines human-computer interaction, psychology, and computer security. Its objective is to explore and promote user-centered design of computer security systems. This is particularly important because attackers are still successfully exploiting users despite various security technologies already in place. The continued exploitation is due in part to unrealistic expectations of security systems, overly complex security advice, and users' insufficient understanding of Internet threats. Previous research [1] has shown that lay Internet users have insufficient knowledge about security threats. Users create mental models[1] of the importance of security and of possible security threats on their own [1] [10] [16] [36] and behave according to these inaccurate models (i.e., folk models[2]) [69], leaving them vulnerable to a number of threats.

Security technologies and security advice can also hinder secure behaviour. Security systems often get in the way of users' primary tasks, and require more time and cognitive load to operate than users are willing to spend [31]. Additionally, the security advice and mechanisms that users are instructed to employ are often "crushingly complex" [36], and none can promise absolute security. The benefits of employing this advice or these technologies often do not justify the time and effort they require [36] and the tasks are often perceived as laborious and unnecessary [1]. The question remains as to how to help users avoid harm. As Herley explains,"{...}

[1] A mental model is a cognitive representation of a system. [52]

[2] A folk model is a mental model that is not necessarily accurate in the real world but is shared among similar members of a culture.

this begins with a clear understanding of the actual harms they face, and a realistic understanding of their constraints" [36]. This thesis addresses this final point by exploring where the most vulnerable users have learned what they know, determining what they know, and determining how they attempt to keep themselves safe from hazards inherent to specific online activities.

2.2 Threats

Roughly 90% of online adults in the U.S. use email [71] and 65% use social networking services such as Facebook [71]. Further, on average 727 million active Facebook users are online everyday [22]. Each of these email and Facebook users runs the risk of falling victim to any number of hazards[3], including social engineering attacks, spam, malware, unauthorized access, and other types of privacy breaches.

2.2.1 Social engineering

Social engineering attacks include a variety of different hoaxes that involve exploiting users' trust, lack of expertise, desperation, or socialization to trick them into providing authentication information or money to the benefit of someone else [67] [5]. Attackers may use the authentication data themselves to exploit a system or account [67], or provide this information to other attackers to do the same, potentially for money. Scams and phishing are two classes of social engineering attacks.

Scams: Online scams are confidence games that trick people into believing they will receive money or property by giving up real money, but the victims do not receive anything of value in return [43] [5]. Previous research regarding email scams has found that users exhibit certain behavioural patterns that can be exploited by these types of attacks, and that awareness of these behavioural patterns can help both users and security engineers build systems that undermine scams [63].

For example, Stajano et al. [63] found that scams distract users with appealing or seemingly important information so they do not notice they are falling victim to the fraud. These researchers also found that society trains people not to question

[3] A hazard meaning exposure or vulnerability to injury, loss, or danger.

authority, therefore when scammers impersonating bank employees or other authority figures demand money or information, users are more likely to provide it.

Phishing: Phishing is another social engineering attack that involves sending email to trick recipients into visiting the attacker's website and entering their sensitive information [5] [43]. Phishers often spoof the sender's name and email address [48] and direct victims to webpages masquerading as legitimate websites, such as banks, credit card companies, and auction sites. Once the sensitive information, such as a username and password, are input, attackers use it for nefarious purposes such as identity theft or to compromise the user's online accounts. One of the most significant increases in reported phishing statistics occurred in Canada, where attacks increased nearly 400% in the first half of 2011 [21]. Global monetary losses due to phishing attacks are valued at approximately 1.5 billion dollars for 2012 [21] .

There has been considerable research on helping users avoid falling victim to phishing [15] [18] [17]. These studies suggest that victims are unfamiliar with phishing attacks and with relevant security indicators. Existing protection mechanisms can help prevent users from falling victim to phishing attacks, but each also has particular vulnerabilities that leave users unprotected [17] [70]. For example, one study found that SpoofGuard, an anti-phishing browser toolbar, only determined whether a web site was fraudulent when it had finished loading [70]. Attackers are able to delay the complete loading of the page, which results in SpoofGuard providing no warning to users regarding the website's authenticity.

2.2.2 Spam

Kim et al. [43] define spam as unwanted notices in the form of email. Over 70% of email traffic falls into the category of unsolicited bulk email [5]. Some spam are attempts to scam people or spread malware [43], however we describe these email threats separately.

Dourish et al. [16] found that participants' often brought up unsolicited email when asked about their experiences with computer security. Participants considered spam and security as aspects of the same problem even though they "may be technically

quite different" [16]. Their participants also believed that security technologies would protect them against both spam and other types of online threats. For example, they had the impression that firewalls would protect them from unwanted visitors as well as unwanted emails when this was not the case. In another study, Grimes et al. [33] examined users' experiences with spam emails and found that older and younger adults receive the same amount of spam despite older users' lesser computer use, and that the youngest and oldest users reported taking the fewest actions (such as filtering) against spam. Grimes et al. also found that older participants were more likely to make a purchase as a result of a spam email.

2.2.3 Unauthorized access

Attackers can gain unauthorized access to people's computers and Internet-based accounts by using password guessing attacks[4] , social engineering (i.e. tricking people to give up their authentication information), or through malware programs that capture authentication information. Attackers are able to then compromise the account and steal the user's identity, impersonate the user, break into other accounts, or otherwise damage the user's data. Previous research [58] found that 21% of the adults surveyed were aware of having had a social media or email account hijacked, and 11% had personal information such as bank account data, social security numbers, or credit cards taken.

2.2.4 Malware

Aycock [5] considers malware (malicious software) to be the most significant threat to computer security. He defines it as malicious software whose intent or effect is harmful. The term malware covers a broad variety of more specific threats classified according to how they work, including viruses, worms, spyware, and Trojan horses. Malware can be spread through malicious emails, Internet connections, and infected hardware. A Trojan horse, for example, "claims to do some benign task, but secretly performs some additional malicious task" [5], which may hinder a computer's performance or

[4]Password guessing attacks involve attempting to log in to an account using a number of different passwords until one works.

collect and send copies of the victim's personal data to thieves.

Anti-malware technology such as Norton Antivirus or Kaspersky Internet Security can help detect and remove malware from users' systems. However, cyber attacks are constantly evolving to work around current technology-based solutions [12]. Attackers are also able to exploit social networks to disseminate malware. Some forms of malicious software can be disseminated through links in a Facebook message [29], and embedded within third-party applications.

2.2.5 Exploitation of information

The 2013 PEW report, "Anonymity, Privacy, and Security Online" [58], found that 66% of Internet users surveyed reported that an image of them was available online, 48% reported using their full name, and 50% reported that their birth date was also available [58]. If accessed by a malicious user, a full name and birthdate can be key pieces of information needed to steal an identity [55]. In their 2011 review of security threats in online social networks, Gao et al. [27] describe three other ways user's information can be exploited in the context of social networks: breaches from the service provider, breaches from other users, and breaches from third party applications.

Provider breach: The risk of a breach from service providers is due to the client-server architecture of social networks which dictates that users must trust the service provider to protect the personal information they have uploaded. However, the benefits service providers can reap by sharing this information results in a conflict of interest on their behalf [27]. For example, selling this information to advertisers would be very profitable but may violate a company's terms of agreement or users' trust.

User breach: Privacy breaches can also occur because of other users' actions. The power of social networks lies in the ability for people to connect and share with each other; however, this also results in vulnerability. If one person is breached, the users they are connected to are also vulnerable to having their shared information

taken and used. This is especially concerning when users share their information with untrusted or unknown users [7] [27].

Third party application breach: Finally, privacy breaches can also occur through the use of third-party applications [27] [19]. When a third-party application obtains access to a user's profile data, it is no longer possible for the service to enforce or assess how this data is used [19]. Facebook requires that application developers agree to their terms for handling user data, however, there have been a number of reported violations of these terms [65]. For example, Facebook IDs have been linked to profiles by third party applications and sent to advertising companies [65].

2.3 Risk perception

A main tenent of risk analysis research is that "while danger (or threat) is real, risk is socially constructed" [62]. As Slovic et al. explain [62], risks do not exist "out there, independent of our minds and cultures, waiting to be measured" [62]. Rather, the concept of risk has been invented by humans to help them understand and confront the various dangers and ambiguity inherent in everyday life [62]. Humans are forced to make judgments about risks without complete knowledge of the possible dangers or the probability of events occurring, and therefore we are forced to rely on a number of heuristics to make decisions regarding risk. These heuristics involve people's psychology, their gender, culture, perceived severity of the consequences of a risk, and immediacy of the consequences [62]. Kahneman, Slovic, and Tversky explain "(lay people) rely on a set of heuristics which sometimes lead to reasonable judgments and sometimes lead to severe and systematic errors" [40]. For example, motorists refused to wear seat belts until they were mandated by law because they considered the likelihood of being involved in a serious accident on their next trip to be so low it was not worth wearing the belts, while this was not the consensus of researchers [62].

Research on risk assessment was influenced dramatically in 1969 by Starr's study [64] that involved using historical data to expose patterns of acceptable risk-benefit

trade-offs. Their findings shed light on how lay people perceive risk. For example their findings indicated that "the social acceptance of risk is directly influenced by public awareness of the benefits of an activity as determined by advertising, usefulness, and the number of people participating" [64].

Starr's risk-benefit trade-off approach, a "revealed" preferences approach, relied on two assumptions of humans and risk: 1) historical records are adequate for revealing patterns of fatalities in the public use of technology, and 2) historically revealed social preferences and costs are sufficiently enduring to permit their use for predictive purposes" [64].

Concerns about these assumptions influenced later work by Fischhoff et al. [24] which instead used questionnaires to gather people's ratings of qualities of risks, e.g., controllability or voluntariness, directly. This new work was called the "expressed" preferences approach' and this approach has influenced more recent research into the evaluation of how users perceive online risks.

However the expressed preferences approach has been commonly used to evaluate perceptions of physical risks with tangible, life threatening consequences. Garg and Camp [28] explain that "online security risks are harder to evaluate and more intractable than physical risks due to a general lack of metrics, awareness of security incidents, and inherent haptic feedback" [28]. This lack of awareness of security incidents and lower likelihood of physical danger makes it more difficult for people to conceive of these types of risk, and therefore makes security more complex to study.

A number of methods have been proposed to study the understanding of risks, including eliciting and measuring users' expressed preferences [45], research into mental models [10] [69] [16] [41] and research into the stories people hear about risks [57]. These methods will be summarized in the next section.

2.3.1 Expressed preferences approach

Leblanc and Biddle [45] applied Fischhoff et al.'s expressed preferences approach [24] to the study of people's perceptions of Internet-related risk. They had 94 Internet users rate 15 different online activities according to heuristics related to risk perception, such as the degree the activity benefitted the general population and the

severity of the hazard's consequences. The results indicated that the severity of a risk's consequences was most indicative of how participants would rate the risk across the remaining heuristics. Participants also had a number of inaccurate understandings of threats and the processes involved in privacy breaches. One misconception was that the full consequences of a privacy breach would be experienced immediately after the information was taken. Another was that financial risks have the most severe consequences, and finally, that embarrassment risks are considered the most likely. Participants also demonstrated a lack of knowledge regarding how loss of information may actually occur. For example, participants did not realize that loss of certain types of information could lead to the installation of malware, which then may lead to monetary loss at a later time. Overall, Leblanc and Biddle [45] found that many users were unaware of hazards involved in Internet-related activities or did not think they would be impacted by them.

Another analysis of online activities and risks using the expressed preferences approach was completed by Garg and Camp in 2012 [28]. They asked 93 students to rank online activities on nine different scales including whether the activities were voluntary, whether the activities were relatively new, or whether they had been around longer. Analysis revealed a four dimensional model that explained the majority of user responses regarding online risks. Newness of the activity, unfamiliarity with the activity, controllability of the consequences, and dread of the consequences of a threat were the most significant determinant of perceived risk. Participants considered identity theft as the threat with the most severe consequences, while phishing, which contributes to identity theft, was ranked much lower. Overall, the research found that users did not demonstrate accurate perceptions of online risk.

2.3.2 Mental models approach

Mental models are broadly defined as cognitive representations of systems [52]. Users' actions and security related decisions are informed by their mental models of online risks [68]. Several researchers [68] [28] [69] [16] reason that because computer users' actions and decisions are influenced by their mental models, it is crucial for designers, developers, and educators to understand these models when developing and designing

security communications and technologies.

To gather users' understandings of how systems work, it is important to avoid influencing how they conceive of phenomena. Expressed preferences researchers [45] [28] often recognize the role providing lists of potential risks to participants may play in affecting users' judgement or understanding. Mental model research is a good alternative approach to risk perception because users are rarely provided with a list of threats to judge, but are instead asked about threats more generally.

Encouraging specific mental models: Camp [10] proposes and critiques five potential mental models of security. She suggests that these models are alternatives for communicating to users about computer security in a way they may better understand, leveraging situations and understandings users already have.

1. *Physical security model* is useful when one thinks of safes, doors, and locks.

2. *Medical model* which involves the analogy of the spread of infectious disease or malware regardless of who the person is, and focuses on the necessity of individuals to protect themselves to fight the spread of disease.

3. *Criminal model* which is based on intrusion

4. *Warfare model* plays on the idea that "perimeter security and constant diligence" are needed to stay safe.

5. *Market model* provides information regarding costs and benefits of staying safe.

Camp explains that each metaphor provides a mental model for different facets of computer security but that these models are not perfect, as each has limitations. She posits that using these types of mental models, or analogies, in security communications may increase understanding. Providing users with a model or analogy of online risk is one way to increase user understanding of online threats and encourage more informed security-related decision making.

Eliciting users' mental models: Other researchers have studied users' current mental models to determine what they know and how this influences their decision making. Gurung et al. [35] surveyed 232 students to determine the factors that motivate users to use anti-spyware tools. They found that users' perceptions of efficacy of the anti-spyware, their perception of their own technical skills, and the perceived severity of the threats all influence whether anti-spyware technology was adopted and used. Gurung et al. suggest that once users understand the severity of successful spyware attacks, they are more likely to adopt anti-spyware technology. The research found that cost influences adoption, particularly when users' perception of the costs of spyware are underestimated. Similar results were also found by others [47] [46].

Dourish et al. [16] elicit mental models through semi-structured interviews to determine how users experience security on a day-to-day basis. They interviewed 20 people in work and learning environments and found that security and privacy issues are poorly understood. Users mistakenly believed that a security system provides protection against a number of threats when the technology actually only protects against one specific threat. Users also frequently discussed problems of personal security, such as stalkers, and took action to protect themselves from this type of direct personal threat. Post hoc analyses revealed that younger participants demonstrated greater confidence regarding their computing abilities and capacity to stay safe. Overall, however, there was a feeling of futility, in that participants felt unable to protect themselves from all threats. Finally, Dourish et al. determined that participants outsourced their computer security to friends, support groups within an organization, or institutions.

