CREATING COMPUTER CONFIDENCE : AN INVESTIGATION INTO CURRENT PRIVACY AND SECURITY CONCERNS OF THE SENIOR DEMOGRAPHIC

Caroline Hillier

Department of Computer Science, University of Guelph, Ontario, Canada

ABSTRACT

The senior demographic has been neglected as technology rapidly develops. The COVID-19 pandemic has escalated technological integration into daily activities. Because of this rapid change there is a pertinent need to ensure that elders have the necessary technological literacy. Previous research showed that elders are not shying away from Internet use but are lacking in willingness to adapt to new methods. This research aims to identify the current knowledge gaps of the senior demographic and propose solutions to those problem areas. This project utilizes a survey to get direct feedback from the target demographic. The results identified specific knowledge gaps, which can be generalized to a lack of awareness of available resources. These observations were used to formulate a list of tools and resources that elders can take advantage of to become more confident on the Internet, and ultimately have the best experience.

KEYWORDS

Security management, Technology education, Senior demographic, Internet Safety, COVID-19.

1. INTRODUCTION

Members of the senior demographic often hesitate to integrate technology into their daily lives. While this demographic is often familiar with device functions such as making phone calls, they are often found missing out on the valuable capabilities that devices can offer [1]. Most devices have capabilities to track medications, request goods and services, and search current news topics, all within just a few clicks [1].

Unfortunately, older adults are an overlooked population as technology is advancing in a way that is not easily adaptable for the older generation [2][3]. Previous research has shown that the older demographic is using the Internet for common tasks, but with a very different perspective compared to a younger generation [4]. While many people have been raised with device use in their daily lives, this is not the case for many seniors. Interfaces that seem quite intuitive to an average person, may be quite intimidating and difficult for another to approach.

Many seniors prefer to have a real human assist them when using technology as they are accustomed to in person learning experiences and can comfortably engage in the experience [5][6]. Because of the familiarity of this type of interaction and the connection that can built by reading another's physical behavior, this learning method has been preferred by many individuals [5][6]. Additionally, when seniors engage in learning from a technologically literate individual, they get an understanding of how to use the device and get to observe the user's behaviour and thought process [3].

1.1. Covid-19 Influence

The COVID-19 pandemic completely changed human behaviour as the globe was forced to remain inside their homes to try and conquer the virus. The elderly and many other groups were categorized as especially vulnerable and required extra protection from the virus [7]. Though there is consistent improvement in medicine, the best course of action for these groups is to remain in isolation [7]. Over two years later, there are still social restrictions on individual's behaviours. People are required to maintain limited contact from others and are suffering the consequences of isolation. [8].

While in isolation many individuals have utilized the Internet to complete daily tasks. In hopes to maintain regular behaviours, organizations enhanced and broadened user capabilities on their websites. The additional functions commonly include pre-ordering and online payment, as well as online appointment bookings [9].

Seniors traversing these new online services are also challenged with the lack of human connection available to them. Confused customers, resource shortages, and employee illness has overwhelmed companies and their customer service departments [10]. Resultingly, consumers have the option to endure the extended wait for a customer service representative or navigate the interface on their own. Moreover, individuals were restricted from visiting other households and were required to maintain social distance when communicating with another person. A large population of seniors lost their connection to their family, friends, and caretakers.

The encouraged use of technology and deprivation of human connection has left the senior demographic especially vulnerable to the risks present on the Internet. Personal information is often required to access certain functionalities online and many users may not consider where this data is transmitted or to who. It is necessary that users understand that there are real security threats online, even if they do not seem as dangerous as a crime in real life [11].

While the Internet may be overwhelming for seniors, it is important that they have the knowledge to maintain their security and privacy. Before learning how to use new apps and websites, it is crucial to understand the threats that may be encountered and how to react. Once the senior demographic has the knowledge and resources to identify and avoid risks, they will be able to confidently ease into learning how to use emerging technologies.

This paper aims to develop a deep understanding of how elders' perception of privacy and behaviour on the Internet has changed during the COVID-19 pandemic. The analysis will be completed by first understanding the trends and changes that are influencing behaviour and the associated potential attacks. Once this background is developed, a survey will be conducted to get current perspectives from the target demographic. Using the background and survey results a list of prominent knowledge gaps can be identified. Finally, a comprehensive collection of resources and tools will be complied to address the knowledge gaps.

