CyberGuardians: Improving Community Cyber Resilience Through Embedded Peer-to-Peer Support

James Nicholson
Northumbria University
Newcastle, UK
james.nicholson@northumbria.ac.uk

Jill McGlasson
Northumbria University
Newcastle, UK
jill.mcglasson@northumbria.ac.uk

Abstract
Older users are rapidly adopting internet-enabled devices, yet are often targeted by cyberattackers with possible disastrous consequences. We describe the CyberGuardians initiative where we train older members of the community to be knowledgeable about cybersecurity so they can spread the information to peers and help protect their communities from cyber harms. Specifically, we focus on a case study evaluating two CyberGuardians and their use of training materials to inform peers in their community about cybersecurity. We discuss the importance of flexible training materials that can be adapted by CyberGuardians for sharing with peers.

CSS Concepts
•Security and privacy~Human and societal aspects of security and privacy~Social aspects of security and privacy

Author Keywords
Cyber resilience; cybersecurity; cyberhygiene; older adults; interactive training.

Introduction
Understanding cybersecurity threats and defences is essential for citizens to protect themselves in an ever-changing technological landscape. Recent work has reported that older adults seek information in different

DIS '20 Companion, July 6–10, 2020, Eindhoven, Netherlands

ACM ISBN 978-1-4503-7987-8/20/07.
https://doi.org/10.1145/3393914.3395871

Training Content & Demos

Session 1: Password Management

- Demo: password guessing software
- Demo: popular passwords
- Demo: Password manager
- Demo: Two-Factor Authentication

Session 2: Scams

- Video: Call scams
- Video: Mind Readers & Social Media
- Demo: Scam step-by-step
- Demo: Vigilance on Mobile Devices
- Activity: Reading URLs
- Demo: Phishing Website Construction
- Activity: Phishing Quiz
- Demo: Reverse Searching

Session 3: Protective Software

- Video: Unsecured WiFi
- Activity: Software Updates
- Video: Ransomware

Figure 1: Training sessions and interactive activities to engage CyberGuardians.

ways to younger users [8]. Specifically, the availability of the source seems to be most important to older users whereas younger users will prioritise expertise [9].

Older users typically struggle to understand the ever-changing landscape of cybersecurity threats and defences and are often targeted by attackers [1–3], resulting in them losing more money than the general population when scammed [1,10]. They generally have more investments and savings but, unlike younger users, will find it more difficult to replace any stolen savings as they may no longer work and are therefore financially dependent on their pensions and savings. This, in turn, can lead to scams having a more detrimental impact on their health and wellbeing [2].

As governments (e.g. UK, US and Singapore) follow a digitisation programme for key services and rural banks/post offices close, older people are having to manage their finances on-line which provides fraudsters with more opportunities to scam this age group. Yet policymakers in the UK have yet to catch up with the problems facing older users (e.g. 65 years and older) despite acknowledging the fact that the UK has a rapidly ageing population which could account for approximately 25% by 2028 [4].

This paper describes an initiative which aims to support older users in becoming knowledgeable about cybersecurity – or *CyberGuardians*. The goal is for our CyberGuardians to promote good cybersecurity behaviours within their local communities with the aim of helping protect peers from cyberattacks through simple guidance, while also serving as an approachable and available source of information for all cybersecurity-related queries.

This paper describes the CyberGuardians process with a focus on the role that training materials play on the confidence and follow-on actions of the participants.

Method: Training the CyberGuardians

The content and structure of the training workshops were discussed thoroughly with our non-academic partners and with the CyberGuardians themselves during a workshop prior to commencing the training sessions. The training focused on three main cybersecurity areas [6]: password management, scam detection and protective software (see Figure 1). The training material was user-friendly in terms of not being technical and relating it to concepts which they could grasp such as describing the process of hashing as "juicing an orange". This was well-received as evidenced by questionnaires after every event – with approximately 70% of participants rating the sessions as excellent and 30% as good – and a 0% dropout rate.