Another example of eliciting mental models is Wash's 2011 study in which he evaluated "folk models": models people have of a system, that while not necessarily accurate, still motivate decision making toward accomplishing the main goal of computer security [69]. He interviewed 33 users regarding computer security and their corresponding mental models. He identified four folk models of viruses and four folk models of hackers. Users base their decisions of which security software to use and which security advice to follow on these models, and as a result may ignore particular software or advice. For example, participants often do not protect themselves

because they do not consider themselves sufficiently wealthy or famous to be a target – or "big fish" [69]. Wash also notes that security experts should not evaluate users' folk models on correctness, rather the models should be evaluated on whether they meet the needs of the users that possess them. He suggests that technologies or communications should expose threats in a way that the user understands and in a way that motivates people to use the technology appropriately. This study was replicated in Germany by Kauer et al. [41], who found similar folk models and identify an additional three models concerning the role the government plays in online risk.

Taken together, these studies of mental models show that users demonstrate and verbalize a variety of different understandings of Internet threats and security. Understanding their mental models helps researchers understand how users make security related decisions and demonstrates why users may not take particular precautions. These studies determined users' mental models of malware, attackers, and general feelings about security but they did not determine how these mental models were formed or how participants learned about security.

2.4 Lessons

The source of users' information impacts what they learned, how they retained it, and how they apply it as they face security-related decisions. Research efforts have focussed on methods of teaching online security but little previous work has been done determining where users are getting their information and in what format it is delivered.

2.4.1 Teaching online security

Advice regarding online security is available from a number of sources. Descriptions of rules people should follow to stay safe are available on many popular websites [59] [30]. The type of rules they recommend users follow include creating long alphanumeric passwords, installing and updating anti-malware software, and releasing limited personal information online [30]. However, other researchers have explained that this type of advice takes too much time and effort for the poorly understood security benefits it offers [36], which dissuades people from applying it regularly. Other

researchers have created game-based approaches to teach people how to stay safe online [60] [13], which Sheng et al. [60] found to be effective in teaching people not to fall for phishing attacks, however future research needs to be done to explore scalability of security education of this kind.

2.4.2 Learning through stories

Baumeister [6] describes the role storytelling plays in learning how to "function effectively in a modern culture". He explains that learning by experience is important but it can be painful and inefficient. Even observational learning is limited by the number of people that must be observed in various situations. He suggests that sharing "the adventures and misadventures of others" is an extension of observational learning. This sharing enables "one to learn from the triumphs and misadventures of people beyond one's immediate perceptual sphere." He concludes that sharing stories regarding other people's experiences and behaviours "greatly expands the opportunities for cultural learning because one can benefit from the experiences of others" outside of someone's habitual group of friends [6]. The impact of story-telling as a source of computer security information has had little attention. To the best of our knowledge, Rader et al. [57] are the only researchers to have studied stories as sources of computer security information. We describe their work below.

Learning online security through stories: Rader et al. [57] explored how non-expert computer users learned about computer security from stories, and how that impacted their decisions. They conducted a survey about security stories and found that most of their participants had indeed learned about Internet security in the form of stories, primarily told by friends and family. Additional information gained from hearing stories influenced users' decision-making processes and stories were often retold, which means that the impact of these stories continues to grow. Rader et al.'s work suggests that future research should be done on communicating security information as stories to give people the necessary information for secure choices in a relatable context.

2.5 Older adults and online security

As adults age, retire from work, and experience new physical limitations, their lives change dramatically. A significant challenge involves staying part of communities [25]. Internet access, particularly access to social media, can play an important role in connecting older adults with others. As Internet popularity grows, and as the world population continues to age, older adults are increasingly accessing the Internet. In 2010, 29% of Canadians over 75 and 60% of those aged 65 to 74 had used the Internet in the previous month [3]. More recently, the 2012 Pew Internet and American Life project [71] reported that 53% of all American adults aged 65 and over were online, 70% of whom use the Internet on a typical day. As general Internet use grows, so does seniors' use of social networking sites. Between 2009 and 2011, older adults accessing social networking sites increased from 13% to 33% [71].

Older adults are more at risk for online attacks than any other age group [11]. The Canadian Anti-Fraud Center [11] explains that fraudsters target seniors because they consider them to be more vulnerable and more lucrative victims compared to other segments of the population. Older adults are considered more vulnerable due to their increased likelihood to feel lonely, their generation's tendency to be more trusting, a potential lack of familial support, and health-related reasons such as Alzheimer's [11]. They may also be more vulnerable due to inexperience and limited access to communications about scams, and thus are more gullible when it comes to attacks relating to technology [26]. Ruined family lives, great financial losses, and suicides have resulted from crimes targeting seniors [11].

2.6 Younger adults and online security

As of February 2012, 94% of American adults between the ages of 18 and 29 access the Internet and 86% use social networks; which is more than any other age group [71]. Most young adults have had access to computers since childhood and this extended experience, coupled with the support of family and friends, results in higher confidence in their computer-related abilities than older adults [61] [16]. Younger users have higher trust in various technologies than other users [61].

In their 2012 study, Manago et al. [51] considered the impact of large networks of social connections on the development of intimacy and social support among emerging adults[5]. Their survey of 89 undergraduate students showed that social networking helps young users satisfy their psychosocial need for enduring relations in the geographically mobile world of today. Manago et al. [51] explain that an important function of Facebook status updates is emotional disclosure, a key feature of intimacy and the building and maintenance of meaningful relationships.

Revealing personal details on Facebook can play an important role in emerging adults' development, however, this tendency for younger adults to emotionally disclose may be used against them during a privacy breach. For example, a 2013 study by Pew [58] found that users 18-29 are more likely to regret some of the things they have posted on social networks than users aged 50+. The Pew Anonymity, Privacy, and Security Online report [58] found that younger adults are more likely to use their real name and/or use a recognizable screen name than other age groups when using social media. Young adults reveal some real parts of themselves to receive support, recognition, and acceptance by others. However, younger adults are also more likely to post content anonymously than adults over thirty [58]. The authors explain that this is likely due to the fact that younger users share more content online than older users overall, some of it anonymously and some of it identified.

Younger adults were most likely to have experienced social media-related breaches (55% compared to 24% of adults over 56) [58]. This included compromised email or Facebook accounts, being stalked or harassed, suffering reputational damage, or finding themselves in physical danger due to online events. Younger adults are also the least likely demographic to report that home address or home phone number was online, and most likely to edit something they posted online in the past [58].

LeFebvre [47] surveyed 88 undergraduate students regarding their motivation to take precautions against social networking and malware related threats. The biggest predictor of taking safety measures was participants' assessment of their vulnerability to the risks. However, participants were less likely to use safeguards that were expensive or time-consuming.

[5]People between 18 and 25 years of age experiencing increased independence [4].

Overall, younger adult Internet users are the most active and the most confident group of Internet users, as well as those who post the most content. However, they feel as vulnerable to Internet hazards as other groups, likely because they have the most experience with hazards.

2.7 Studies comparing younger and older adults

In 2004, Grimes et al. [33] explored Internet users' experience and attitudes towards spam. They surveyed 205 adults ranging from 18 to 83 years of age and discovered that significantly more older adults reported having made a purchase as a result of spam email than younger participants. Older respondents received the same amount of spam as participants in other age groups despite lesser Internet related activity. In a later study, Grimes et al. [32] explored participants' understanding of computer related security hazards. They surveyed a group of 120 housing authority residents, older persons with low income or persons with disabilities, and compared them to 47 college students. They found that the housing authority residents answered fewer of the Internet security and threats related questions correctly than did the college students.

However, weaker security knowledge in older adults is not always the case. In 2010, Hoofnagle et al. [39] compared younger adults and older adults' privacy-protecting behaviours, attitudes toward online privacy protection, and knowledge of information privacy law. They analyzed results of a survey of 1000 English speakers in the United States and demonstrated that adults aged 55-65 knew more about online privacy law in the US than did younger adults (aged 18-24), who knew roughly the same as adults aged 65+. Further, younger adults and older adults had very similar attitudes towards online privacy norms and policy.

While they may have similar attitudes toward privacy, there are marked differences between younger and older adults in terms of their online activities. According to a 2013 report by Statistics Canada [3], only 10% of Canadians over 65 watched movies or videos on the Internet compared to almost 80% among those age 18 to 24.

Hill et al. [37] found that older Internet users have varying degrees of understanding of computing and the Internet, and their online behaviours vary widely from one

person to the next. They conclude that older adult Internet users are a heterogenous group whose behaviours are influenced more by each person's unique perceptions, culture, interpersonal relationships, and operational skills than their age. While there are mixed findings on knowledge of Internet related hazards in older adults, the findings concerning younger adults were more homogeneous.

The following research questions guided our exploration of older adults' perceptions of online risk:

R1: What are older adults' perceptions of risk in email and Facebook and how do these differ from younger adults'?

R2: What safety strategies do they use to stay "safe" from risks in these online activities and how are these different from younger adults'?

R3: What are older adults' sources of security-related information and how do they differ from younger adults'?

We address these questions qualitatively in order to determine what older users know without limiting their responses to certain risks or closed answer questions. We explore these topics with both older and younger adult Internet users and compare them quantitatively to provide a frame of reference for interpreting the findings from older adults.

Chapter 3

Methods

We conducted semi-structured interviews with younger and older adults to discover similarities and differences in their understanding of online security and privacy risks, the safety strategies they use to mitigate these risks, and their sources of information on these topics. To provide context for the study results, participant demographics, procedures for ethics approval, participant recruitment, and interview procedures are described in this section. Discussion regarding the rationale and reasoning behind the interview questions and the quantitative and qualitative methods used to analyze and contextualize the data are also included.

3.1 Participants

3.1.1 Demographics

As Morse [53] explains, when using semi-structured interviews, if one obtains a small amount of data per interview question, the researcher needs at least thirty participants to obtain the richness of data required for qualitative analysis. We interviewed thirty-one participants; fifteen older adults and sixteen younger adults. Younger adult participants ranged in age from 18 to 29 years old (M = 23.2) and the older adults ranged in age from 65 to 88 years old (M = 71.7). Demographics information is summarized in Table 3.1.

Nearly all of the younger adults (n=13) reported using the computer 31 hours or more per month. In the older adult group, nine of the 15 participants use the computer 31+ hours a month with the remaining six participants reporting using the computer in varying lower amounts as detailed in Table 3.1.

Only one participant reported formal training in computer security, having taken a course in systems analysis. This participant was an older adult and was included

in interviews to represent a more complete spectrum of computer knowledge in older adults. The demographics questionnaire included a Likert scale question about computer help with response options ranging from "1: I often ask for help" to "5: Others often ask me for help" (see Table 3.1). This question was obtained from related work [20] to help determine users' self-assessed computer knowledge. In general, younger adults reported being asked for help more often and older adults reported asking for help more often.

Two participants in each age group had programming experience; one older adult had programmed in Cobol, Fortran, C++, SAP and HTML, and the other older adult had programmed in Fortran. Both younger adults had programming experience in Java and HTML, and one of them had also programmed using the Processing and Visual Basic languages.

Participants in both groups had completed a broad variety of formal education ranging from high school to graduate studies. For example, seven younger participants had completed some university, and two completed high school. Four of the older adults had received a high school diploma while three others had completed a graduate degree. A larger percentage of older adults with graduate degrees are included in the study than is likely found occurring in the general population. We hypothesize this is the case because these individuals may have been more aware of the nature of graduate student research in terms of the need for participants and the interview process, and as such were more willing to volunteer to participate. However, because none of these participants had graduate degrees related to computing, we do not think this will skew the results.

3.1.2 Recruitment and sampling

The thirty-one participants were recruited from three Canadian cities: Ottawa, Ontario; London, Ontario; and Charlottetown, Prince Edward Island. We recruited users who accessed the Internet at least once a month on a computer, who did not have extensive training in computer science, and who fell within the 18-29 years age group or the 65+ years age group. These age groups were used in related research [33] [16] [39] [50] therefore we chose to apply similar inclusion criteria to improve

comparability of the results.

In Ottawa, purposive sampling was initiated by placing posters advertising the study on Carleton University campus, at a community center, and at a seniors' center. Other participants were recruited using word-of-mouth and snowball sampling, through participants who had previously been interviewed, as well as young adults and seniors already known to the author. Non-probabilistic sampling is often used to find participants who are otherwise difficult to contact [44], which was the case for recruiting the older adult Internet users.

3.2 Procedure

3.2.1 Ethics

We completed a Minimal Risk Ethics Protocol Application in the Fall of 2012. The Carleton University Research Ethics Board determined that the project met appropriate ethical standards as outlined in their Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, 2nd edition and the Carleton University Policies and Procedures for the Ethical Conduct of Research. Ethics clearance was given on 11 October 2012 until 31 May 2013 and extended until 31 May 2014.

3.2.2 Piloting

Prior to formal participant interviews, five pilot interviews were held to receive feedback on question clarity as well as to determine whether questions should be added or removed. Lazar 2010 [44] describes pilot testing as beneficial to the interview process because it aids in determining questions that may be difficult to understand. Pilot testing may also give researchers a more accurate idea of the potential length of the interview. This practice also aids researchers by helping them feel more comfortable conducting the interview. Pilot participants met the age group criteria of the study; two participants were between 18 and 29, and three participants were 65+. All participants accessed the Internet at least once a month and consented to participate in the pilot interview, and none had a degree in an IT or related field. All of the five pilot interviewees were recruited via convenience sampling.

Category		Younger adults		Older adults	
		n	%	n	%
Age					
	18-19	5	31%	0	0%
	20-29	11	69%	0	0%
	65-69	0	0%	7	47%
	70-79	0	0%	6	40%
	80-89	0	0%	2	13%
Gender					
	F	9	56%	9	60%
	M	7	44%	6	40%
Computer help					
	1: I often ask for help	0	0%	4	27%
	2	2	13%	6	40%
	3	4	25%	4	27%
	4	8	50%	0	0%
	5: Others often ask me for help	2	13%	2	7%
Hours of computer use/month	1-5	0	0%	2	13 %
	6-10	0	0%	0	0%
	11-20	0	0%	1	7%
	21-30	3	19%	3	20%
	31+	13	81%	9	60%
Highest level of education	High school diploma	3	19%	4	27%
	Some university	7	44%	2	13%
	Bachelor's degree	0	0%	2	13%
	Bachelor's degree and some professional	4	25%	1	7%
	Professional degree	0	0%	1	7%
	Some graduate school	1	6%	1	7%
	Graduate degree	1	6%	3	20%

Table 3.1: Participant demographics

Participants were asked whether they felt there was ambiguity in the questions, or if they could think of any questions that had not been asked, but likely should be asked to more fully address their perception of online risk. Based on pilot feedback, we decided to specify that the interview covers home computer use instead of business computer use (because businesses often have IT departments that look after computer security), and that the questions would not pertain to tablet use. We also added a question regarding what users think viruses can do, as the previous questions failed to address this subject in sufficient detail.