2. BACKGROUND

To maintain some normalcy, many individuals transferred their daily activities to an online platform. A Canadian survey found that 75% of individuals engaged in more Internet related activities since the beginning of the pandemic, and almost half of Canadians started using the Internet for new tasks [12]. Within these statistics, it was found that more than half of Canadian senior citizens increased their Internet usage [12]. A previous study identified that as the elder demographic migrates their actions to online platforms, they will be at a higher risk to be a

victim of cyber crime. This population is less tech-savvy than younger demographics and is more prone to becoming a victim to Internet fraud ploys [4]. Previous research has identified that there is a need for a sufficient teaching system to assist elders in technology security, and with the modern societal changes this need is escalated drastically [2]. It is of paramount importance that each person is educated on the information and resources required to protect themselves. The typical Internet behaviour of elders has previously involved bonding over social media sites, consulting healthcare websites, and searching for a booking travel and tourism experiences [13][14]. Elders are becoming more dependent on their devices and are comfortable within their established routine [13]. As they use their preferred websites more frequently, and observe their peers doing the same, there is a deeper level of trust for the website [13]. Similar work has shown that elders prefer to use a tool they are familiar with, and do not feel a need to use other tools if it is not necessary. Regardless of this opinion, many new tools are required for daily tasks, to reduce the amount of human interaction during the pandemic [15]. These new systems require that all individuals have the technological literacy requited to successfully use these tools.

2.1. Adapting to Current Structures

Because of its ease of use, the Internet has become a necessary part of people's routine [16]. When the global quarantine forced Internet dependency, elders did their best to quickly adapt. The pandemic caused high levels of uncertainty and the Internet provided great information sources [17]. Despite the benefits, seniors are sometimes not comfortable with new applications and are hesitant to use them [3]. It has previously been found that elders are comfortable using websites that someone else has taught how to use [3]. For example, elders could independently use a booking site that a travel agent had demonstrated to them but were not comfortable downloading and using a newer app like Uber [3]. The hesitation to explore new tools is driven by fear of misuse and the possible resulting consequences [3]. Unfortunately, the lack of use has led to an increase in potential vulnerabilities as there is a high level of unfamiliarity [15].

2.2. Common Attacks

Because of the understood behaviours of the senior demographic there are certain attacks that are target towards these individuals.

2.2.1. Phishing Attacks

Seniors are a prime target for phishing attacks based on their financial standing, trusting demeanor, lack of knowledge, and poor response procedures [4]. This population is typically unsuspecting of fraudulent messages as they are used to in person transactions and have a more stereotypical perception of a criminal [18]. Because of elders generally trusting demeanor, they have been identified as the most susceptible target for phishing messages [19]. Currently many individuals are trying to make meaningful connections using the Internet which escalates the potential of being a victim to phishing [20] [21].

2.2.2. Illegitimate Websites

Illegitimate websites can be seen as stand-alone sites, popups, or overlays of otherwise legitimate sites [22]. The malicious sites are typically showing false security alerts, giveaways, or mocking real websites [22]. Elders usually have low experience interacting with obscure websites so it is unlikely they will have success identifying fraudulent websites [4].

3. METHODS

This work aims to investigate the knowledge and perspectives of the senior population regarding their current Internet interactions. Previous work has noted that firsthand information is essential to obtaining accurate data [18]. An online survey was created and distributed to a group of elders. Using the data from the survey, the main knowledge gaps were identified, and a collection of useful resources was compiled.

3.1. Survey of Knowledge and Perspectives

The survey was created to gain a deeper understanding of elder's perception of privacy and behaviour on the Internet has changed during COVID-19. The topics of the survey include privacy concerns, privacy attitude, perceived threat, confidence to protect self, and the cost of security [2] [14]. The categorization of the "elder demographic" has been listed as many different ages. Many technologies related studies have established this age as 55, so that is the threshold used in this survey [23]. The survey was developed with each of the established concern areas as the discovery goal. The question structure asks general questions on knowledge and perception, as well as how the pandemic has changed the related behaviour. The online website Qualtrics was used to assemble and share the survey to the public. When the survey completed, the results were interpreted using R for analysis and visualization. The results were interpreted using R for statistic analyses and the results are presented as percentages to maintain anonymity of the participants. The responses were recorded in multiple choice and text entry format for quantitative and qualitative analysis.

4. SURVEY RESULTS

4.1. General Information

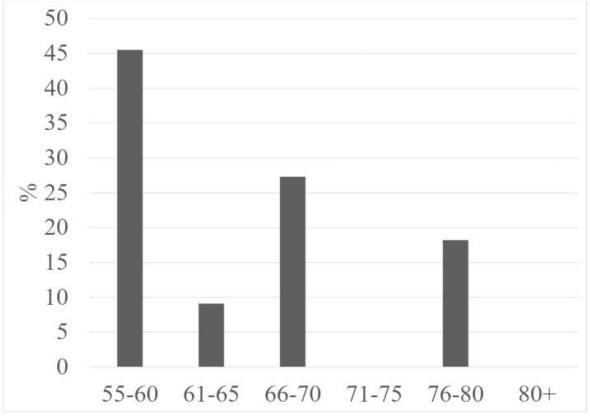

Figure 1. Age distribution of survey participants

The survey was available to the public from November 15 to 25 of 2021 and 11 participants completed the survey. The demographics of the survey included 100% females, with ages ranging from 55-80 (Fig. 1). The most common devices of the participants include laptops, smart and tablets/ iPads (Fig. 2). The "other" in Figure 2 are one Apple Watch and one smart doorbell. All participants claimed that they currently use the Internet every day and 70.8% of participants expressed that they use the Internet more frequently than prior to the pandemic (Tab. 2 in 7.7.2).

