

# Improving Older Adults' Online Security: An Exercise in Participatory Design

Cosmin Munteanu<sup>1,2</sup>  
cosmin@taglab.ca

Calvin Tennakoon<sup>3</sup>  
calvin.tennakoon@mail.utoronto.ca

Jillian Garner<sup>3</sup>  
jillian.garner@mail.utoronto.ca

Alex Goel<sup>3</sup>  
alex.goel@mail.utoronto.ca

Mabel Ho<sup>3</sup>  
mabel.ho@mail.utoronto.ca

Clare Shen<sup>3</sup>  
clare.shen@mail.utoronto.ca

Richard Windeyer<sup>3</sup>  
r.windeyer@mail.utoronto.ca

<sup>1</sup>)Technologies for Aging Gracefully  
Department of Computer Science  
University of Toronto

<sup>2</sup>)Institute for Communication, Culture,  
Information, and Technology  
University of Toronto Mississauga

<sup>3</sup>)Faculty of Information Studies  
University of Toronto

## ABSTRACT

Older adults (65+) are often considered to be technologically less savvy than the average population, particularly with respect to using online applications [4]. This can have negative consequences for their financial, health, and well being, by hindering their access to resources such as online banking, relevant health information, and connections with family members and friends. The 2011 Census [7] indicate that 66% of such adults are daily Internet users; as such, it is important to also protect older adults' online safety and privacy – especially since seniors are a significant target of Internet scams or email phishing attacks. Solutions have been proposed to address this significant problem; however, these are not widely reaching – just in one year alone, older Canadian adults have lost an estimated \$10 million to Internet scams [2]. Moreover, there is very little understanding of why seniors are disproportionately falling victim to online threats, despite the availability of various technologies that block such threats (e.g. browser add-ons). For this, we have begun studying the technological and non-technological barriers to the adoption of digital security technologies by older Internet users, and exploring design changes that increase their adoption. This paper presents a preliminary investigation of a participatory design approach to developing adoptable and usable online security interfaces for older adults.

## 1. INTRODUCTION

Several statistics in Canada [7] or the United States [6] indicate that older adults are users of a wide range of online services. However, as pointed out by research such as [4], older adults are more vulnerable to online threats than younger users. Unfortunately, very little research exists that aims to understand the root causes leading to such vulnerabilities, particularly from a multidisciplinary perspective that looks at the interplay between social and economical factors, information practices, attitudes toward technology, and usability of safety features. One notable exception is [1], whose ground-breaking fieldwork revealed that older adults are generally aware of the dangers of privacy and security breaches, and that their main sources of education are media and friends/family. This is consistent with research showing that fears of privacy and online security are among the factors that hinder Internet adoption by seniors [5].

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

Symposium on Usable Privacy and Security (SOUPS) 2015, July 22-24, 2015, Ottawa, Canada.

Boothroyd's research [1] was limited to email and Facebook, and some of the findings invite further research – such as understanding older adults' lack of appropriate strategies to deal with online threats, particularly in the context of general online activities, not specific to a certain service. In order to gain such an understanding, we have begun investigating if (and how) widely-available security features such as browser add-ons are used by older adults to enhance their online safety. In this paper we briefly report on the very preliminary findings arising from this study.

## 2. STUDY GOALS

From a technology perspective, numerous tools exist (widely and freely available) that greatly enhance online security – such as the very effective browser add-ons (e.g. Adblock, NoScript, Ghostery, Web-of-Trust) which work by blocking the main channels that are often exploited by security threats, by “blacklisting” websites that are known threats, or simply by filtering out parts of a website that may compromise a users' privacy. However, there seems to be little evidence in studies of older adults' online risks [3] of the adoption of such tools as a more universal instrument for mitigating the risks of online threats. This is unsurprising, since, as shown by Boothroyd [1], older adults rely on sources such as popular media for their education about Internet safety. We therefore proposed to answer the following research questions:

*Q1: What are the information practices employed by older online users that make them particularly vulnerable to security threats?*

*Q2: What are the factors affecting the adoption of existing solutions designed for preventing online scams and attacks?*

*Q3: What is the best form of cybersecurity protection for older adults? This includes browser add-ons specifically designed for seniors, easy access to educational resources (such as websites), or a combination of both?*

The above questions frame our overall research goals. This paper presents the findings from our pilot study that sought to provide a preliminary insight into the design and technology adoption challenges pertinent to improving older adults' cybersecurity. Our pilot study was carried out in two phases, using different methodologies: a guided interview phase and a participatory design phase.

## 3. INTERVIEWS

The aim of the interviews was to gain an early insight into why seniors are not currently adopting the cybersecurity tools and techniques available, and to inform the setup of the subsequent

participatory design phase. The guided interviews were administered in the form of semi-structured questionnaires and open-ended discussions. Three participants were recruited (all males, retired), as described in Table 1.