3.2.3 Semi-structured interviews

The three research questions and the direction of the project largely determined the most appropriate data gathering method. We were primarily interested in users' perceptions of online risk, how they had handled previous security related events, and where they had learned about Internet security. Semi-structured interviews provide researchers control over the basic structure of the interview and the questions asked. They also allow for opportunistic interviewing; the capacity to follow up on any new or related topics the interviewee may bring up that were not originally included in the interview questions [44]. We considered and discarded other research methods because a rich understanding of user cognition cannot be determined by other methods such as participant observation alone, by the necessarily rigid structure of surveys or questionnaires, or even in focus groups. Limitations of using semi-structured interviewing are discussed in Chapter 7.

Screening and interview processes: Participants who were interested in the study replied to the poster or contacted the author separately via e-mail or phone to find out more about the interview. The author used e-mail and phone communications to screen the participants, asking if they fell into either of the necessary age groups, if they had a degree in an IT related field, and if they used a computer at least once a month. Once participant eligibility was determined, the participants were provided with details about the type of questions we would ask during the interview. If they agreed to participate, a time and location were decided.

Interviews were conducted in various locations (e.g., at the participant's home, in a private room on Carleton campus, or at a local coffee shop), digitally recorded, and later transcribed for analysis. The session started with introductions and small talk to create a common ground between the interviewer and the interviewee, followed by more detailed information about what type of questions would be asked during the interview. Participants were welcome to skip any questions, stop the interview at any time, ask that the audio recorder be turned off, or ask that anything they said be stricken from the record. We asked the participants to sign a consent form (Appendix A) for our records. Participants completed a demographics form, so that we could explore whether relationships exist between demographic factors and how users perceive online risk, the results of which are in Table 3.1.

Each interview began with questions regarding the participant's online behaviours to determine which follow up questions would be the most appropriate. The interview guide is discussed in Section 3.3.1. The interviews lasted approximately 60 minutes each. Participants were then thanked, provided with $20 remuneration, and asked to sign a form confirming they had received their remuneration.

3.3 Measures

3.3.1 Interview guide

The interview guide included 17 core questions and four concluding questions. The 17 questions were broken up into eight sections; Confidence, Computer Behaviours, Risk, Strategies, Knowledge of assets, Lessons, Prevention and treatment, and Experience (see below and Appendix C).

3.3.2 Interview questions – risk, threats and security

Confidence: The confidence section simply asked how confident participants felt in keeping their computer safe. We asked this question to determine what, if any, relationship existed between users' perceptions of online risk and their confidence rating. This question was asked twice, once at the beginning of the interview and once at the end, the second time specifically to determine whether the interview itself

had an impact on participant responses.

1. On a scale of 1-10, 1 being not at all confident and 10 being completely confident, how confident are you that you know how to keep your computer safe?

When participants asked what was meant by keeping their computer safe, we explained that it was what "safe" meant to them, as we prioritized their perception of the term over ours and did not want to influence their response with new information. Any further comments and questions were transcribed along with the remainder of the interview.

Computer activities: Participants were asked whether they partake in particular online behaviours, with the option to add other relevant activities. The list of activities was used to guide follow-up questions.

2. Do you use the Internet for:
   (a) E-mail? Yes/No
   (b) Online Banking? Yes/No
   (c) Browsing for health information? Yes/No
   (d) Shopping? Yes/No
   (e) Social Networking? Yes/No
   (f) Other:

Risk: We asked participants if there were risks associated with each online activity identified in question 2. If so, we asked participants to discuss these perceived risks. These questions were intended to elicit initial perceptions of Internet risk.

3. Are there risks involved in:
   (a) Using Email? Yes/No. If Yes, What are they?
   (b) Online Banking? Yes/No. If Yes, what are they?
   (c) Browsing for health information? Yes/No. If Yes, what are they?

(d) Online Shopping? Yes/No. If Yes, what are they?

(e) Social Networking? Yes/No. If Yes what are they?

(f) Other - as identified by participant

Strategies: The strategies section of the interview followed the same format as the risk section; asking participants if they had strategies to stay safe(r) while participating in each online activity, and if so, what that strategy was.

4. Given those risks you just identified, do you have any strategies to stay safe when:

   (a) Using Email?

   (b) Online Banking?

   (c) Searching for and finding health information?

   (d) Online Shopping?

   (e) Social Networking?

Knowledge of assets: We asked participants to imagine that an attacker had broken into their computer, then envision what this attacker might do or what they might want. Responses to this question provide insight into what users think attackers are able to exploit, and thus what they may not realize attackers can exploit. Two follow up questions asked participants to prioritize their answers to the preceding question in terms of value, and to explain what they thought could be done with each stolen asset (if they had mentioned any). These were added to gather further insight into users' understanding of the extent of damage they could experience at the hands of an attacker, and thus the related risk.

5. If an attacker were to break into your computer, what do you think they would do or want?

   (a) (If they talk about different types of attacker – ask them what each "attacker" would want)

6. Of those assets that could be stolen, can you prioritize which you think is the most valuable to which is the least valuable?

7. What do you think could be done with this information?

Lessons: Participants were asked three questions in the lessons section of the interview. These include where they had learned about computing and computer security, including details regarding what they had learned, if they had ever had a computer security breach (or knew someone who had), including details regarding the security problems, and what security advice they would give.

8. Where did you learn about computing and computer security? Example: Work, Friends, School, Family.

   (a) What did they teach you?

   (b) Where did they learn what they know?

9. Have you or someone you know ever had any computer security problems? For example: got a virus, had an account broken into?

   (a) How did you know there was a breach?

   (b) What did they do to fix the problem?

   (c) Did you learn from that breach? If so, what did you learn?

10. If a friend of yours just got a new computer and came to you for advice about protecting their computer – what would you tell them?

Prevention and treatment: There were five questions in the prevention and treatment section of the interview guide. These varied from asking participants for their opinions regarding how to help users better protect themselves to asking them their opinion of their current antivirus software (if they used one). We decided that asking users how we as researchers could help them stay safe, directly, may give some new perspective on the topic. This section also included a question regarding what they would do if they were to discover that they had a virus on their computer

(that their antivirus could not heal), and to describe their thoughts on attackers. These questions included follow-ups clarifying who the participants think attackers are, and what attackers' motivations and goals might be. We asked these questions to determine how users thought about and understood malware and attackers.

11. Can you think of any way we, as researchers, can help computer users better protect themselves against attackers?

12. Do you use an antivirus program? Yes/No

    (a) If Yes, do you pay for the antivirus program?

    (b) What do you think the antivirus program does?

    (c) Do you think it does enough to keep you protected?

    (d) Can you think of any way the antivirus program could be improved?

13. If you were to find out you had a virus on your computer; what would you do about it?

14. What do you think about attackers? (Main goals, motivation, who are they)?

15. On a scale of 1-10, how confident are you that you can keep your computer safe?

Experience: We asked participants two questions to establish an estimate of their current security experience and knowledge. For example, participants were asked what they thought a computer virus could do. They were also asked to explain their understanding of the term "phishing", in an effort to gain a rough estimate of their familiarity with security terminology.

17. Can you please explain what is meant by the term "phishing"?

18. What do you think a computer virus can do?

Conclusion: Participants were asked four concluding questions to provide opportunity to add any further details before finishing the interview.

18. Is there anything you would like to add?

19. How did the interview go for you?

20. Do you have any questions for me?

21. Can you think of any questions that I could have asked but didn't?

3.3.3 Demographic questionnaire

The demographics questionnaire (Appendix B) included questions regarding participants' gender, computer use, formal training in computer security, year of birth, education attained, occupation, and type of computer they use. We also adapted three demographics questions from previous work in usable security [20]. These included participants' self-rating on computer help (whether they often ask for help or are often asked for help), experience with programming, and whether they had a degree in an IT-related field.

3.4 Focus of analysis

We decided that analysis and description of all of the interview results was beyond the scope of a Master's thesis and therefore chose to analyze and report on a subset of the interview questions. We analyzed participants' responses to Question 3 "Are there risks involved in: X and if Yes what are they?" focusing on responses about risks in email and social networking. Responses to Question 4, "Given those risks you just identified, do you have any strategies to stay safe when you X", were also analyzed, focusing on email and social networking safety strategies. Finally, we analyzed responses to Question 8, "Where did you learn about computing and computer security?", with a focus on participants' sources of information regarding computer security.

3.5 Data Analysis

Thematic analysis is described as a qualitative research method that goes beyond counting specific words or phrases within textual data and instead identifies and describes both implicit and explicit concepts [34]. The process involves developing codes to represent identified themes and applying them to raw data as markers for later analysis. This process lets the researchers compare code frequencies to determine prevalence of certain perceptions as compared to others. In terms of limitations, Guest [34] explains that "reliability is of greater concern with thematic analysis than with word-based analyses because more interpretation goes into defining the data items as well as applying the codes to chunks of text. This issue is even more pronounced when working in teams with multiple analysts." In the current research only the primary researcher defined data items and applied codes to chunks of text, and therefore concern regarding reliability is lesser than it would have been with multiple coders. We decided to use this method to analyze our data despite these reliability issues because thematic analysis is still the most useful, and most commonly used, method of textual analysis in capturing the complexities of ideas within a data set [34].

We implemented thematic analysis by following the six qualitative data analysis steps described by Creswell [14].

Steps 1 and 2: The first step involves organizing and preparing the data for analysis, and the second step involves reading or looking at the data to become familiar with the data and beginning to look for trends in what participants are saying. Both this first and second step were completed as we transcribed the 31 hour-long participant interviews and became familiar with the content as we listened to and typed out the interviews.

Step 3: This step involved coding the data of the two age groups separately, so that themes that may not have been apparent in the larger context of the groups taken together were taken into account. Coding the data involves consistently labelling sections of text that are similar to or relate to each other [66]. We used the Dedoose mixed methods data analysis software [49] which allowed us to take sections of data called "excerpts" and apply any number of codes to each one. By the end of analysis codes had been applied to 1233 excerpts of text totaling 4439 applications of codes.

An example of coding is provided in Table 3.2.

Step 4: Once open coding was completed, we grouped codes that related to each other under a new heading – a theme [9]. For example, when participants were asked how they stay safe using Facebook, we received a broad variety of responses such as double checking privacy rumors to see if they are true, being mindful that scams happen on Facebook, confirming they sign out when they are finished, changing their password frequently, and using a safe browser. These were grouped together into an overarching theme: general security behaviours.

Grouping codes together into themes was completed by printing the codes on slips of paper and physically arranging them into groups. The primary researcher independently grouped the codes in a first iteration and secondary researchers also thematized the codes to provide alternative interpretations and reduce bias introduced by the primary researcher. Inconsistencies were resolved through discussion between the primary researcher and the secondary researchers. After groups of themes were confirmed some codes were merged and data was re-examined to ensure consistent application of the codes. Quantitative analysis was completed by considering the relative frequency of each theme and differences between them.

Step 5: This step involved confirming how the themes were defined and represented. We describe the findings by providing a detailed discussion of several themes and subthemes, and providing participant quotations to illustrate each. To compare themes between the two age groups, we tabulated the number of participants who spoke about each topic and divided this by the total number of respondents in the age group to calculate the percentage. We then used Fisher's exact test and a cutoff of 0.2 to consider similarities and differences between the groups' reported themes (discussed further in Chapter 4).

The results of the thematic analyses are reported in Chapters 4 5 and 6. Chapter 4 discusses the themes concerning risks of email and social networking, Chapter 5 discusses results regarding participants strategies to stay safe while using email and social networking, and Chapter 6 describes where and how participants learned about online security.

Data extract	Codes	Theme
You can build a fake persona, I'm–I'm sure, if you studied people's submissions on Facebook–enough, but is that a real risk? Naw, I don't think so. I'm not looking at that as being a–a real, serious risk in this country in this day and age.	Aware of capacity to steal identity Not plausible in this country at this time	Doesn't feel at risk personally
I don't–I don't know enough about Facebook and I don't even know that now if I have my site setup, um, as secure as it could be. I don't really care–because I'm not going to put anything on it.	Report lack of understanding Not a risk for them given how little they post	
I put pictures of our family and yeah, I still feel comfortable	Doesn't feel at risk personally Posts pictures of family	
No, I don't feel a threat for a problem with privacy on social media because I'm more a looker than a sender	Doesn't feel at risk personally	

Table 3.2: Social media risk interview data analysis: sample data extracts with corresponding codes and theme.

Chapter 4

Risks

In this chapter, we address our first research question: *What are older adults' perceptions of risk in email and Facebook and how do these differ from younger adults'?* The results of our qualitative and quantitative analysis of participants' responses are organized into several main themes and subthemes that occurred in the data. In Section 4.1, we describe older participants' responses to the interview question asking if there are risks involved in using email and what those risks are, then compare them to younger participants' responses. Two older adult participants reported that there were no risks involved in using email, so our reported results represent the responses of the remaining thirteen older adults and all sixteen younger participants. In Section 4.3, we describe the risks reported by older adults regarding the use of Facebook and note differences between their responses and those of the younger adults'. Only seven older adults reported both using Facebook and that there are risks involved in doing so, therefore the results reflect responses of those seven older adults and all the younger adults.

When comparing the two user groups, we define our cutoff for notable differences between the frequencies using Fisher's exact test. Fisher's exact test compares frequencies on a 2×2 contingency table with small samples of categorical data [23]. This is appropriate given the binary "did or did not report" tabulating, and the small sample size in each group. When Fisher's exact test indicated a $p < 0.2$ we describe them as *notably different*; otherwise we report them as *not notably different*, or similar, in frequency. The typical $p < .05$ level was not applied as we were not interested in identifying only statistically significant differences. Instead we applied $p < 0.2$ as a guide to identify potentially interesting differences between the groups. For example, this corresponded to a difference of at least four people when comparing knowledge of email risks.

Theme	Sub-theme	Percentage of older adults	Percentage of younger adults
Receiving risks		92	75
	Virus	54	50
	Spam	38	38
	Scams	31	44
Account being hacked		15	31
Sending risks		31	19

Table 4.1: Email risks

The typical $p < 05$ was not applied because we were not interested in identifying only statistically significant differences, but instead use it as a guide or heuristic to identify potentially interesting differences between the groups.