The most common uses of the Internet are to purchase goods and services, as well as watch streamed video content (Fig. 3). The increase of Internet purchases is most prominent for privacy related concerns.

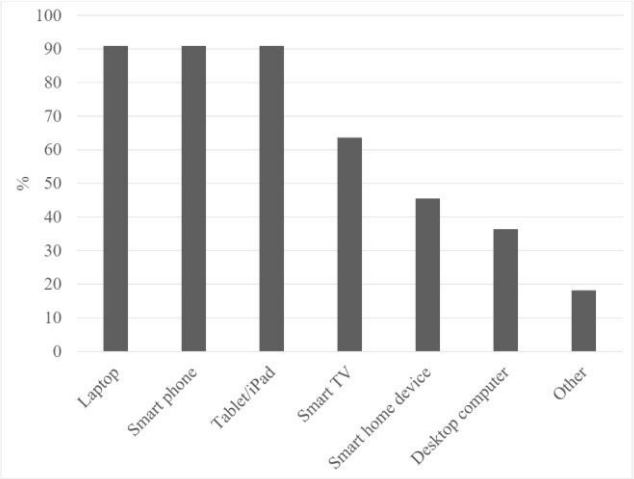

Figure 2. Percentage of participants that own each device

Participants answered that the Internet is extremely beneficial to daily life and have provided personal notes stating that they have been able to learn new hobbies and make global connections using the Internet. 72.7% of respondents said they do prefer to use the Internet for their daily tasks, while only 9.1% said that they did not (Tab. 1 in 7.2.1). Some participants said that using the Internet is the easiest way for them to check traffic and search for other information, as well as stay entertained while completing other activities.

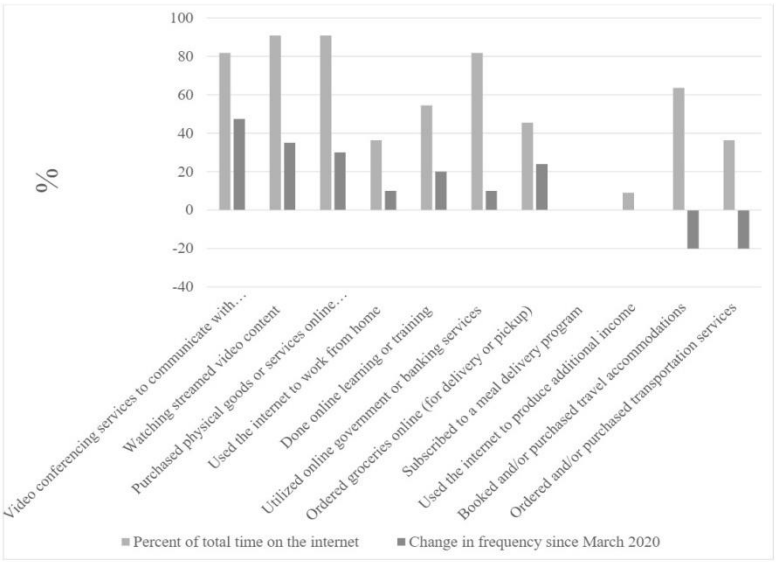

Figure 3. Change of Internet use during the COVID-19 pandemic

4.2. Privacy Attitude

100% of the survey participants said that privacy and security on the Internet are absolutely to them, with many comments regarding that they prioritize keeping information safe and a high concern regarding cyber attacks (Tab. 1 in 7.2.1).

When visiting frequently used sites over half of the participants said that they are more willing to trust the links or information requests from that website. 45.5% said that they are somewhat more willing to trust, and 36.4% expressed that they are absolutely more willing to trust these sites (Tab. 1 in 7.2.1). When asked about trusting websites that are suggested by family or peers 54.5% said that they are absolutely willing to trust, and 36.4% said that they are somewhat more likely to trust the website (Tab. 1 in 7.2.1).

4.3. Privacy Knowledge

The survey results showed that 81.8% of participants regularly update their devices, and 63.6% understand why these updates are (Tab. 1 in 7.2.1). The direct feedback was very promising with many participants explaining that the updates can fix bugs and security, with one participant even explaining how patches are deployed. When asked about the diversity and strength of passwords, 72.7% said that they use both and understand the reasoning for the requirement (Tab. 1 in 7.2.1). The participants expressed an understanding of preventing hackers and maintaining security. Though some participants did note that it was difficult to remember all their passwords for each site.

