

Teaching Microsoft Windows and Cybersecurity to Senior Citizens

Zakiria A. Jordan

Old Dominion University

CYSE 280 – Windows Systems Management and Security

Professor Malik A. Gladden

December 8, 2024

Introduction

As the digital world continues to evolve, seniors experience unparalleled opportunities that are paralleled by unparalleled challenges. In a time when technology bridges communications, provides access to many services, and facilitates monetary transactions, the ability to safely navigate digital tools is an acquired necessity for everyone, including older adults. Sadly, most of these seniors lack the fundamental digital skills necessary to protect them from ever-evolving cyber threats. The digital divide particularly makes them vulnerable to scams, phishing, fraud, and numerous other devastating situations with huge financial and emotional loss.

The technology adoption rate for seniors is increasing. According to research from the Pew Research Center, the use of the internet and just simply having a phone have increased steadily over the past decade among those aged 65 and older. Being that this had such a growth, seniors face great challenges from the rapid changes characterizing the growth of technology and its related cybersecurity risks. The National Institute on Aging has concluded that scams against older adults, such as phony tech support calls or phishing emails, are an alarming reality, and targeted education is seriously needed

This paper talks about the critical need to teach seniors digital literacy and give them the basic principles of cybersecurity. This will be realized through three objectives: designing an effective teaching strategy, raising awareness about cybersecurity, and describing common cybercrimes affecting seniors. By addressing these areas, we can empower seniors to use

technology confidently while safeguarding their personal and financial information from cyber threats.

Overview of the Research/Required Information

The point of this research study is to try to find useful ways to teach cybersecurity to senior citizens so that they can grow their knowledge regarding the risks to which they are exposed in the digital world. It has been found that older adults have been considered the favorite victims of cybercriminals because of their ignorance regarding online security practices. The National Institute on Aging stated older adults tend to be big victims of fraud in tech support fraud, investment scams, and other devious methods to make quick profits from unsuspecting targets due to their trusting nature (National Institute on Aging, 2023).

These scams led to huge financial losses, with this being just one example of the many that may afflict seniors day in and day out. With this, training needs to be made relevant to not only know how they arise but to avoid falling into these pitfalls. Resources from organizations like Cyber Seniors and the National Council on Aging (NCOA) emphasize the importance of teaching basic cybersecurity principles such as using strong passwords, enabling two-factor authentication, and recognizing phishing emails (Cyber Seniors, 2023; National Council on Aging, 2023). This research will also find out what common scams the seniors tend to fall for and provide solutions for preventing them.

Methodology

I would then apply the NIST Cybersecurity Framework in teaching cybersecurity to seniors. The steps involved in the NIST are identification of potential risks, protection of personal data, detection of cyber threats, response toward security events, and recovery from any attacks. These steps would be simplified to make it easier for seniors to understand and apply in their daily digital activities. Training sessions will focus on practical actions like using strong passwords, recognizing phishing emails, and protecting online accounts, all of which are common targets for cybercriminals (Cyber Seniors, 2023; National Council on Aging, 2023).

There would be short surveys and interviews to try to track the learning of the seniors from the training. Before the program, I would have them answer a survey to see their current knowledge in the field of cybersecurity; after the training, they will take another survey about how much they learned. Interviews will also be conducted to understand the problems seniors face in using cybersecurity tools and to hear about their past experiences with online scams or fraud (National Institute on Aging, 2023). By combining survey data with personal stories, the research will gather valuable insights into what works best for teaching cybersecurity to seniors.

Finally, to determine how well the learning retains over a period of time, the participants will be surveyed again after six months from the training. This will help in establishing if seniors continue to use what they learned to stay safe online. Additionally, the study will look at using peer mentoring, a method where older adults help each other learn about technology, which has been shown to improve learning in other programs like Cyber Seniors (Cyber Seniors, 2023). By

using this approach, the research aims to create an effective, long-lasting way to teach cybersecurity to seniors.