Throughout the results chapters we discuss each theme and provide supporting quotes to illustrate user responses. Finally, when fewer than 15% of participants in either group reported on a particular theme, that response was not included in the tables as it was considered to be an inconsistent theme. Since participants' responses often covered a variety of themes and subthemes, the percentages reported below are overlapping. In Sections 4.1 and 4.4, we summarize our findings, beginning with those themes in which we saw notable differences between groups followed by themes with no notable differences between groups. Table 4.1 summarizes the themes and sub themes pertaining to email risk and Table 4.2 includes risks relating to social networks.

4.1 Email risks - no notable differences

The risks reported by both groups of participants fall into three main categories: risks involved in receiving or opening e-mails, risks involved in sending e-mails, and risks involved in having an email account accessed without their permission. Table 4.1 presents the main themes and the percentage of participants who spoke about each. Overall, older and younger adults brought up the same themes, and in similar frequency, which indicates no notable differences between the groups. We find that older and younger adults perceive email risks similarly.

4.1.1 Receiving/opening risks

Receiving/Opening risks involve receiving some kind of malicious email that, if opened, read, and acted upon, could result in loss or damage for the recipient. Older and younger adults reported this type of risk with similar frequency; 75% of younger adults and 92% of older adults reported such risks. Further, participants reported three specific types of receiving/opening risks: getting a virus from email, receiving spam, and falling for an email scam. We discuss each sub-theme separately.

Virus from an email: Roughly half of young adults and older adults (44% and 54%, respectively) reported the risk of getting a virus from an email. Our two groups appear to have the same level of virus email risk awareness. Participants in both groups described a number of different ways to get malware from e-mail. Specifically, four older adults and two younger adults described "virus emails" as those containing malicious links. Demonstrating learning from personal experience, one young adult described their experience with a malicious link: "I had one where I got an email, it had a little link, [I] clicked on it and then suddenly, my computer shut down". Further, three older adults and two younger adults described "virus emails" as email containing a malicious attachment. An older adult and two younger adults more vaguely mentioned "virus emails" that could download viruses onto their computer.

It is important to note that approximately half of participants made no mention of malware ridden email during the interview. Perhaps they do not consider downloading malware as a risk, or they receive "virus emails" so frequently that they are desensitized to the phenomenon. Another possible explanation is that our participants rarely receive malicious emails due to using email services with more built-in malware protection or by providing their email address to fewer email harvesting websites [43] and thus have no reason to consider them a risk.

Spam: Thirty-eight percent of participants in both age groups reported spam as an email risk. They defined this most frequently as receiving information they did not want, including advertisements or newsletters. While less straightforward as a risk, a few participants explained that they felt "inundated with emails" and felt

overwhelmed by the volume they were receiving. As one older participant described, "it's just annoying that it's there and I don't want it and I have to–I just delete it." They consider the risk as having their "findability" and availability exploited; in much the same way that telemarketing is disliked, there was a sense that spam invaded their personal space and this made them uncomfortable. As one younger participant explained, they are careful to whom they disclose their email so that this does not happen: " I don't like, give my e-mail address out to people, not like anybody {...} they could misuse it or send me stuff that I don't want". This animosity toward spam was felt by both younger and older adults equally.

It is possible that the remaining two thirds of participants do not consider spam as a risk because they receive less, and therefore do not feel inundated by it. Alternatively, they may have a different working definition of *risk* since we allowed users to choose their own definition. One participant identified their experiences with spam and how they defined risk in email as a "downside" to using email rather than something "unsafe". "If you sign on to a store, they send you their specials. Like some of the stores {...} I'm trying to delete them because they–you just get bombarded with emails. They ask you {...} 'Oh, we're having a draw. Can you give us your email address?' sort of thing. Guaranteed, you're going to be on their mailing list for life {...} I suppose that that's a risk. {...} I don't consider it unsafe. I just consider it a pain in the neck. I suppose it is a risk {...} this is the down side. If you're talking about risk as a downside".

Scams: Thirty-one percent of older adults described scams as email risks, similar to the 44% of younger adults. There were no notable differences between the groups in the types of scams reported. For example, 31% of younger adults and 15% of older adults mentioned phishing, either by name or by describing emails who pretend to be your bank to get your information.

The low frequency with which phishing was reported by both groups is concerning. This is especially worrisome for the older adults because they are more targeted for scams [11] and often have more to lose in attacks.

4.1.2 Account being hacked

Fifteen percent of older adults and 31% of younger adults described the risk of having their email accounts broken into and the private information within their e-mails accessed. For example, one participant explained unauthorized access in this way: "A password is a fairly simple protection, {...} the risks being people can take your information, if they could get in past your password they could get whatever you e-mail {...} and all the information you put to make the account, presumably, right? Like your address and all that".

4.1.3 Sending risks

Younger and older adults were similarly worried about the sending risks involved in using email. Thirty-one percent of older adults and 19% of younger adults described risks involved in sending emails. Participants were worried that the delivered email would be read by someone other than the intended recipient and therefore private information would be disclosed. As one older participant explained: "part of the risk is that email is unforgiving. You can make mistakes and, you know, inadvertently send an email to the wrong individual [...] I've done that before now and, uh, fortunately, I've not been embarrassed, [...] but you could wind up in an embarrassing situation". Additionally, participants in both age groups worried that the email address could be misspelled, the message unintentionally sent to the wrong person, and therefore the communication would be lost.

4.2 Email risks summary

In response to the first half of our research question: *What are older adults' perceptions of risk in email?*, we found that older and younger participants' perceptions of risks fell into the following themes: *receiving/opening risks*, *sending risks*, and *unauthorized access risks*. In response to the second half of our research question *how do these differ from younger adults'?*, we found that older adults reported these risks in equal frequency as younger adults.

These results provide evidence that older adults were equally familiar with email

Theme	Percentage of older adults	Percentage of younger adults
Unauthorized viewing	57	100
Uncertainty of risks	71	–
No personal risk	57	–
Privacy settings mistrust	–	19
Posting x is risky	43	44
Consequences	86	88

Table 4.2: Social networking risks

risks as younger adults. These results do not necessarily refute previous findings by Grimes et al. [33] [32] who suggested that older adults have less technical knowledge about email risk. Taken together, we suggest that older adults have similar knowledge of types of email risks, but do not have equal technical knowledge of the risks. We therefore assert that older adults have a similarly broad or surface understanding of email risks, but suggest that their understanding is more shallow than younger adults'.

4.3 Social networking risks

The thematic results regarding risks in social networking represent the responses from 7 older adults and 16 younger adults. All participants were Facebook users, so the results reflect experience in the context of Facebook rather than in social media more generally.

Participants' responses regarding their perceptions of Facebook risks were more varied than those of email risks. Participants described several risks in the context of email, but when asked about Facebook risks older adults spoke more about their thoughts and feelings regarding risks of using Facebook than list potential hazards.

As summarized in Table 4.2, older adults' responses to the question about risks in social networking fall into five main themes: *risky posting x*, *unauthorized viewing*, *consequences*, as well as *uncertainty of risks*, and *no personal risk*. Their responses differed notably from younger adults' who did not describe the *uncertainty of risks* or *no personal risk* themes, but instead included responses in the *privacy settings mistrust* theme. All younger adults also reported the risk of unauthorized viewing

while only four older adults reported the same, indicating another notable difference between groups.

4.3.1 Fewer older adults: Unauthorized viewing

Fifty-seven percent of older users reported the risk of unauthorized people viewing their posted information. Some participants refrain from posting certain information because of this risk. Some explained possible consequences, while others cited having only a minimal understanding of who could see their information. As one user reported: "I suppose the risks that are there are in divulging private information to people who you have no intention of divulging it to. So {...} I don't understand the technology well enough to know when I put something on the Facebook site, for example– how far that can be disseminated, you know. Is it just to my friends? I hope it is but then what can my friends do with it. I don't know". Comparatively, this risk was described by every young adult, which indicates that notably fewer older adults were concerned about unauthorized viewing or considered it a plausible risk.

4.3.2 Older adults only: Uncertainty of risks

Seventy-one percent of older adults reported a lack of understanding regarding Facebook risks. No younger adult mentioned uncertainty, indicating a notable difference between the groups. Older adults knew there were risks, but felt uncertain regarding what they were or how they worked. As one participant explains: "I don't know all of the risks because I don't understand it well enough." Many older users felt less aware of social networking risks and reported being cautious about what they post on Facebook in an attempt to protect themselves from unknown harm.

Most older Facebook users reported not starting to use Facebook of their own volition, but instead were prompted to join by their children or other family members. Thus their motivation to understand and use the application may be different from younger users. This differing motivation may influence their interest or willingness to consider the possible risks, or any desire to become informed on the topic. It may also impact how they explore and utilize the various privacy settings options available on the site.

4.3.3 Older adults only: No personal risk

Fifty-seven percent of older adults said that although they realized there were risks involved in using Facebook, they were not personally at risk given how little personal information they felt they revealed on the site. No younger adults reported not feeling at risk. One older participant explained "I'm only on Facebook to stay in touch with my grandchildren, so what risks would there be for me, because I don't put that much information on [Facebook]?" We note that this only reflects user perception of the information they post and may not accurately portray of the actual hazards, particularly if users misunderstand the value of posting some types information.

4.3.4 Younger adults only: Privacy settings mistrust

Nineteen percent of young adults voiced concerns related to Facebook privacy settings, while no older adults mentioned similar concerns. While this difference is interesting, it does not meet the threshold to be considered a notable difference between the two age groups as it was reported by very few participants. As one younger adult explained: "The only thing about Facebook is that they change it all the time. {...} So sometimes I've set it to a certain thing but once they change it, it resets everything or it doesn't set it the way I wanted it. {...} And I don't find out 'til like months later {...} where someone brings up like, 'Oh, I saw this on your Facebook.' I'm like, 'What?{...} I don't–I didn't want anyone to see that.' But, so when they change it and change the way you set things, it–it's really annoying." These younger adults actively manage their Facebook settings, but have had experiences with their settings not being applied as intended, or their settings having been updated by Facebook to allow for more public access than they would like.

In contrast, older adults did not report mistrust of Facebook privacy settings, likely because none use the settings in the first place. This lack of use, and therefore lack of reliance on, Facebook's privacy settings may mean that older participants' strategy of posting very little is the only strategy they have to stay safer from people misusing information about them or from privacy breaches. This strategy may not in fact provide adequate protection as older users unknowingly post information that may still be exploited.

4.3.5 Both older and younger adults: Posting x is risky

Older adults reported *Posting x is risky* in the same relative frequency as younger adults at 43% and 44% respectively. This theme represents responses regarding the risk involved in posting sensitive information on Facebook. Examples of sensitive information included posting that they were leaving on a trip, posting their home address, and, more generally, posting "too much about yourself".

One older adult explained that they did not know why posting certain types of information was dangerous, but felt that it was risky: "I don't know what the risk is, however, I knew that I decided that if any friend wants to contact me, my birth date is not useful or helpful information." Some of the participants stopped there, without explaining the danger. Other participants elaborated that a "bad guy" or "unauthorized viewer" could possibly see it, which we categorize separately in the *Unauthorized viewing* theme. Further, some gave examples of consequences that could occur if this risky information was used maliciously; these are included in the *Consequences* theme.

4.3.6 Both older and younger adults: Consequences

Eighty-six percent of older participants and 88% of younger adults reported a variety of consequences that could occur due to exploitation or unauthorized viewing of posted information. Older adults spoke of physical consequences such as being robbed while away from home. One older adult explained that they avoid posting they are away from home for this very reason: "I'm really careful not to ever say 'I'm going on a vacation"' V [1] –" you don't want to put yourself at risk?" P[2] – "for theft here, at the house, even though they don't have my address, I'm easily findable in terms of the telephone book or canada411".

Other older adults spoke of general privacy when reporting consequences. While not physically or financially damaging, they spoke of embarrassment that could occur. One older adult explains their attitude towards this type of risk: "Privacy is something that you open up as much as you want – and if you want to open up and tell the

[1] V stands for the interviewer
[2] P stands for the participant

world about all your warts, then don't complain that the people know about all your warts".

Older adults also brought up damage to reputation as a possible consequence of using and sharing information on Facebook. However, they explained this more often as a risk for younger people than a risk that personally impacted them. As explained by one older adult: "I think for young people today they have to be damn careful about what they're putting on Facebook because it's going to come out and bite them in the ass {...} ten years down the road, twenty years down the road when they're looking for a job".

Only two older adults and one younger adult discussed identity theft as a possible consequence of social networking. This was lower than we expected given the media attention and severity of that particular risk.

4.4 Facebook risks summary

In this section we answered our research question: *What are older adults' perceptions of risk in Facebook and how do these differ from younger adults'?* Overall, older and younger adults seemed to have similar ideas of some Facebook risks, notably regarding posting, viewing, and exploitation of information. Media and other educational efforts appear to have been successful in communicating risks regarding the release of personal information, or users have been able to determine this risk on their own. However, we note that knowing not to post personal information or knowing that information can be exploited does not necessarily indicate deep understanding of why personal information should not be promulgated.

Older and younger adults differed in their understanding of other risks. Older adults expressed uncertainty regarding Facebook risks, a theme not brought up by younger adults. This uncertainty may be due to inexperience and possibly a lack of exposure to relevant Facebook privacy and security information. Further, only older adults reported not feeling at risk while using Facebook; this notable difference may be due to their primary Facebook strategy, which will be discussed further in Chapter 5 as well as in Chapter 7.

Chapter 5

Mitigation Strategies

In Chapter 4, we addressed our first research question and determined that older adults reported three types of email risks and brought up five themes regarding risks of using Facebook. We follow up in the current chapter by reporting on research question *R2: What safety strategies do older adults use to stay "safe" from risks in these online activities and how are these different from younger adults'?* The results are organized into several main themes and subthemes that occurred in the data.

In Section 5.1, we describe older participants' risk mitigation strategies in the context of email, and compare them to younger adults' responses. Our results represent the 13 older adults and 16 younger adults who reported that there were risks involved in using email. In section 5.2, we discuss the single Facebook risk mitigation strategy reported by the older adult Facebook users, summarize their perceptions of Facebook strategies, and compare their strategies and perceptions to younger adults' strategies. In each section we first discuss themes with notable differences between groups and follow with themes that were reported with equal frequency by participants in both groups.

5.1 Email safety strategies

All thirteen older adult email users reported actively taking measures towards secure email usage. Participants' individual strategies reflected their perceived risks, with more effort concentrated on threats viewed as more severe, namely the receiving risks. Many participants stated that they employ multiple strategies to stay safe. Older adults often depend on secondary sources to offer protection such as advice from a trusted advisor or their antivirus software. The two groups' mitigation strategies are summarized in Table 5.1. We discuss each strategy in turn and provide supporting quotes to illustrate user responses.