4.4. Perceived Threat

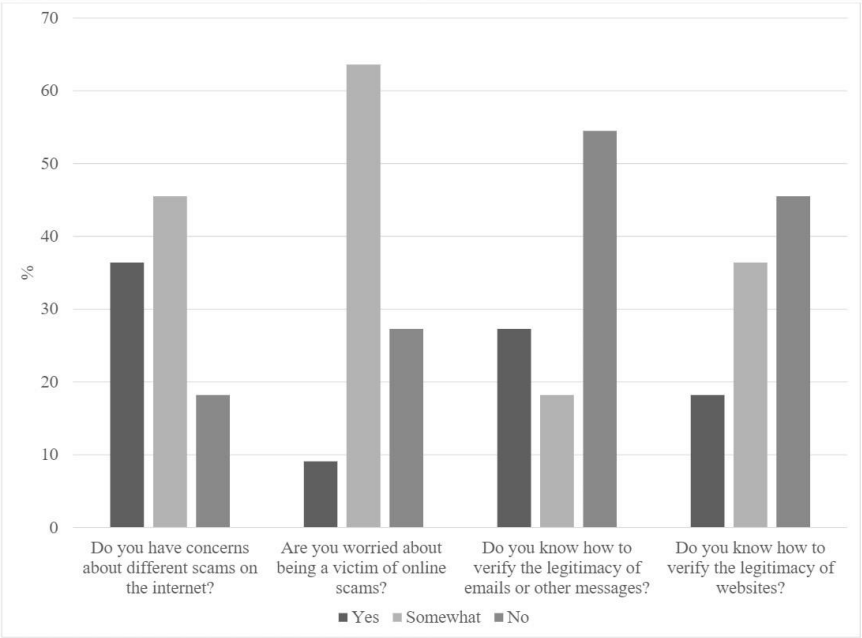

Figure 4. Perspective on potential threats

The participants of the study all expressed that they feel nervous about their privacy on the Internet and face the risk of a privacy breach whenever they do share personal information (Fig. 4). More than a few participants shared that they had been victim of a financial scam on the Internet and are nervous of it happening again. When asked about personal knowledge of phishing scams 63.6% said that they do know what they are, and 27.3% said that they somewhat understand them (Fig. 4). Though only 9.1% stated that they are worried about being victim to phishing scams, with 63.3% stating that they are somewhat worried (Fig. 4).

4.5. Confidence to Protect Self

Looking into the participants desire to protect self, majority stated that they want to protect themselves from the potential scams (Tab. 1 in 7.2.1). It was expressed that the pandemic has not changed the level of concern regarding potential scams on the Internet.

54.5% said that they do not know how to verify the legitimacy of emails or messages, and only 27.3% said that they are confident in their verification methods (Fig. 4). Similarly, 45.5% of participants stated that they do not know how to verify the legitimacy of websites, with 18.2% sure of their verification techniques (Fig. 4). Some promising verification techniques were explained including immediately deleting unrecognized messages, running anti-virus software, and looking for 'https' in the URL. Participants have also used separate email accounts for sensitive accounts and ones that may be less legitimate.

4.6. Expected Cost of Security

Regarding the perceived cost of privacy there are many barriers that may keep individuals from achieving their goals. When asked if Internet security is personally attainable 54.5% stated that they believe it is possible, but they have not achieved it. 36.4% stated that they have achieved it, and 9.1% said that they do not believe that Internet security is attainable. Despite this array of answers, 100% of participants said that they would increase their security of they were provided with the resources (Tab. 3 in 7.2.3). Participants stated that there are both knowledge and monetary barriers keeping them from attaining Internet security (Tab. 3 in 7.2.3). From a list of options of potential resources 100% said that they would like access to a software that alerts to scams of viruses, 72.7% said that they would utilize education resources, and 63.6% said that laws or legislation specifically regarding the Internet safety of seniors on the Internet would be beneficial (Tab. 3 in 7.2.3).

5. DISCUSSION

There have been efforts to assist elders and protect them from cyber crime, but these measures are insufficient for proper protection [4]. For over half a century there has been a conscious effort to engage and empower older adults to learn about technology and the Internet, yet there are still shortcomings [24]. Many different methodologies have been proposed, and significant progress has been made. There was a high level of enthusiasm regarding the participants willingness to use the Internet for their daily tasks. I believe that elders have become more adapted to using the Internet compared to previous studies [2]. The results of the survey show that elders are commonly using the Internet for purchasing goods or services and accessing bank and government sites. Because of the high sensitivity of information associated with these tasks, there is a higher importance to better protection systems. The most prominent concerns include confidently securing online financial transactions, identifying fraudulent websites, messages and other scams, and the memory of passwords. Additionally, the participants had a strong awareness of many of the threats online, but there was an optimistic bias present that participants did not

think it would happen to them. Overall, participants had an impressive amount of personal knowledge and provided strong techniques that are currently used.