Participant	Mr. A	Mr. B	Mr. C
Age	84	84	71
Education	High school	University	College
Status	Middle class	Middle class	Middle class
Career	Railway Supervisor	Chemical Engineer	Finances
Internet use	Mostly for email and online shopping	Mostly for email with friends and family)	Active, but avoids shopping and banking
Tech knowledge	Took online workshops ten years ago	Limited	Aware of (some) security risks
Online time	1-2 hours a week	Only a couple hours a week	Several hours daily

The interviews were conducted in the participants' homes and lasted about 1 ½ hours each. Beside direct and open-ended questions, researchers also asked participants to exemplify their answers by executing the tasks they were describing (e.g. checking email or accessing a website).

Through this interviews we have discovered that our participants were largely not knowledgeable of online security threats – keywords such as “virus” or “phishing” were mostly unfamiliar. Only Mr. C was moderately aware of these, through an identity theft prevention workshop he attended; however, his online prevention strategy consists of completely avoiding certain activities such as shopping. One of the most salient observation was that our participants preferred to be taught about cybersecurity by their family members and/or caregivers instead of on their own, and that in general even basic security precautions such as keeping software updated was a struggle. Moreover, one participant (Mr. A) described the difficulties in typing and general UI navigation due to his limited dexterity, which has prompted his grandchildren to help him with general IT support – as such he relies on them to protect him from “problems on the internet” although he does not know what these may be. This was similar to Mr. B's assertion that he would like to easily find out if a website is “good or bad”.

#### 4. PARTICIPATORY DESIGN

The observations from our interviews (particularly Mr. A and Mr. B) have prompted us to conduct a short participatory design session investigating what solutions work better for improving seniors' cybersecurity. These sessions aimed to deepen our understanding of the required design criteria for such solutions. For this, we have developed a prototype of an online reference resource that could be easily accessed by seniors based on their security needs. The resource provides comprehensive information and solutions for each problem by linking to external relevant websites – users can select what specific problem they have (e.g. Skype, Email), solicit help through an online form, or contribute feedback. The design was iteratively refined after individual sessions with each participant. The sessions were conducted with Mr. B and Mr. C, as well as with one new tech-savvy participant (Mr. D, aged 72, a former instructor of general computer use and

programming at a local community college, and very frequent Internet user). Sessions started with participants providing info on problems encountered while online, clustering it on post-it notes, and using these to reflect on, suggest, and iteratively sketch revisions to the online resource prototype.

One of the key findings was that participants are familiar with specific services that may use (e.g. Skype, Google) but not with their more abstract description (e.g. VoIP, search engine). This has been reflected in the redesign of the resource prototype, where users can explicitly select the name of the service with which they have problems – an important consideration for any web-based security assistance service aimed at seniors. Due to the lo-fi status of our prototype, most of the feedback received was less aimed at design revisions and more focused on information practices. We have found out that most of our participants prefer to receive support and learn from peers or family members. Mr. D even exemplified this by phone-calling a friend from whom he received a suspicious email in order to verify the authenticity of the sender. This highlights the need for any solution to be designed for social use. We have also observed that our participants were very diligent in reading any on-screen information in its entirety, which suggests that on-line educational resources can be designed to be rather extensive.

#### 5. CONCLUSIONS AND NEXT STEPS

In this paper we presented a preliminary investigation of the technology adoption challenges faced by older adults with respect to improving their online safety. We have employed semi-structured interviews and a participatory design approach to gaining a first insight into such challenges.

The findings of this preliminary study suggest that seniors are largely not knowledgeable of online security threats beyond occasional awareness of some of the most common ones. Consequently, they do not employ any technology-based solutions to reduce the risks of such threats. We have also found that any web-based solution must be designed with consideration of its users' lack of familiarity with technical terms, preference for receiving assistance from their social network, and need to provide learning resources. Our immediate future work aims to more rigorously investigate the root causes behind the low uptake of online security features among older adults, as well as of the technological and digital literacy challenges faced by older adults in safely accessing Internet resources. Subsequent research will employ participatory design to explore solutions that will empower users to control their own safety online.

#### 6. REFERENCES

- [1] Boothroyd, V. (2014). Older Adults' Perceptions of Online Risk. Master of Arts Thesis, Carleton University. May 2014.
- [2] CFAC (2013). The Canadian Anti-Fraud Centre Criminal Intelligence Analytical Unit Annual Report.
- [3] Garg, V., et al. (2011). Designing Risk Communication for Older Adults. In Symposium on Usable Privacy and Security
- [4] Grimes, G.A. et al (2010). Older Adults' Knowledge of Internet Hazards. In J of Educational Gerontology. 36 (3).
- [5] Neves, B.B., et al. (2013) Coming of (old) age in the digital age. In J of Sociological Research Online 18, 2.
- [6] Smith, A. (2014). Cell Phones, Social Media and Campaign. Pew Research Center Survey, November 2014.
- [7] Statistics Canada 2011 Census of Population.