Tools/Resources/Results

There are a variety of tools and resources that will be leveraged to effectively educate senior citizens on cybersecurity. Organizations such as Cyber Seniors provide a comprehensive suite of resources tailored specifically for older adults, including webinars, online training modules, and in-person workshops that cover essential topics like password management, safe online shopping, and recognizing phishing attempts (Cyber Seniors, 2023). Further, NCOA has made available various materials regarding those kinds of frauds where the senior member gets targeted. Some of their suggestions also emphasize how the concepts of digital literacy will actually enable seniors to make smart choices online. National Council on Aging, 2023.

The Operating system used by the elderly is Microsoft Windows, and it contains some inbuilt security features that will be utilized during training. These include things like automatic software updates, applying security patches without user intervention, and real-time malware protection with Windows Defender antivirus. Teaching seniors how to use these features can help reduce the risk of cyber threats. Additional ideas concern simple yet efficient facilities and strategies: firewalls, password generators, two-factor authentication-as highly useful security measures to take easily by seniors.

Peer-to-peer mentoring has also shown to be a useful tool in cybersecurity training for seniors. According to Cyber Seniors, seniors tend to feel more comfortable learning when they receive guidance from their peers, as they can relate to them better than instructors from younger generations (Cyber Seniors, 2023). This approach builds a supportive community where seniors share knowledge and experiences, further reinforcing security awareness.

The findings of this study will be evaluated by comparing pre- and post-training surveys, along with in-depth interviews with senior participants. The main objective is to find out whether seniors are more aware of the risks in cybersecurity and if their behavior has changed, such as using stronger passwords or recognizing phishing attempts. Tracking the usage of security tools, such as the enabling of 2FA and regular software updates, will also be indicative. It is expected that with these resources, seniors will have more confidence in their ability to protect their online data, which in turn will lead to safer browsing. These outcomes will be measured to determine how effective the teaching strategies are, and further adjustments can be made to enhance the cybersecurity education for seniors.

These findings will be critical in informing future cybersecurity training programs for older adults and could serve as a model for other vulnerable demographics in mitigating risks associated with the growing presence of technology in daily life.

Conclusions

In conclusion, with the rapid adoption of technology by seniors, major focus needs to be placed on cybersecurity education. Strategies from established frameworks like NIST to resources from trusted organizations, such as Cyber Seniors and the National Council on Aging, go a great deal in enhancing the ability to protect oneself from cyber threats. This research underlines the pertinence of teaching simple and effective cybersecurity practices to older adults, such as strong passwords, recognition of phishing scams, and securing devices. As seniors become more aware of cybersecurity risks and methods for safeguarding their personal information, they will be better prepared to safely navigate a digital world. The ultimate goal would then be to make the seniors themselves capable of taking proper informed decisions online and reduce the threat of cybercrimes by helping them safeguard both their personal and financial wellbeing. With appropriate training and with the help of appropriate tools, seniors can engage fearlessly in the digital environment while reducing their risks relating to cybersecurity.

Resources

The National Council on Aging. (2023, July 6). Wwww.ncoa.org.

<https://www.ncoa.org/article/how-older-adults-can-improve-their-personal-cyber-security/>

Cybersecurity for Seniors: A Caregiver's Guide. (n.d.). Morgan Stanley.

<https://www.morganstanley.com/articles/cybersecurity-for-seniors>

Programs for Senior Organizations - Cyber-Seniors Inc. (2024, July 18). Cyber-Seniors Inc.

<https://cyberseniors.org/organizations/senior-orgs/>

Faverio, M. (2022, January 13). *Share of those 65 and older who are tech users has grown in the past decade.* Pew Research Center.

<https://www.pewresearch.org/short-reads/2022/01/13/share-of-those-65-and-older-who-are-tech-users-has-grown-in-the-past-decade>

Beware of Scams Targeting Older Adults. (n.d.). National Institute on Aging.

<https://www.nia.nih.gov/health/safety/beware-scams-targeting-older-adults>

UCL. (2021). *POLICY BRIEFING Older adults as victims of online financial crime DAWES*

CENTRE FOR FUTURE CRIME AT UCL 1 DAWES CENTRE FOR FUTURE CRIME AT UCL.

https://www.ucl.ac.uk/future-crime/sites/future_crime/files/ucl_policy_briefing_-_older_people_and_financial_crime_december21.pdf