5.1. Identifying Suspicious Sources

A significant level of trust in family and friend recommended websites was expressed from the results of the survey. This trust is not always unwarranted, but individuals should always do some independent inspection of the site to look for malicious components. The survey results showed that participants were unfamiliar with what to look for when trying to verify websites, emails, and other messages (Fig. 4.4). Though navigating to a new area of the Internet can be intimidating, avoiding it all together can be more dangerous. Using a browser extension (7.1.2) to alert suspicious websites when browsing will provide reassurance while navigating a search page [25].

Additionally, there are ways to manually verify a website. Techniques include searching the URL to ensure that there is an “s” in “https” or that a lock symbol in the URL [26]. Another tactic is to take a moment to really look at what is on the website. Poor grammar or low-quality logos are a good indication that the website is fraudulent [26].

When verifying the legitimacy of an email or message it is important to take a step back and consider what the content is. Typically, if a message is “too good to be true”, it is not true [27]. If someone receives a suspicious message from a known or unknown contact, it is wise for them to contact that person or company via a different method [27]. For example, if a friend suddenly emails begging for thousands of dollars for an emergency, it is smart to use another platform, such as calling to confirm their identity.

During financial transactions it is especially important to understand that relatives and banks usually do not put an intense time pressure on individuals. If there is a short time-period given with the message, it is most likely fraudulent [27]. A collection of useful resources to learn more about identifying and responding to scams on the Internet can be found in section 7.1.1.

Many of the participants explained that they are aware of scams, but there was a drastic difference in responses when asked about the worry of the scam happening to them. Figure 4.4 shows how the proportion shifts between knowledge of scams and the idea of it happening to them. This optimistic bias is a major downfall as it suggests people may not take their privacy as serious as they claim [28]. Though participants claimed that privacy is a concern there is still a nuance that the attack won’t happen to them. In the future I hope to see similar results to those questions but driven by an increase of confidence to protect oneself.

5.2. Securing Financial Transactions

Contradictory to the optimistic outlook many of the participants expressed that they had been victim to a financial scam. These breaches can occur from many different attacks such as phishing, fake transfers, or even physically stealing your card [29]. To prevent the attack there are an array of methods that can be taken such as using prepaid cards, or a middleman such as PayPal [30] [31]. A prepaid card acts almost exactly as a credit card does and can be used for online transactions without having to share your real banking information. Though there are some fees involved this method can be beneficial, especially for unfamiliar websites. Another option for secure payment or transfer is a middleman tool that encrypts your banking information and limits the amount of accessible funds. These tools are listed in 7.1.3.

In the case of a successful breach, it is important that the user has no liability for the unauthorized charges [29]. If you are using your banking card online, it is important to contact your financial institutions and inquire about this feature.

5.3. Password Security

The survey showed that many participants did use strong and diverse passwords, but some did have difficulty remembering each of them. One participant said that they use mostly numerical passwords for security, but this may be more difficult to remember. Using a tool such as a password manager can be very beneficial for maintaining accounts. Password managers securely encrypt all sensitive information that is needed to login to a site [32]. The password manager also has capabilities of generating long and complex passwords when registering for a new account or updating current accounts [32]. This information is locked in the secure vault and can only be accessed using a master key [32]. By having the password manager in place, the user only has to remember one password but maintains the security that a diverse set of passwords provides. Some recommended password managers are listed in 7.1.2.

5.4. Learning Tools

Many respondents of the survey said that they struggled with the monetary barrier of ensuring security. Many operating systems offer a free built-in firewall, but some need to be installed and enabled [33]. Learning how to enable and effectively use these can be a challenge for some elders. A group of technological women realized they were spending countless hours teaching older adults to develop their computer skills [34]. This team developed a website where volunteers offer tutorials and live help sessions to teach computer topics to elders (7.1.4).

Overall, there have been many developments in resources and tools to assist all people and seniors in achieving privacy and security while on the Internet. Some legislation has been established to penalize cyber criminals, but these efforts had little effect [20]. There is such a rapid change in technology and tools, that legislation and other protective measures may not be able to keep and maintain protection. The best way to protect elders is by providing a strong education so they can use their devices confidently [4].

Previous research has provided feedback stating that elders do want to learn how to use new apps and services but feel like they have a lack of resources for learning how to use them so avoid them all together [3]. By increasing awareness and providing trustworthy tools will encourage elders to become more involved in the technology world. There will never be an absolute way to ensure security but encouraging a privacy mindset promotes users' success [35].

6. CONCLUSIONS

Since the beginning of the pandemic, we have seen major changes in peoples' interaction and reliance on technology. Though the world has moved to a more technology integrated atmosphere, elders have had little opportunity to make the necessary adaptations.