Theme	Sub-theme	Percentage of older adults	Percentage of younger adults
Antivirus will protect		38	-
Actively filter		-	31
Advice from mentor		31	-
Considers context		77	63
	Consider sender	69	50
	Consider subject line	31	44
	Consider content	46	25
Contact sender		-	19
Cautious sending		23	13

Table 5.1: Email strategies

5.1.1 Older adults only: Antiviruses

Thirty-eight percent of older adults reported using their antivirus system(s) to keep them safe from email threats, but offered no further explanation as to how. No younger adult mentioned their antivirus in this context, which indicates a notable difference between the two age groups. Older adults rely heavily on their antivirus systems to keep their computer free from malware in the event that they do open a malicious link or attachment. As one participant put it, in regards to staying safe while using email: "Um, we have AVG on the computer {...} and, uh, it seems to do the work for us". These older adults fully trust their antivirus protection and seem unaware of its potential limitations. For example, none indicated an understanding that antivirus software may be ineffective against zero-day threats[1] or malware variants that have not yet been recognized and addressed by the antivirus provider.

As a related strategy that also relies on third party assessment of risk, a few older participants discussed immediately deleting emails that had been flagged by their email provider as being malicious. One participant explains "if an e-mail message comes in and it's got a 'we believe this message is –' it's always tagged in red, I immediately send it to trash and double trash it, so it's out of my system I hope". Taken together, it appears older adults fully trust their email provider and anti-virus software to keep their computers safe from infection. While using these security mechanisms is prudent, older adults displayed an over-reliance on the systems and

[1] A zero-day attack is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known.

assumed that they offered more protection than is realistically possible with current technology. This reliance on third parties may be putting these older adults at risk by giving them a false sense of security and reducing their vigilance in other respects.

5.1.2 Older adults only: Lessons from advisors

Thirty-one percent of older adults reported having a trusted security advisor whom they consulted for security related questions or problems, and whom they considered as a resource that helped them stay safer online. Comparatively, no younger adult reported access to such an advisor as a resource they used to stay safe from online risks. A few older participants explained that they paid these computer advisors for their services of helping, teaching, or fixing things for them. As one participant explains: "I use a woman who works for Bell and she comes to me privately and I pay her. She's coached me [...] she's coached me not to open anything I don't recognize." Other older adults had adult children with IT backgrounds who provided security and other computer related support. Some participants trusted "computer-savvy" friends with more computer experience or whose exposure to the latest risks and strategies was greater than their own. These friends had no formal computer security training. For example, when talking about malicious emails, one adult explained that "usually there's nothing in the subject line apparently {...} I've never had one but my friend says that you can often tell". This demonstrates not only these participants' reliance on others for their security information and risk mitigation, but also the importance of learning through hearsay and stories, which is discussed in further detail in Chapter 6.

5.1.3 Fewer older adults: Active filtering

Only one older adult mentioned actively using filtering tools offered by their email provider to eliminate potentially malicious emails from their inboxes. Comparatively, 31% of younger adults reported using this strategy. As the older adult explains: "I just want to keep all that crap out of my inbox, and so then I check the junk-mail because it goes into a separate file, and if it looks like I might want to read it, I do occasionally open the e-mail and check it". Younger adults specified actively blocking emails from particular senders, creating different folders for differently trusted senders

or moving emails into their junk mail folder. Neglecting to use filtering options may result in more malicious messages arriving in the inboxes of older users, and this increased exposure may increase the likelihood of exploitation.

5.1.4 Both older and younger adults: Consider email context

Older adults reported considering the context of the email as frequently as younger adults when deciding whether or not to open emails they receive. The context of email involves the information readily presented to a user about an email in the user's inbox. Overall, 77% percent of older adults reported checking the context of the email and 63% of younger adults reported the same.

Participants reported considering three different aspects of the email as part of the decision making process. Specifically, participants reported considering the sender of the email and its subject line to determine the likelihood that the email was sent by the person identified in the From field. If participants trust the email up to this point, they consider the content of the email for legitimacy and cohesion with their relationship and the sender's previous behaviour before taking any action, such as clicking a link within the email, or downloading an attachment. We discuss each as aspect of email context separately below.

Both older and younger adults: Consider the sender: Sixty-nine percent of older adults consider whether they know the sender before opening the email, which was similar to the 50% of younger adults who reported the same. Both groups explained that, as a rule, they do not open email from senders they do not know. As one participant explains: "I only open, say, emails from people I know. If I don't know [the sender], I don't open it, I erase it". Even if they do recognize the sender, participants consider the likelihood of that person sending an email. One example of this plausibility consideration is explained by another participant "well if it's from a bank or something it's kind of fishy, like if it's from a bank that's not my bank".

It is surprising that not every email-using participant reported these safety strategies. It may be because this strategy is so automatic for some users that they did not even consider it to be a safety strategy when asked the question. Further, participants

in both groups recognized that malicious emails could be sent by both strangers and senders they know. One participant elaborated "you could get a virus from e-mail, not knowing who's sending it or sometimes it's disguised as someone that you may think you know".

Both older and younger adults: Consider the subject line: After checking the From field, 31% of older adults consider the subject line to determine whether they will open the email, as did 44% of younger adults, which indicates no notable difference between the groups. Older adults consider whether the subject is missing, is written in all caps, is generic or vague, or does not seem like something that sender would send them before deciding whether to open the message. For example, one participant discusses the signs of potentially malicious email: "in like the subject it's not very personalized, kind of generic, or sometimes they use capitalized letters, I don't know, it's very weird, and you can kind of like tell that it's not something from like a real person". All but one younger adult who had described checking the sender originally also reported checking the subject line. However, there was a 38% decrease between those older adults who considered the sender and those who considered the subject line of the email.

Both older and younger adults: Considering the body: Forty-six percent of older users consider the body of the email before deciding to delete it or to follow through with any additional action. Twenty-five percent of younger users reported using this strategy as well, indicating no notable difference between groups. Participants consider whether the information in the body of the email is characteristic of the sender, given their relationship. Uncharacteristic emails get deleted without further action. As one older participant explains "I have received some from my brother and what they were talking about was not something that he would talk to me about so I deleted it. Though I did open it. Unless it's something I definitely know then I would not open an attachment because the way I understand it is the threat is in the attachment. And that you could download something that will affect your computer." Another older adult described their strategy to avoid scams "If you take the attitude that there–you're never going to get something for nothing, it's obvious."

5.1.5 Both older and younger adults: Confirm with sender

One older adult reported that they would contact the sender prior to opening the email if the subject line seemed unusual given their previous knowledge of the sender's behaviour. Young and older adults did not differ in this respect, as only three of the younger adults reported the same. As one younger adult explained: "if it looks suspicious I'll text my mom and say 'Hey, did you send me this?' and she'll either say 'no, I didn't send you an e-mail today' or 'yes I did'. While effective, this additional out-of-band verification is reported only by a minority of participants in circumstances deemed suspicious, likely because it is time-consuming and may take more effort than most users are willing to spend.

5.1.6 Both older and younger adults: Avoid sending damaging information

To protect themselves from sending risks such as unintended disclosure, a minority of older adults avoid sending potentially damaging information over email. Twenty-three percent of older adults claim that they do not email information such as credit card numbers, banking numbers, or personal information that they would not want the public to see. This was not notably different from the 13% of younger adults who reported the same. Participants explained that if they needed to share such information they would do so on the phone or in person. One older adult explained that they send "just messages that I wouldn't mind being forwarded to anybody in the universe" because they realize that sending more private information could be dangerous.

These types of strategies were not commonly reported, likely because few participants reported any type of risk involved in sending email, and therefore saw no need to take protective action. An alternate explanation may be that users are so conditioned to avoid entering such information that it did not occur to them to bring it up during the interview, however we have no data to verify this conjecture.

5.1.7 Email safety strategies summary

Our second research question was "*What safety strategies do older adults use to stay "safe" from risks in email and how do these differ from younger adults?"* We found that older participants' mitigation strategies primarily involved scrutinizing emails before opening them or before taking further action. This reflects the previous chapter, where older adults were most concerned with receiving unwanted or malicious email. Older adults were more likely than younger adults to report using antivirus protection and receiving guidance from others as resources to stay safe from email risks. They were also less likely to proactively use email-filtering tools.

The older adults compensate for a lack of experience (indicated by their reported lesser time spent computing), and lower confidence in their email security knowledge by using antivirus software which they believe protects them, and by consulting with advisors to gain further insights. Relying on a third party for security is a common finding in risk perception literature [16], especially when security is not a primary task or concern.

5.2 Social networking strategies

Participants were asked if they used any strategies to stay safe when using social networks, and if so, to describe these strategies. Analyses of their responses resulted in the themes and frequencies included in Table 5.2. Older adults' responses fell into two main themes: mindful release and unfamiliarity with privacy settings. Younger adults' responses were more nuanced and fell into four main themes: preventative settings management, friend management, mindful release, and general security practices.

5.2.1 Younger adults only: Preventative setting management

Sixty-nine percent of younger adults reported using privacy controls to narrow who could access their Facebook information, while no older adults reported using this strategy. This represents a notable difference between the two age groups.

Younger users are taking advantage of the privacy settings provided by Facebook and relying on them to some degree to keep their information away from unintended

Theme	Percentage of Older adults	Percentage of Younger adults
Mindful release	71	63
Privacy setting management	–	69
Privacy settings elusion	43	–
Friend management	–	38
General security practices	–	25

Table 5.2: Social networking strategies

viewers. On the other hand, our results suggest that older adults may have more public profiles or have more of their information available to other users than they realize. Despite being careful about what they post, not using Facebook privacy settings may be exposing these older users to greater risks than they realize.

5.2.2 Older adults only: Privacy settings elusion

Forty-three percent of older adults do not know how to use Facebook's privacy settings. As one participant explained: "I understand that there are more safeguards that you can put in place by, um, modifying the settings on your Facebook account, but I don't really understand how to do that". This lack of understanding may be putting these users and their contacts at increased risk of data misuse. Some older adults were ambivalent about privacy settings. As one participant explained "I don't even know that I have my site setup, um, as secure as it could be. I don't really care – because I'm not going to put anything on it." However, another older participant expressed frustration about the lack of usability of the privacy settings, explaining that "I don't know what I can do and what I can't. It's certainly not obvious. There's supposed to be a way you could control public information versus friends but, uh, it's not obvious. It doesn't tell you. And I think that's not fair that they're not–they're not telling me. You have to know what you're doing before you go on it. I don't know what I'm doing."

This lack of usability of Facebook's privacy settings for our older adult users is concerning. Usability should not be a barrier for increased privacy, and the poor usability of privacy features is putting users at increased risk. From the users' perspective, privacy settings should be easy to understand, be easy to apply, and be

conservatively set by default.

5.2.3 Fewer older adults: Friend management

Only one older adult reported actively managing their Facebook friends, while 38% of younger respondents reported the same, which indicates a notable difference between groups. Actively managing Facebook friends involves being selective about the people they add on Facebook and/or pruning their Facebook friends according to changing comfort and disclosure levels. Older adults may not actively manage their Facebook friends because they are less concerned about others seeing their posts, given how little value they attribute to the information. Older adults also primarily included only family and close friends on Facebook, who they have less reason to prune, whereas younger adults often have a broader variety of Facebook friends [51]. Younger adults are more likely to include acquaintances and other near strangers, leading to a greater need to actively manage their list as their relationship with those people changes [51].

5.2.4 Both older and younger adults: Mindful release

Seventy-one percent of older adult users reported using only one strategy to stay safe when using Facebook: minimal release of information. They reported including little information on their profile, as well as posting little in terms of status updates. Similarly, 63% of younger adults were careful about the information they disclosed on Facebook. For example, they reported including only minimal or false personal information on their profile. A number of younger adults also discussed limiting their text and photo posts to things they considered "grandma appropriate". Interestingly, older adults did not see a risk in posting photos. One participant explained that "I don't see a risk in, in people knowing that I have grandchildren out in (city) and all that. Me sending pictures of a family gathering in the house. No, I don't see a risk in that." It seems the older adults are careful regarding posting explicit pieces of information about themselves, but they are less cautious when it comes to information and photos of their family.

Posting limited or false information is certainly a good strategy, however, it remains unclear whether older adults in particular understand enough about exploitation of information to make educated decisions regarding what they release. Pictures in particular can be used for nefarious purposes and it seems that at least a few older adults post these freely. While younger users report mindful release of their information in roughly the same frequency, they also report a number of other strategies that offer a second line of defense against exploitation of that information.

5.2.5 Few older and younger adults: General security practices

Finally, 25% of younger adults applied general security practices to Facebook, however, while this was only brought up by one older adult, it does not demonstrate a notable difference between the two groups. The 'general security practices' theme is characterized by users confirming they had signed out of their account when finished with it, and/or changing their login password regularly. This minority of participants is applying the same security practices they already have in place for other accounts, indicating that security training in other areas of computer security is being applied across platforms.

5.2.6 Social networking strategies summary

These results address our second research question: regarding safety strategies older adults use to stay "safe" from risks in Facebook and how they are different from younger adults'? Older adults reported mindful posting as their sole safety strategy. Comparatively, younger adults reported using this strategy as well as a number of others. An important finding is that older users discussed unfamiliarity with Facebook's privacy settings; features that most younger adults used extensively. Additionally, younger adults actively manage their Facebook friends and apply general security practices but very few older adults mentioned these topics. It is unclear whether older adults failed to mention these strategies because they consider themselves at low risk of attack or whether they feel their account has little value due to the limited information posted on it. Older adults limit their release of potentially damaging information because they do not understand the possible risks.

While not completely safe, older adults' hesitancy may keep them out of harm's way to some degree. However, given their unawareness of Facebook's privacy settings paired with their uncertainty of the risks, it is debatable whether their feeling of safety, or "no personal risk" as mentioned in Chapter 4 is merited. For example, several older adults mentioned posting pictures of grandchildren, or other family and friends, on Facebook. Without increased privacy settings, they may unwittingly open the subjects of the photos to risks such as stalking, identity theft, or even pedophilia. It is clear that younger adults have more safety strategies and take greater advantage of available security tools than older adults when it comes to Facebook use.

Chapter 6

Lessons

As computing and technology develop over time, so does learning about how to use the technologies, and how to stay safe using them. It is not practical for any person to have only a single source of information regarding computing and computer security. We are surrounded by information about technology supplied by the media, people we talk to, literature, formal courses, and personal experience. We explore our third research question in this chapter: *What are older adults' sources of security-related information and how do they differ from younger adults'?* The explanations below summarize participants' most prevalent responses when asked where they learned about computer security.

We separate storytelling as a format in which information was communicated from the information sources in our data analysis. Related research suggests that lessons learned from stories play a significant role in making security related decisions [57] and we wanted to determine the prevalence of this teaching format for our participants. After coding and thematizing older adults' responses, we found that their learning came in the form of stories, and from any number of external sources including: family, friends, media, a computer course, work experience, and paid help.