It is difficult to make accurate assumptions about a demographic we are not a part of. To assist the senior demographic in their transition into the evolving technology landscape it is necessary to understand where their needs lay. Getting direct feedback from this demographic allowed for genuine understanding of the knowledge gaps that need attention. The results of the survey show that this demographic has a great foundational knowledge of using the Internet and governing their privacy and security. The most prominent obstacle is the lack of awareness of the tools that

are available for elders to ensure their privacy and security on the Internet. Promoting the conversation of the resources available and the need for them will increase awareness of the subject and give more opportunity for involvement.

Individual's will be able to build their confidence to protect themselves with the utilization of the tools provided. Once user confidence is built, I expect that this demographic will be able to adapt to current technology trends and ultimately thrive in the digital environment.

6.1. Future Work

The survey group in this project provided valuable information regarding the current knowledge gaps of the elder demographic. Future research could further explore this demographic by involving a larger sample with a more diverse range of participants. This study would provide deeper insight to more specific needs of seniors using technology. Deploying a large-scale project could bring more attention to the actual needs of seniors and provide developers with the incentive and necessary topics needed to build a comprehensive site for seniors.

The development of one platform that encompasses the information and attributes of the previously listed resources would be extremely beneficial for educating the senior demographic. Incorporating personal connection into learning platforms would also restore some normalcy to the participants learning style. For example, in an online class for technology education it would be interesting to see a feature that allows the participants to connect with other students to discuss their takeaways from the lesson and further deepen their knowledge. A system that connects similar participants for collaborative engagement in a e-learning environment would be extremely beneficial in this setting.

Additionally, investigation into what the technologic landscape will look like after the pandemic would be an interesting topic for further work. Many of the newly created interfaces may be abandoned and left with copious amounts of personal information. A study on personal information management techniques would compliment the resource suggestions in this work.

7. APPENDIX

7.1. Resource Topics and Links

7.1.1. Identifying Scams

• Senior Fraud Protection Kit

This document includes some information about why seniors are targeted for attacks, as well as a check list for identifying a scam and a plan of action in the case of an incident.
https://www.caregiverstress.com/wp-content/uploads/2012/07/1 Seniors Fraud Protection Kit_ US.pdf

• Internet Safety Guide for Seniors

This blog post discusses phishing, password theft, social media scams, and banking fraud. https://www.safetydetectives.com/blog/the-ultimate-Internet-safety-guide-for-seniors/

• The Little Black Book of Scams

The author explains that “knowledge is power” and understanding these concepts can help improve personal security.

https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04333.html

• Seniors’ guide to staying cyber safe during COVID-19

This brochure includes some techniques for making secure passwords as well as scam avoidance and response. https://www.getcybersafe.gc.ca/en/resources/seniors-guide-staying-cyber-safe-during-covid-19

• Recent scams and fraud

A lists of scams currently targeting individuals and businesses that are sorted by delivery mechanisms as well as information of procedures if you are a victim.

https://antifraudcentre-centreantifraude.ca/index-eng.htm

7.1.2. Security Tools

• 1Password

The most intuitive password manager and has the option to schedule a demonstration of its functions, though this does come with a monthly fee.
https://1password.com/

• Bitdefender

A free alternative is Bitwarden, which only requests an annual fee when you choose to upgrade to apremium package. https://bitwarden.com/

• Bitdefender Traffic Light

A free browser extension that scans the pages you visit for malware and phishing attempts.
https://www.bitdefender.com/solutions/trafficlight.html

7.1.3. Securing Online Payments

• Visa Reloadable Prepaid Cards

These cards have the zero-liability feature that ensures compensation in the event of an unauthorized transaction.

https://www.visa.ca/en CA/pay-with-visa/cards/prepaid-cards.html

• PayPal

Securely send money to other users or complete online transactions with services to help remediate fraudulent transactions. paypal.com/ca/home

7.1.4. Learning New Tools

• Connected Canadians

This organization provides a wide array of groups and individual help sessions, covering many topics.

https://www.connectedcanadians.ca/

7.2. Survey Results

7.2.1. Yes/No Questions

Table 1. General results from the survey

		Yes (%)	Somewhat (%)	No (%)
General Perspective	Do you think that privacy and security is important while on the internet?	100	0.0	0.0
	Do you prefer to use the internet for daily tasks?	72.7	18.2	9.1
	Do you feel nervous about your privacy and security on the internet?	63.6	36.4	0.0
	Has the COVID-19 pandemic made you **more** worried about internet scams?	9.1	0.0	90.9
Online Security and Privacy Behaviour	Do you update your devices regularly? (when the device suggests)	81.8	18.2	0.0
	Do you know why updating devices regularly is important?	63.6	36.4	0.0
	Do you know why using strong/ different passwords is important?	72.7	27.3	0.0
Privacy Attitude	Do you trust websites that you use often? (eg. social media sites, online ordering/ booking sites)	36.4	45.5	18.2
	If your family or peers suggest a website to you, are you more willing to trust it?	54.5	36.4	9.1
Perceived threat	Do you know what a phishing scam is? (eg. phone call or email)	63.6	27.3	9.1
	Do you have concerns about different scams when on the internet?	36.4	45.5	18.2
	Are you worried about being a victim of online scams?	9.1	63.6	27.3
Perceived Self-Efficacy	Do you know how to verify the legitimacy of emails or messages?	27.3	18.2	54.5
	Do you know how to verify the legitimacy of websites?	18.2	36.4	45.5