Younger adults' learned from stories as well, and, unlike the older adults, also reported being self-taught. Their other sources of computer security information were family, friends, media, and a computer course. They did not report work experience or paid help as informational sources, as older adults did. A summary of the prevalence of each theme is provided in Table 6.1. The self taught theme is presented first, as it was the only theme to be reported in notably different frequency between the groups, followed by the remaining themes that were reported in similar frequency by both groups.

Theme	Percentage of older adults	Percentage of younger adults
Self taught	–	44
Work experience	13	–
Paid help	13	–
Family	53	50
Friends	25	19
Media	40	31
Computer course	13	13
Stories	40	44

Table 6.1: Security lessons

6.1 Younger adults only: Self taught

Only one older adult reported teaching themselves about Internet security, however, 44% of younger adults report being self taught on the subject, which demonstrates a notable difference between the groups. The self-taught theme is characterized by demonstration of proactively finding or determining safe practices on one's own rather than taking in information provided by others. For example, one participant explains learning about secure online behaviour: "(I'm) Just self-taught, I guess. {...} it's more like general common sense. Like you know that {...} with online banking, when you finish, sign out". Interestingly, this "common sense" approach was not reported by the older adults.

In general, older adults had more difficulty remembering where they had learned about computer security because the learning tended to have happened over a longer period of time than it had for younger adults. One older adult explains: "I don't know, (I learned from) nobody specific, but I don't think you could be exposed to computer for 25 years without figuring out that there are issues out there." Therefore, it is possible that older adults were self taught years ago but fail to remember specifically teaching themselves. Older adults also were slightly more reliant on lessons from external sources, such as friends, family, media, and paid help, rather than teaching themselves. This may be due to their lesser overall computer use, as found in our demographics, and their lower confidence in computing found by other researchers [16].

6.2 Older adults only: Work experience

Two older adults reported learning about security risks and mitigation strategies from exposure to computer security practices in the workplace. No younger participant mentioned this method of learning. The older adults' experiences came in the form of conversations with IT staff and observation as their antiviruses were updated. As one older participant explains: "we also have an IT guy at work who does ... all our computers and he's the guy that I talk to a lot so if there's any problems or whatever or I'm wary about something I talk to him". Another participant learned about antiviruses and the importance of keeping them updated from her workplace experience: "we would get e-mails from the tech people in our building whenever there was something new that we had to do {...} they would come to your office and do the installation for you. Each new version of (antivirus) because it came out and if there were security upgrades that needed to be done on the computers they would come to all the computers in the building and do those for us."

These participants learned as their colleagues informed them about and protected them previously unfamiliar risks. This is similar to how some older users initially learned about viruses and the possibility of malware from the person who sold them their first computer: "when we got our computer first–which would be back in about 1995 {...} the young man that installed it for us said we should have some kind of anti-virus protection. And Norton was one of the choices".

6.3 Older adults only: Paid help

Two older adults reported learning about computer security from someone they paid to come to their home and help with their computers, while none of the younger adults reported this behaviour. One older adult explained that she has a trusted advisor: "she comes to my house when I call her and I pay her and she walks me through the problem and teaches me something." In contrast, younger adults reported asking a computer-savvy family member or friend when they needed help. This may be due to generational differences, in that not all older adults have relationships with technical helpers who they can contact and have their help for free.

6.4 Older and younger adults: Family

Fifty-three percent of older adults reported having learned about computer security risks and mitigation strategies from their family, which is similar to the 50% of younger adults with similar experiences. Clearly, family plays a significant role in security education.

Older adults reported learning about Internet-related risks and strategies primarily from their computer-savvy children, grandchildren, or spouses, but provided few details regarding what these family members had taught them. One older adult did elaborate about how she learned to avoid opening certain attachments. She explains: "my daughters-in-law apparently open attachments from Korean sources, which are horrible, {...} they get viruses apparently all the time, I don't know very much about that, I just know what –'s told me {...} (so) I don't open attachments, especially from Asian sources." This demonstrates the role children and grandchildren play in teaching older adults about computer security, a trend that may be leveraged to increase or improve older adults' access to information on the topic.

For younger adults, learning from "family" typically meant their parents, who had taught them about not giving out personal information, not interacting with strangers online, and using antiviruses. As one participant reported: "my mom always said 'don't open up anything from somebody you don't know' and then obviously my parents have talked about Facebook". Others reported how they learned about security by witnessing their parent protecting them from malware: "my dad used to work for [computer company], so he knows about antiviruses, like he doesn't really, but if I got a computer or something, he would put on antiviral software". Other important security information, such as identity theft or phishing, were not brought up, potentially because these young adults had few assets at the time of this instruction, and therefore parents felt little need to speak about it.

6.5 Older and younger adults: Media

Forty percent of older adults and thirty-one percent of younger adults reported learning about computer security from a number of different media channels. Older adults

specified hearing about Internet security topics on the news (television), in the newspaper, and/or hearing it on talk radio. One older adult explained that she learned about browser cookies from a newspaper column "change the cookies to the lowest amount except when you really need them." V - "Where did you learn to do that?" {...} I read it somewhere. In a newspaper or something. There's–there's a hint column."

Younger adults reported hearing about Internet security from the news (television) and Internet articles. As one participant explained: "I think there's a lot, I see online, just like little things, like 'don't put your password out there' and stuff, there's like a million websites on website safety and Facebook safety and things like that, {...} I'm sure I've seen it at some point".

These results suggest that media plays a significant role in informing both groups regarding online risks and how to stay safe, and therefore media could be leveraged even more to increase users' exposure to Internet security-related information.

6.6 Older and younger adults: Friends

Nineteen percent of older adults report learning about computer security strategies or risks from their friends, which was not notably different from the 25% of younger adults who reported the same. One role played by friends is to suggest safer or less expensive alternatives to current online services. One younger adult explained that they had learned to use AVG from a friend, rather than pay for antivirus software. Similarly, one older adult explained how she passes on Internet security information "you see - Bell antivirus program is free and so is Rogers. It's a complete program. It's anti-spam, anti-virus, um, you can stop pop-ups {...} I found out about it somewhere along the way and I've used it ever since, and told everybody else about it." While less frequent than lessons from family members, friends are the third most common source of security information for older adults and therefore still an important source of information.

6.7 Older and younger adults: Classroom education

Two older adults and two younger adults reported learning about computer security specifically in a classroom setting, demonstrating no notable difference between the groups. This suggests a relative lack of formal instruction in this area.

One older adult reported learning about security risks and skills to mitigate them in a basic computing course at community school, which offers informal courses on life skills or hobbies to community members. Another reported learning about it in college as part of their secretarial diploma. Further, older adults reported learning about general computer use by taking courses at work, but they were not provided with formal security instruction even in those environments. As one participant explains: "I took a course on PowerPoint for example - but in terms of safety, that's one course that was–it was never offered."

The situation is similar for younger adults; two reported learning computer security in high school, however, only one reported learning about it as part of the curriculum. One student explains hearing it informally in school: "my teachers will be like 'watch out what you put on Facebook because it always comes back' or like 'watch out for Facebook safety' and sort of things like that, but we never had any kind of like specific class on it". While privacy lessons are currently part of Ontario junior high curriculum [54], this was not the case when all but one participant was in high school.

6.8 Older and younger adults: Stories

Forty percent of older adults reported learning about computer security from stories, indicating no notable difference from 44% of younger adults who reported the same. We coded "learning from stories" when participants reported hearing and learning from tales about incidents that had happened to other people. For example, one participant explained that he learned he should change his passwords through hearing stories from others: "things I hear from people, {...} saying like 'oh yeah, my husband, someone got into his e-mail and stole his house', {...} like these huge stories which could be real or fake you know what I mean? But then it would just kind of

sink into my brain 'oh I should really change my passwords more, because I haven't changed my password in like 6 years". In these responses, participants talk about stories regarding misfortunes and attacks that had happened to other people, often known to the storyteller, and through vicarious learning, the participant now knows to avoid falling into similar traps. This provides support for the prevalence of learning from stories that Rader et al. [57] found from their survey on security stories. They reported that most people have learned lessons from stories, and this impacts their security-related decisions.

6.9 Lessons summary

This chapter addresses the third research question: What are older adults' sources of security-related information and how do they differ from younger adults'? Results indicated that almost all participants acquired their knowledge of computer security from family, the media, and friends, rather than through formal education. A significant number received Internet security related information in the form of stories, highlighting stories as an especially important medium for teaching users in both age groups about hazards. These results echo similar findings by Rader et al. [57] who also found that stories are an important tool for online security risk communication. Overall, most participants learned about computer security from multiple sources. No one source emerged as the primary vehicle for all learning, which is fitting given that learning about computer security is an ongoing process. These findings also indicate that it will be important to leverage family, media, and friends to help keep older adults safe, rather than relying on formal lessons or self-teaching.

Chapter 7

Discussion

This study was conducted with the purpose of exploring older adults' perceptions of online risks, and how their perceptions compared to those of younger users. We interviewed sixteen younger adults and fifteen older adults from three different cities regarding risks and strategies of email and social networking, and sources of Internet security information. We approached these topics with the following research questions:

R1: What are older adults' perceptions of risk in email and Facebook and how do these differ from younger adults'?

R2: What safety strategies do older adults use to stay "safe" from risks in these online activities and how are these different from younger adults'?

R3: What are older adults' sources of security-related information and how do they differ from younger adults'?

In this chapter, we discuss the results of the study in the context of older adults' outsourcing of online security issues, a topic which came up frequently throughout the interview process. This interpretation emerged from analysis of the interview data and was supported by similar findings in previously published literature [16] [32] [1] [42] [50] [58].

Later in this chapter we discuss the limitations of this study and offer recommendations based on our findings.

7.1 Interpretation

We found that older and younger adults have different perceptions of risk, different safety strategies, and different sources of information, however, these differences are

not solely due to age. Generational factors may also be at play. For example, in twenty years researchers may not see the same differences in risk perception, safety strategies, and information sources that were found in the present study. Most current older adults have become acquainted with online technology later in life than younger adults, and this likely influenced their experience with the technology and their perspectives on risk.

Age alone may still predict some amount of differences. For example, older adults may have slowed learning capability or accessibility challenges due to age-related illness [38].

This study does not attempt to identify the source(s) of differences between younger and older adults' perceptions. However, we speculate that both generational factors and factors inherent to older adults played a role.

Our results indicated that older users outsource their Internet security to third parties. These users rely on outside technical mentors and their system's antivirus software to stay safe from a variety of online risks. This reliance on third parties may leave these users more vulnerable to online threats than users who take on more personal responsibility. Our findings were similar to those found by Dourish et al. [16] who conducted a qualitative study of perceptions of security in the workplace. They determined that users delegate responsibility for security to technology or to another individual [16] whom they term a "technical friend."

Further, older adults frequently reported that their antivirus software kept them safe from a number of threats in different situations. Some reported that it kept them safe from Facebook-related hazards. After being asked if there were threats involved in using Facebook, one participant explained "yeah, there could be, with what I have I always feel very protected, {. . . }I have the Bell protection plan that I pay for by the month, and they really really keep an eye on all of that; virus protection ..and they do a scan all the time .. so I really feel comfortable." So these participants, despite knowing about some privacy threats related to Facebook, still felt safe because they had antivirus protection. Similarly, participants in Dourish et al.'s study [16] also expected that their security system would protect them from dangers for which the system was not designed.

We draw on our results of older and younger adults' perceptions of online risk, safety strategies, and lessons to explain older adults' outsourcing behaviour. We argue first that compared to their younger counterparts, older adults experienced impoverished learning contexts which may not provide them with the skills needed to make security decisions themselves. We suggest that these impoverished learning contexts led to decreased understanding and, therefore, more limited use of online safety strategies. Furthermore, older adults report a lack of understanding of online risk. These circumstances may leave older adults feeling that it is in their best interest to outsource security to a more knowledgeable third party. While this is a reasonable strategy, it could result in feeling more secure online than their less-informed behaviour warrants.

7.1.1 Impact of learning contexts

We found that very few participants, both younger and older, had learned about computer security in a formal environment; the majority having learned in a more casual context. We further noted differences between the younger and older adults' casual learning contexts that may have influenced their delegation of security behaviour. Both groups of participants reported learning about computer security from family, from friends, from the media, in the form of stories, and, for younger adults, by self-teaching. Although similar, we posit that those casual learning contexts were experienced quite differently between groups. These differing learning experiences paired with a notable difference in reported self-teaching behaviour, appear to have resulted in a more limited learning of security. We suggest that this limited learning resulted in an increased tendency to delegate security-related decisions to third parties.

Older and younger adults both reported learning computer security from family; however, "learning from family" looks quite different to individuals in different age groups. Many younger participants had grown up with computers, and were taught how to stay safe by parents, siblings, or other caregivers in the home. Some reported having supervision and consistent support from these family members, and therefore ample time to learn and to practice using various Internet-related tools and features

in relative safety.

The older adults most often reported learning about computer security from their children or spouses. In fact, it was often at their adult children's or extended family's suggestion that the older adults acquired and started using a networked computer — to stay in touch with remote family and friends. When being taught primarily by younger family members, older adults learned to send, receive, and delete email and, for some, how to post and read information on Facebook. However, given that they were taught by family members who visit rather than live with them, these teaching sessions are likely infrequent. Due to their infrequency, these sessions likely consisted of teaching only basic functions, rather than secondary functions such as security. Older adults also reported teaching themselves about computer security notably less frequently than younger adults; therefore, older adults were less likely to explore security on their own in between training sessions. Older adults who learned from spouses had more consistent help and supervision. Instruction was limited by their own interest and capacity to learn and by the extent their significant other understood and was able to teach them about Internet security. Given these circumstances, older adults received less extensive training of Internet services and safety strategies than younger adults. We contend that advanced information about online risks and safety strategies is unlikely to have been learned in any detail, and therefore leveraged by these users.

7.1.2 Limited use and understanding of safety strategies

Older adults' impoverished learning contexts result in some similar and some differing perceptions of online risk compared to younger adults. Firstly, results suggest that older adults know as much about *types* of email risks as younger adults. For example, older participants reported each type of email risk (receiving risks, sending risks, and hacking risks) with the same relative frequency as did younger adults. In comparison, Grimes et al. [32] previously found that older adults have lesser technical understanding of email risks than younger adults when tested on definitions of viruses, of spam, and how infections occur. Further, Dourish et al. [16] found that younger adults have more nuanced understanding of online security than older adults.

We contend that our findings and those of Grimes et al. [32] and Dourish et al. [16] are not contradictory, but rather complementary; taken together they indicate that older adults have similar general knowledge of *types* of risks, but have a more limited understanding of their technical details.