7.2.2. Internet Use and Recent Changes

Table 2. Frequency of Internet use and influence from the pandemic

	How often do you use the internet? (%)		How has your internet usage changed since the start of the pandemic? (%)
Everyday 0-1 hours/ day	9.1	It has not changed	27.3
Everyday 2-5 hours/ day	63.6	Somewhat more	27.3
Everyday 6+ hours/ day	27.3	More	45.5

7.2.3. Future Resources

Table 3. Feedback on the future of privacy and security resources

	I have achieved this (%)	Yes, but I have not achieved it (%)	No (%)
Do you feel that internet privacy / security is attainable for you?	36.4	54.5	9.1
	Monetary barrier (%)	Knowledge barrier (%)	Other (%)
What are the barriers that keep you from achieving your privacy / security goals?	36.4	72.7	18.2 - concerns and fear
	Software installation that alerts scams (%)	Education resources that teach detection and avoidance (%)	Laws and legislation to protect the elder demographic (%)
Please select the resources that you would use	100	72.7	63.6

ACKNOWLEDGEMENTS

The authors would like to thank everyone that participated in the survey as well as the family members that inspired this research!

REFERENCES

[1] M. Myint, "SAFESTART: Simplifying Technology for Seniors," 2020 Intern Reports, Apr. 2020. Available: https://digitalcommons.imsa.edu/intern_reports_2020/31

[2] Chakraborthy, Rajarshi, S. Bagchi-Sen, Rao, R. H, Upadhyaya, andShambhu, "An exploration of security and privacy behavior of elders on the Internet and comparison with younger adults," WISP 2012 Proceedings., p. 16, 2012.

[3] M. Shirgaokar, "Expanding seniors' mobility through phone apps: Potential responses from the private and public sectors," Journal of Planning Education and Research, vol. 40, no. 4, pp. 405– 415, 2020, publisher: SAGE Publications Inc.

[4] E. L. Carlson, "Phishing for elderly victims: As the elderly migrate to the Internet fraudulent schemes targeting them follow note," Elder Law Journal, vol. 14, no. 2, pp. 423–452, 2006.