With their broad yet shallow understanding, older adults use Internet services to complete basic functions requiring minimal technical knowledge. Adams and Sasse [1] and Kempton [42] have also observed users functioning within a system despite imperfect knowledge of its innerworkings. Our older adults use many of the same email safety strategies as younger adults. For example, both groups consider the sender and the subject line of a suspicious email before opening it. We also saw evidence of older adults' correct decision making despite limited understanding in social networking. Older adults' reported *mindful posting* as frequently as younger adults. This functioning despite incomplete understanding occurs for most computer users; however, we argue that older adults' especially limited understanding leaves them more vulnerable than those with more detailed understanding.

Differences in safety strategies were apparent in older adults' notably less frequent use of email filtering tools and Facebook privacy settings although both are significant security features of their respective services. This demonstrates a more limited understanding of the finer nuances of online threats and security tools, and illustrates situations where limited knowledge is insufficient to allow correct decision making and secure behaviour. It is in these particular circumstances that we should be most concerned with bolstering older adults' knowledge.

7.1.3 Feelings of uncertainty

Our final reasoning for older adults' greater outsourcing of Internet security-related decisions is based on their reported uncertainty of Facebook risks and unfamiliarity with Facebook privacy settings. These older adults are aware of their lesser knowledge and consider that outsourcing to a third party may be their best option.

Several variables may impact older adults' perceived understanding of risks and privacy settings. Information regarding Facebook risks and privacy settings may simply be inaccessible for older adults. As one older adult explained "There's supposed

to be a way you could control public information versus friends but, uh, it's not obvious. It doesn't tell you. And I think that's not fair that they're not–they're not telling me. You have to know what you're doing before you go on it. I don't know what I'm doing." This inaccessibility may be due to language, symbols, or interaction mechanisms that are not intuitive for older adults. The interfaces are not designed for elderly users, who have different needs than younger ones [2]. Further, older adults are not the only users who find Facebook settings difficult to use. In their 2012 report on "Privacy management on social media", Pew [50] found that "Half of social networking website users reported they have some difficulty managing privacy controls". Given these challenges, it is little wonder older adults feel uncertain about Facebook risks and do not use its privacy controls.

Older adults have only one Facebook security strategy, further illustrating their avoidance of security decisions. Older adults avoid individual security decisions by being mindful about what they post online. They believe that if they post minimal information on Facebook, then there is little reason to take extra precautions. They avoid putting themselves in a position where they would be faced with decisions that they are ill-equipped to handle.

Previous work by Rainie et al. [58] had adult computer users identify previously used behaviours from a list of online anonymity enhancing behaviours. They found that adults 65 and over did much less to protect themselves than all other age groups, particularly in regards to editing or deleting things previously posted on social networks. This may be due to older adults' less frequent posting, but may also be due to a limited understanding of the risks. Ignoring Facebook settings comes at a cost. A number of older adults posted pictures of their family and friends on Facebook, yet did not worry about the potential risks. However, without using privacy settings, these pictures are publicly available.

Literature on decision making may also shed light on the relationship between older adults' uncertainty of risk and outsourcing of decision making. Botti and McGill [8] explain that "[d]elegating decision making could improve (peoples') subjective well-being by relieving them of the responsibility of unwanted decision consequences and subsequent regret". Older adults' uncertainty causes them to feel at greater risk for

making a wrong security decision, therefore outsourcing of these decisions provides relief from the worry of making incorrect choices, having to deal with the consequences thereof, and the associated negative feelings.

7.1.4 Summary of interpretation

Our results show that older adults are more likely than younger adults to delegate their Internet security to antivirus technologies and technical mentors. Delegating Internet security to third parties may still leave users vulnerable because they attribute more protective qualities to these third parties than they may actually deliver. For example, as Dourish et al. [16] found, "a technology deployed to solve one problem may be mistakenly interpreted as providing protection against (an)other ''. We conclude that, although helpful, minimal posting to Facebook and outsourcing of security are insufficient to keep one safe from online dangers. We suggest that more be done to encourage, support, and enable older adult users to better understand risks, safety strategies and service tools.

7.2 Limitations

As with any study, a number of design trade-offs were necessary. Although we tried to reach participants with a wide range of backgrounds, self-selection is a concern because participants who are most interested in technology and security, and most experienced, are the most likely to want to participate in an interview on the topic. Additionally, the sample size was small (although similar to other published studies of similar scope) and therefore any conclusions drawn from this sample needs to be confirmed through a follow-up study. Interviews rely on participants to report their own behaviours [14], and whether these reports are accurate or complete cannot be known. This is a common problem in qualitative data gathering and, as such, data is not treated as absolute; it reflects participants' perception of their behaviour.

Participants responded to interview questions according to their definitions of "risk", "safe", and "computer security". This was encouraged to find out more regarding how they conceptualized each of these terms and to avoid imposing a definition which may have limited participants' responses. However, it is more challenging

to compare responses when different perceptions of "risk" are used. For example, one participant defined risk to mean "inconvenience" and therefore considered spam to be a risk, while other participants may not have.

Although frequently used in research, some academics argue that qualitative interviews are flawed in that they do not treat the interview as an interaction and therefore meaningful context is lost [56]. They also note that the delivery and structure of interview questions can be indicative of a particular research agenda. To address these concerns, the researcher made an effort to speak only when reassuring the participant that they were heard, and when summarizing responses to ensure complete understanding. However, at times it was necessary to draw out opinions and understandings from participants. For example, when people claimed they could not remember where they had learned about computer security the researcher provided prompts such as "in a class, or from a friend?" to clarify the type of information we were seeking. In this case, we wanted the source of the information instead of the geographic location of "where" they had learned about computing and computer security.

7.3 Recommendations

Based on our results, we provide the following recommendations to augment older adults' understanding of online security and ease their learning curve as they continue to take advantage of new and existing technologies.

Design services and features for safer use: We suggest that services such as Facebook should be designed with users' security in mind. For example, default privacy settings on Facebook could be set to maintain privacy until they are changed, rather than set low and allow users' posts to be viewed publicly. Privacy settings could also be redesigned to be more accessible for all users, leveraging increased visibility, more accessible language, easy to access definitions for necessary complex terms, and simplified interaction mechanisms. We realize this would necessitate realignment of Facebook's business practices, however any steps in this direction would be viewed favourably by the general public and by privacy advocates.

Leverage media to educate older adults: Media was one of the most frequently reported sources of online security information. This suggests that Internet, radio, television, and print media can and should be further leveraged to communicate with users of all ages regarding Internet-related hazards. Further, specific media can tailor information to their target audiences. For example, newspapers are accessed more often by older adults. These could present a regular Internet security hint column to which readers could write in and have their questions addressed. This leverages a communication model that is already familiar to older adults; newspaper advice columns have a long history. Further, readers could cut out and save the column in a physical location to reference when needed. Along a similar vein, a television news segment dedicated to informing users of Internet risks and safety tips may greatly impact users' computer security knowledge.

Use stories to teach older adults: Information disseminated by the media is often portrayed in the form of stories, a powerful communication format [6]. It can be used to highlight dangers, the importance of risk awareness [57], and the resulting significance of taking steps to protect against risk. We therefore recommend framing security lessons as stories. Benefits from framing security lessons in a story format, such as a security breach that happened to a relatable character, results in increased memorability of these security lessons [6]. This may then leave users better equipped and motivated to behave securely than before hearing the story.

Train specialized technical helpers: Our results also highlighted a need for reliable technical helpers to assist older users who are struggling to learn how to use a computer or who are having problems with their computers. We recommend implementing a service that provides this type of support. These technical helpers, trained in computing and in teaching older adults, would come to the client's home to help and to teach inexperienced computer users. Users' would receive more accessible and more customized support than traditional customer service. One user spoke about learning to use the computer at a library, but then going home and not recognizing things because she used a different system. This participant spoke further about having called customer service for help but not understanding what the technician

was trying to explain. We envision that this service could be a viable business option for computer experts who are looking for additional income and are interested in helping older adult users in the community. It might also be offered on a volunteer basis by community organizations.

7.4 Future work

The next step in the research is to analyze our remaining data to determine prominent themes on other topics and compare responses from older and younger adults. From a brief preliminary exploration, we expect interesting differences in the areas of reported confidence, knowledge of computer assets, and perceptions of attackers.

The data analyzed in this thesis revealed several related questions that should be addressed in future work. These will provide a more complete understanding of how usable security communication should be tailored for older adults, and potentially provide insight into accessible and secure systems design.

Future research should look into the impact of security stories on users' mental models of online risk. In particular, it would be interesting to determine the kinds of stories that are most impactful, the traits of a compelling storyteller, and the components of effective stories.

Our results offer insight into older adult's behaviour and understanding with respect to online security. However, additional studies should look beyond self-reported data and measure actual practice. Furthermore, the actual effectiveness of security-related programs, security campaigns, and paid help should be assessed to determine their efficacy for older adults. A potential project to assess this could involve monitoring users' security practices over a period of time, providing Internet security training to the users, and then observing to assess the impact of the training.

Finally, continued research on older adults' use of social media should be completed with a larger sample size. Our small sample revealed interesting usage patterns that should be further explored. Usability issues related to privacy settings should also be addressed, including their ease of use, efficiency, and trustworthiness. Our results demonstrated that they are not accessible or usable for older adults, and this should be remedied.

7.5 Contributions

This was the first study comparing older and younger adults' perceptions of online risks, safety strategies, and methods of learning. Our results provide useful information relating to these age groups, the older adults in particular, and relate it to previous research on mental models and perceptions of risk.

To our knowledge, this was the first study to provide insight into users' sources of Internet security information. We found that our older and younger adults learned about computer security from media, family, and friends most frequently. We also confirmed findings by Rader et al. [57] regarding hearing about computer security in the form of stories.

The study provided details regarding which hazards and safety strategies need to be more clearly conveyed to the older user community. These include explaining risks associated with posting photos publicly and emphasizing the use of email filtering tools and Facebook privacy settings.

To our knowledge, this study is the first to have older participants discuss their own perceptions of risk. Whereas related research [32] [45] [58] provided participants with a list of risks to discuss, the present study used no preconceived definition of risks. Participants spoke about their own conception of risks - our results therefore represent the threats and strategies most familiar to participants. Our approach also minimized prompting to avoid influencing users' mental models and we believe that this resulted in more realistic and representative results than alternative methods.

7.6 Conclusion

This thesis explored the following research questions:

R1: What are older adults' perceptions of risk in email and Facebook and how do these differ from younger adults'?

R2: What safety strategies do older adults use to stay "safe" from risks in these online activities and how are these different from younger adults'?

R3: What are older adults' sources of security-related information and how do they differ from younger adults'?

Our results indicated that older adults demonstrated roughly the same knowledge of types of email risks as younger adults, but demonstrated and expressed less understanding of Facebook risks. In response to the second research question, we found that older adults employed fewer strategies to stay safe from risks in both email and Facebook. Older adults also reported feeling uncertain regarding risks of using Facebook, and at the same time, not feeling at personal risk using the service. Older adults were less likely to apply Facebook privacy settings or take advantage of email tools to filter or block unwanted emails. Older adults also relied more often on antivirus software and technical helpers. Finally, in regards to the third research question, older adults reported receiving information from almost all of the same sources as younger adults: family, media, and friends; the one notable difference being the infrequency of self-teaching by older adults. In conclusion, Internet security tools are the same for both younger and older users, regardless of demographic. It is untenable for non-expert older adults to understand risk and safety strategies given the current education and resources provided. Even in outsourcing security to third parties these older adults remain at increased risk. There is need, therefore, for accessible security features, education, and communication efforts that empower older adults to better protect themselves online.

Bibliography

[1] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[2] Silvana Maria Affonso de Lara, Willian Massami Watanabe, Eduardo Pezutti Beletato dos Santos, and Renata PM Fortes. Improving wcag for elderly web accessibility. In *Proceedings of the 28th ACM International Conference on Design of Communication*, pages 175–182. ACM, 2010.

[3] Mary K Allen. Consumption of culture by older canadians on the Internet. Technical report, Statistics Canada, 2013.

[4] Jeffrey Jensen Arnett. Emerging adulthood: A theory of development from the late teens through the twenties. *American psychologist*, 55(5):469, 2000.

[5] John Aycock. *Computer viruses and malware*, volume 22. Springer, 2006.

[6] Roy F Baumeister, Liqing Zhang, and Kathleen D Vohs. Gossip as cultural learning. *Review of General Psychology*, 8(2):111, 2004.

[7] Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. The socialbot network: when bots socialize for fame and money. In *Proceedings of the 27th Annual Computer Security Applications Conference*, pages 93–102. ACM, 2011.

[8] Simona Botti and Sheena S Iyengar. The dark side of choice: When choice impairs social welfare. *Journal of Public Policy & Marketing*, 25(1):24–38, 2006.

[9] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[10] L Jean Camp. Mental models of privacy and security. *Technology and Society Magazine, IEEE*, 28(3):37–46, 2009.

[11] Canadian Anti-Fraud Centre. Canadian anti-fraud centre - senior busters program. `http://www.antifraudcentre-centreantifraude.ca/english/cafc_seniorbusters.html`, 2007.

[12] Charlie C Chen, RS Shaw, and Samuel C Yang. Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. *Information Technology Learning and Performance Journal*, 24(1):1, 2006.

[13] Sonia Chiasson, Manas Modi, and Robert Biddle. Auction hero: The design of a game to learn and teach about computer security. In *World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education*, pages 2201–2206, 2011.

[14] John W Creswell. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications, Incorporated, 2013.

[15] Rachna Dhamija, J Doug Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 581–590. ACM, 2006.

[16] Paul Dourish, Rebecca E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6):391–401, 2004.

[17] Julie S Downs, Mandy Holbrook, and Lorrie Faith Cranor. Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, pages 37–44. ACM, 2007.

[18] Julie S Downs, Mandy B Holbrook, and Lorrie Faith Cranor. Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security*, pages 79–90. ACM, 2006.

[19] Manuel Egele, Andreas Moser, Christopher Kruegel, and Engin Kirda. Pox: Protecting users from malicious facebook applications. *Computer Communications*, 35(12):1507–1515, 2012.

[20] Serge Egelman. *Trust me: Design patterns for constructing trustworthy trust indicators*. ProQuest, 2009.

[21] EMC Corporation. The year in phishing. Technical report, EMC Corporation, 2013.

[22] Facebook. Newsroom-key facts. `http://newsroom.fb.com/Key-Facts`, 2013.

[23] Andy Field. *Discovering statistics using SPSS*. Sage publications, 2009.

[24] Baruch Fischhoff, Paul Slovic, and Sarah Lichtenstein. Fault trees: Sensitivity of estimated failure probabilities to problem representation. *Journal of Experimental Psychology: Human Perception and Performance*, 4(2):330, 1978.

[25] Maria Foverskov and Thomas Binder. Super dots: making social media tangible for senior citizens. In *Proceedings of the 2011 Conference on Designing Pleasurable Products and Interfaces*, page 65. ACM, 2011.

[26] Susannah Fox. *Older Americans and the Internet*. Pew internet & American life project, 2004.

[27] Hongyu Gao, Jun Hu, Tuo Huang, Jingnan Wang, and Yan Chen. Security issues in online social networks. *Internet Computing, IEEE*, 15(4):56–63, 2011.

[28] Vaibhav Garg and Jean Camp. End user perception of online risk under uncertainty. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 3278–3287. IEEE, 2012.

[29] Vindu Goel. Malicious software poses as video from a facebook friend. `http://bits.blogs.nytimes.com/2013/08/26/malicious-software-poses-as-video-from-a-facebook-friend/?_r=0`, 2013.

[30] Google. How you can stay safe and secure online. `http://www.google.ca/goodtoknow/online-safety/`, 2013.

[31] Steven J Greenwald, Kenneth G Olthoff, Victor Raskin, and Willibald Ruch. The user non-acceptance paradigm: Infosec's dirty little secret. In *Proceedings of the 2004 workshop on New security paradigms*, pages 35–43. ACM, 2004.

[32] Galen A Grimes, Michelle G Hough, Elizabeth Mazur, and Margaret L Signorella. Older adults' knowledge of Internet hazards. *Educational Gerontology*, 36(3):173–192, 2010.

[33] Galen A Grimes, Michelle G Hough, and Margaret L Signorella. Email end users and spam: Relations of gender and age group to attitudes and actions. *Computers in Human Behavior*, 23(1):318–332, 2007.

[34] Greg Guest, Kathleen M MacQueen, and Emily E Namey. *Applied thematic analysis*. Sage, 2011.

[35] Anil Gurung, Xin Luo, and Qinyu Liao. Consumer motivations in taking action against spyware: An empirical investigation. *Information Management & Computer Security*, 17(3):276–289, 2009.

[36] Cormac 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*, pages 133–144. ACM, 2009.

[37] Rebecca Hill, Paul Beynon-Davies, and Michael D Williams. Older people and Internet engagement: Acknowledging social moderators of Internet adoption, access and use. *Information Technology & People*, 21(3):244–266, 2008.

[38] Scott M Hofer and Duane F Alwin. *Handbook of cognitive aging: Interdisciplinary perspectives*. Sage, 2008.

[39] Chris Hoofnagle, Jennifer King, Su Li, and Joseph Turow. How different are young adults from older adults when it comes to information privacy attitudes and policies? *Available at SSRN 1589864*, 2010.

[40] Daniel Kahneman, Paul Slovic, and Amos Tversky. *Judgment under uncertainty: Heuristics and biases*. Cambridge University Press, 1982.

[41] Michaela Kauer, Sebastian Günther, Daniel Storck, and Melanie Volkamer. A comparison of american and german folk models of home computer security. In *Human Aspects of Information Security, Privacy, and Trust*, pages 100–109. Springer, 2013.

[42] Willett Kempton. Two theories of home heat control. *Cognitive Science*, 10(1):75–90, 1986.

[43] Won Kim, Ok-Ran Jeong, Chulyun Kim, and Jungmin So. The dark side of the Internet: Attacks, costs and responses. *Information systems*, 36(3):675–705, 2011.

[44] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research methods in human-computer interaction*. Wiley. com, 2010.

[45] Daniel LeBlanc and Robert Biddle. Risk perception of Internet-related activities. In *Privacy, Security and Trust (PST), 2012 Tenth Annual International Conference on*, pages 88–95. IEEE, 2012.

[46] Younghwa Lee and Kenneth A Kozar. Investigating factors affecting the adoption of anti-spyware systems. *Communications of the ACM*, 48(8):72–77, 2005.

[47] Rebecca LeFebvre. The human element in cyber security: A study on student motivation to act. In *Proceedings of the 2012 Information Security Curriculum Development Conference*, pages 1–8. ACM, 2012.

[48] Albert Levi and Çetin Kaya Koç. Risks in email security. *Commun. ACM*, 44(8):112, 2001.

[49] Eli Lieber and Thomas S. Weisner. Dedoose. `http://www.dedoose.com/Discover/l`, last accessed 2013.

[50] Mary Madden. Privacy management on social media sites. Technical report, Pew Internet & American Life Project, 2012.

[51] Adriana M Manago, Tamara Taylor, and Patricia M Greenfield. Me and my 400 friends: The anatomy of college students' facebook networks, their communication patterns, and well-being. *Developmental psychology*, 48(2):369, 2012.

[52] Margaret W Matlin. *Cognition - Sixth edition*. NJ: Wiley, 2005.

[53] Janice M Morse. Determining sample size. *Qualitative Health Research*, 10(1):3–5, 2000.

[54] Ontario Ministry of Education. The Ontario curriculum grades 1-8 health and physical education. Technical report, Government of Ontario, 2010.

[55] Pilar Olivares. Facebook users risk identity theft. `http://rt.com/usa/facebook-users-risk-identity-theft-575/`, 2013.

[56] Jonathan Potter and Alexa Hepburn. Qualitative interviews in psychology: Problems and possibilities. *Qualitative research in Psychology*, 2(4):281–307, 2005.

[57] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, page 6. ACM, 2012.

[58] Lee Rainie, Sara Kiesler, Ruogu Kang, and Mary Madden. Anonymity, privacy, and security online. Pew Internet & American Life Project, September 5, at `http://pewinternet.org/Reports/2013/Anonymity-online.aspx`, 2013.

[59] Facebook security team. Security on facebook. `https://www.facebook.com/about/security`, 2014.

[60] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 88–99. ACM, 2007.

[61] Supriya Singh, Anuja Cabraal, and Gabriele Hermansson. What is your husband's name? sociological dimensions of Internet banking authentication. In *Proceedings of the 18th Australia conference on Computer-Human Interaction: Design: Activities, Artefacts and Environments*, pages 237–244. ACM, 2006.

[62] Paul Slovic. *The perception of risk.* Earthscan Publications, 2000.

[63] Frank Stajano and Paul Wilson. Understanding scam victims: Seven principles for systems security. *Communications of the ACM*, 54(3):70–75, 2011.

[64] Chauncey Starr. Social benefit versus technological risk. what is our society willing to pay for safety? *Science*, 1969.

[65] Emily Steel and Geoffrey A. Fowler. Facebook in privacy breach. `http://online.wsj.com/news/articles/SB10001424052702304772804575558484075236968`, 2010.

[66] Anselm L Strauss, Juliet Corbin, et al. *Basics of qualitative research*, volume 15. Sage publications Newbury Park, CA, 1990.

[67] Tim Thornburgh. Social engineering: The dark art. In *Proceedings of the 1st annual conference on Information security curriculum development*, pages 133–135. ACM, 2004.

[68] Melanie Volkamer and Karen Renaud. Mental models a general introduction and review of their application to human-centred security. In Marc Fischlin and Stefan Katzenbeisser, editors, *Number Theory and Cryptography*, volume 8260 of *Lecture Notes in Computer Science*, pages 255–280. Springer Berlin Heidelberg, 2013.

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

[70] Yue Zhang, Serge Egelman, Lorrie Cranor, and Jason Hong. Phinding phish: Evaluating anti-phishing tools. In *14th Annual Network and Distributed System Security Symposium*. ISOC, 2007.

[71] Kathryn Zickuhr and Mary Madden. Older adults and Internet use. Pew Internet & American Life Project, June 6, 2012, at `http://pewinternet.org/Reports/2012/Older-adults-and-internet-use.aspx`, 2012.

Appendix A

Consent form

Carleton UNIVERSITY
Canada's Capital University

Informed Consent Form

Comparison of Risk Awareness and Security Behaviours in Younger and Older Adults

This project was reviewed and received ethics clearance by the Carleton University Research Ethics Board on Date of ethics clearance: Ethics Clearance expires on May 31st, 2014.

The interview component of this study will assess participants' awareness of Internet threats and security behaviours. The goal is to determine 1. what our participants know in regards to internet threats and 2. what they do to protect themselves. This research is being conducted as part of a Master's student's thesis. Final results will inform researchers of any gaps or differences in these areas and may inform both future Internet security education initiatives and computer security software design.

As a participant, you will be asked a number of questions regarding Internet threats and security behaviours. If it's easier for you to answer the questions while you are sitting at or using the computer you are welcome to do so, however I will not be touching your computer or specifically asking you to show me anything.

The session will take approximately one hour and your interview will be recorded using a digital audio recorder. Data collected during your session will be associated with an anonymous username that has no connection with any personally identifiable data. Only researchers directly involved in the research will have access to the study data. Digital audio recordings will be erased from disk by April 31st, 2013. Since this work is part of a larger research project, transcriptions of the interviews may be kept for future research. Transcribed data will be stored in on a secure server in the United States for up two years and is subject to the Patriot Act. (See http://www.dedoose.com/Public/Terms.aspx for more information). The data will only be used for these purposes.

There are no known risks involved in these interviews, however, you may decline to answer any questions, end the interview at any time, or withdraw from the study and have your data destroyed any time before April 31st 2013. As a participant in this study you may benefit from asking questions and gaining additional knowledge at the end of the session regarding Internet risks and behaviours that may improve online security. At the end of the interview you will be compensated $20 in cash for your time in participating in this session, even if you withdraw from the study.
As a study participant, you may choose to be notified when the results of this study are published. If you wish to be notified, please include your email

address below.

_____ I wish to be notified when the results of this study are published. Please contact me at this email address:
_____

_____ I do not wish to be notified when the results of this study are published.

Study Contact Information

Vanessa Boothroyd Principal Investigator Carleton University Vanessa_Boothroyd@carleton.ca 613-983-8932	Dr. Sonia Chiasson Faculty Supervisor Carleton University Chiasson@scs.carleton.ca (613) 520-2600 ext 1656

This research has been reviewed and cleared by the Carleton University Research Ethics Board

Ethics Contact Information

Professor Antonio Gualtieri, Chair Research Ethics Board Carleton University Research Office 613-520-2517 ethics@carleton.ca

I, _____ volunteer to participate in this study on Internet risk awareness and security behaviours.

_____ _____
Signature of participant Date

_____ _____
Signature of researcher Date

Appendix B

Demographics questionnaire

Demographics Questionnaire

1) Which gender do you primarily identify with? M/F/Other

2) Do you use a computer to access the Internet at least once a month? Yes/No

3) If yes, do you use your computer:

   a) 1 to 5 hours
   b) 6 to 10 hours
   c) 11 to 20 hours
   d) 21 to 30 hours
   e) More than 31 hours

4) Have you taken a course or received formal training in computer security? Yes/No. If yes, can you tell me about it?

5) Rate yourself on this scale regarding computer help:

"I often ask for help"	1	2	3	4	5	"Others often ask me for help"

6) Have you ever done any programming? Yes/No
   a) If yes, in which languages?

7) Do you have a degree in an IT-related field (e.g. computer science, electrical engineering, etc.)? Yes/No

8) Year you were born: _____

9) Highest level of education attained

a. Some grade school
b. High school diploma
c. Some university
d. Bachelor's degree
e. Some professional school
f. Professional degree
g. Some graduate school
h. Graduate degree

10) What is/was your occupation?

11) What type of computer do you use?
a. PC
b. Mac
c. Other

Appendix C

Interview questions

Interview Questions – Risk, threats and security

Confidence

1) On a scale of 1-10, 1 being not at all confident and 10 being completely confident, how confident are you that you know how to keep your computer safe?

Computer Behaviours

2) Do you use the Internet for:
   a) E-mail? Yes/No
   b) Online Banking? Yes/No
   c) Browsing for health information? Yes/No
   d) Shopping? Yes/No
   e) Social Networking? Yes/No

   Other: youtube

Risk

3) Are there risks involved in:
   a) Using Email?
      i) Y/N
      ii) If Y, What are they? Wrong person, hack
         (1) Example: Fraud e-mails or phishing attacks
   b) Online Banking?
      i) Y/N
      ii) If Y, what are they? Hacking into your banking information – tv news/documentary
         (1) Example: Fake banking websites, password guessing attacks
   c) Browsing for health information?
      i) Y/N
      ii) If Y, what are they? Invalid/incorrect information – goes to gov health websites
         (1) Example: Inaccurate information or privacy concerns
   d) Online Shopping?
      i) Y/N
      ii) If Y, what are they?
         (1) Example: Dishonest shops, unsecure payment transactions
   e) Social Networking?
      i) Y/N
      ii) If Y what are they?
         (1) Privacy violations

(2) More probing questions: photos

Strategies

4) Given those risks you just identified, do you have any strategies to stay safe when you:
   a) Email?
      i) Example: What do you do when you receive an e-mail from someone you don't know? What do you do when you receive an e-mail from a family member?
   b) Online Banking?
      i) Example: Do you type the website address directly?
   c) Searching for and finding health information?
      i) Example: Do you check more than one website to verify the information?
   d) Shop?
      i) Example: Do you look for https when you're paying?
   e) Social Network?
      i) Only post information that you are willing to make completely public?

Follow up?

Knowledge of Assets

5) If an attacker were to break in to your computer, what do you think they would do or want?
   a) (If they talk about different types of "attacker" – ask them what each "attacker" would want)

6) Of those assets that could be stolen, can you prioritize which you think is the most valuable to which is the least valuable?

7) What do you think could be done with this information?

Lessons

8) Where did you learn about computing and computer security? Example: Work, Friends, School, Family.
   a) What did they teach you?
   b) Where did they learn what they know?

9) Have you or someone you know ever had any computer security problems? For example: got a virus, had an account broken into?

   a) How did _ know there was a breach?
   b) What did they do to fix the problem?

c) Did you learn from that breach? If so, what did you learn?

10) If a friend of yours just got a new computer and came to you for advice about protecting their computer – what would you tell them?

Prevention and Treatment

11) Can you think of any way we, as researchers, can help computer users better protect themselves against "attackers"?

12) A) Do you use an antivirus program? Y/N
b) If Yes, do you pay for the antivirus program?
c) What do you think the antivirus program does?
d) Do you think it does enough to keep you protected?
e) Can you think of any way the antivirus program could be improved?

13) If you were to find out you had a virus on your computer; what would you do about it?
14) What do you think about "attackers"?
a) Main goals, motivation, who are they?
15) On a scale of 1-10, how confident are you that you can keep your computer safe?

Experience

16) Can you please explain what is meant by the term "phishing"?

17) What do you think a computer virus can do?

Conclusion

18. Is there anything you would like to add?

19. How did the interview go for you?

20. Do you have any questions for me?
21. Can you think of any questions that I could have asked but didn't?