[5] F. Molloy, "The Teachers Experience of Practice-based Education in Hybrid Delivery Mode," International Journal on Integrating Technology in Education (IJITE), vol. 10, no. 4, Art. no. 4, Dec. 2021, doi: 10.5121/ijite.2021.10401.
[6] G. Yaw Koi-Akrofi, E. Owusu-Oware, and H. Tanye, "Challenges of Distance, Blended, and Online Learning: A Literature based Approach," IJITE, vol. 9, no. 4, pp. 27–39, Dec. 2020, doi: 10.5121/ijite.2020.9403.
[7] Kuy, Tsai, Raymond, Bhatt, JayChu, Q. D., G. Pritesh, Gupta, Rohit, Gupta, Reshma, Hole, M. K., Hsu, B. S., Hughes, L. S., L. Jarvis, S. Jha, A. Annamalai, M. Kotwal, J. V. Sakran, S. Vohra, T. L. Henry, and C. Ricardo, "Focusing on vulnerable populations during COVID-19," Academic Medicine, p. 10.1097/ACM.0000000000003571, 2020.
[8] Hagerty and Williams, "The impact of COVID-19 on mental health: The interactive roles of brain biotypes and human connection," Brain, Behavior, & Immunity - Health, vol. 5, p.100078, 2020.
[9] S. Kohli, B. Timelin, V. Fabius, and S. M. Veranen, "How COVID-19 is changing consumer behavior –now and forever," p. 6.
[10] A. Haleem, M. Javaid, and R. Vaishya, "Effects of COVID-19 pandemic in daily life," Curr Med Res Pract, vol. 10, no. 2, pp. 78–79, 2020, doi: 10.1016/j.cmrp.2020.03.011.
[11] A. P. Sethi and R. Subramoniam, "USE OF TECHNOLOGY IN EDUCATION, BUT AT WHAT COST?," IJITE, vol. 08, no. 01, pp. 13–18, Mar. 2019, doi: 10.5121/ijite.2019.8102.
[12] S. C. Government of Canada. Internet use and COVID-19: How the pandemic increased the amount of time Canadians spend online. Last Modified: 2021-06-24. Available: https://www150.statcan.gc.ca/n1/pub/45-28-0001/2021001/article/00027-eng.htm
[13] M. J. Kim, W. G. Kim, J. M. Kim, and C. Kim, "Does knowledge matter to seniors' usage of mobile devices? focusing on motivation and attachment," International Journal of Contemporary Hospitality Management, vol. 28, no. 8, pp. 1702–1727, 2016, publisher: Emerald Group Publishing Limited.
[14] Sheng, Xiaojing, Simpson, and P. M., "Seniors, health information, and the Internet: Motivation, ability, and Internet knowledge," Cyberpsychology, Behavior, and Social Networking, vol. 16, no. 10, pp. 740–746, 2013, publisher: Mary Ann Liebert, Inc., publishers.
[15] S. C. Government of Canada. Evolving Internet use among Canadian seniors. Last Modified: 2019-07-10. Available: https://www150.statcan.gc.ca/n1/pub/11f0019m/11f0019m2019015eng.htm
[16] K. Zickuhr and M. Madden, "Older adults and Internet use," Pew Research Center, p. 23, 2012.
[17] E. M. Suh, "Culture, identity consistency, and subjective wellbeing."Journal of Personality and Social Psychology, vol. 83,no. 6, p. 1378, 2002, publisher: US: American Psychological Association.
[18] R. Chakraborty, R. Rao, V. Sankaranarayanan, and S. Upadhyaya, "Mediated Internet experience for senior citizens," Cyberpsychol Behav Soc Netw., p. 11, 2008.
[19] T. Lin, D. E. Capecci, D. M. Ellis, H. A. Rocha, S. Dommaraju, D. S. Oliveira, and N. C. Ebner, "Susceptibility to spear-phishing emails: Effects of Internet user demographics and email content," ACM Trans Comput Hum Interact., vol. 26, no. 5, pp. 32:1–32:28, 2019.
[20] M. S. Clark, R. Oullette, M. C. Powell, and S. Milberg, "Recipient's mood, relationship type, and helping." Journal of Personality and Social Psychology, vol. 53, no. 1, p. 94, 1987, publisher: US: American Psychological Association.
[21] X. Li, M. Zhou, J. Wu, A. Yuan, F. Wu, and J. Li, "Analyzing COVID-19 on online social media: Trends, sentiments and emotions," arXiv:2005.14464 [cs], 2020
[22] What are scam websites and how to avoid scam websites. Section: Resource Center. Available: https://www.kaspersky.com/resource-center/preemptive-safety/scam-websites
[23] C. W. Phang, Y. Li, J. Sutanto, and A. Kankanhalli, "Senior citizens' adoption of e-government: In quest of the antecedents of perceived usefulness," in Proceedings of the 38th Annual Hawaii International Conference on System Sciences, 2020, pp. 130a–130a, ISSN: 1530-1605.
[24] C. C. Sharpe, Online Resources for Senior Citizens. McFarland, 2003,
[25] Bitdefender TrafficLight - free add-on for secure web browsing. Available: https://www.bitdefender.com/solutions/trafficlight.html?sm id=siteshare
[26] 11 ways to check if a website is legit or trying to scam you | home bank of California. Available: https://www.hbc.bank/11-ways-to-check-if-a-website-is-legit-or-trying-to-scam-you/
[27] Scam alert: That text from your bank about possible fraud may not be from your bank. Section: NewsChannel 5 Investigates. Available: https://www.newschannel5.com/news/newschannel-5investigates/scam-alert-that-text-from-your-bank-about-possible-fraud-may\\-not-be-from-yourbank
[28] "it won't happen to me": The optimism bias. Available: https://ekuonline.eku.edu/blog/psychology/optimism-bias/

[29] A. White. Here's how credit card fraud happens and tips to protect yourself. Section: Select: Resources. Available: https://www.cnbc.com/select/credit-card-fraud/
[30] Prepaid credit cards. [Online]. Available: https://www.visa.ca/en CA/pay-withvisa/cards/prepaid-cards.html
[31] Send money, pay online or set up a merchant account - PayPalCA. Available: https://www.paypal.com/ca/webapps/mpp/home
[32] M. Fukumitsu, S. Hasegawa, J.-Y. Iwazaki, M. Sakai, and D. Takahashi, "A proposal of a password manager satisfying security and usability by using the secret sharing and a personal server," in 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), 2016, pp. 661–668, ISSN: 1550-445X.
[33] J. Mora. Best antivirus software protection for seniors (2021). Available: https://dailyhomesafety.com/antivirus-for-seniors/
[34] Connected Canadians. Available: https://www.connectedcanadians.ca
[35] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in Proceedings of the 2005 ACM workshop on Privacy in the electronic society, ser. WPES '05. Association for Computing Machinery, 2005, pp. 71–80.

AUTHOR

Caroline Hillier is a current student at the University of Guelph enrolled in the Masters of Cybersecurity and Threat Intelligence program. In 2021 she graduated from Trent University with a B.Sc. in Forensic Science and Biology. She has worked on digital security projects which inspires her research objectives of creating secure environments for end users.