We recruited fourteen older users aged between 55 and 80 years from the North East of England with the help of our project partners. They were not selected for their IT skills as some were highly competent whereas others just managed with basic skills. Participants were promised free training on cybersecurity-related topics in exchange for them passing on that knowledge to peers. No guidance – or obligation – was given about how to spread this knowledge as we were interested in the methods employed by our CyberGuardians to engage with their peers.

All our CyberGuardians received formal training through interactive workshops with presentations, videos, live demonstrations, (e.g. password cracking) and hands on activities (e.g. phishing tests). The topics covered had been identified by the group themselves as well as existing literature on older users (e.g. [5,8]). The full training

Term	Definition
Authentication	The act of proving to a system that you are who you say you are (e.g. with *knowledge* (text password), a *token* (a card), or a *biometric* (a fingerprint))
Password	The most common form of authentication. Knowledge-based, meaning it is a secret between you and the computer. Usually text.
Strong Password	A password that is unlikely to be guessed. Traditionally contains 8 or more characters, uppercase and lowercase letters, numbers and symbols. Completely random. New research (and advice) suggests three random words for most users.
Guess a Password	Most likely done by a computer program (password cracker).

Figure 2: Part of glossary provided to CyberGuardians during training (session 1). Later used by Jane and Joe as interactive activity with attendees of their training session.

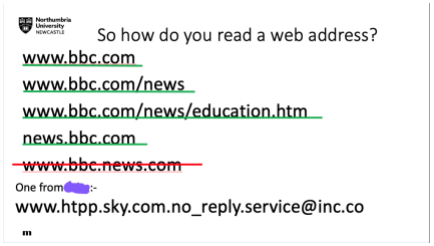

Figure 3: Training slide modified by Joe.

consisted of three workshops, each lasting three hours and held on university premises.

The live demos (see Figure 1) included showcasing the ease with which commonly used passwords can be guessed using password crackers, how to read URLs, and an interactive quiz on spotting phishing emails to reinforce the main social engineering concepts. There had to be a balance between making them aware of the threats out there in the cyber world whilst encouraging them to be part of that world. Feedback from CyberGuardians emphasised the importance of the demonstrations in helping them understand key cybersecurity advice.

The CyberGuardians were given paper handouts of the presentations as well as digital copies. All training sessions were also video recorded and were made available to the CyberGuardians for watching at a later time if necessary. Glossaries of key terms were provided for all CyberGuardians (see Figure 2).

Following the training sessions, the CyberGuardians returned to their everyday lives armed with new cybersecurity knowledge to disseminate. It is important to note that while CyberGuardians were encouraged to help as many people as they felt comfortable with, they were not forced to carry out any particular activities. The research team kept in touch with Guardians regarding support options and to remind them to keep notes on any of their on duty encounters. This study was approved by our University's Ethics Committee.

Findings: Jane and Joe

The CyberGuardians disseminated their knowledge in a variety of ways, from one-on-one chats with friends to setting up training sessions for groups. The number of people that the CyberGuardians interacted with varied on a per-person basis, but averaged on 9 people per CyberGuardian after an initial one-month period.

Here, we present a case study of two CyberGuardians, Jane and Joe (not real names) who decided to work together and deliver a session on cybersecurity to a group of peers following their CyberGuardians training. Initially, both Jane and Joe were unsure about attending the CyberGuardians training, but decided that they would attend together in order to *"find out how to better protect [themselves] online"*.

In order to disseminate their cybersecurity knowledge, Jane and Joe decided to replicate the training they received as they had a *"model to work from"* as well as materials (e.g. the original presentation slides and recordings from the training sessions) that they could repurpose (see Figure 3). However, they needed to condense the training from nine hours to two hours, so decided on two topics that *"would appeal"* to their age group: They felt passwords and scams would be useful as passwords are a necessity and scams are becoming more sophisticated.

The modification of the content resulted in some of the demonstrations being removed due to both lack of technical skills to reproduce these and the time taken to run them. However, other activities, such as how to read URLs and guessing the common passwords were kept and enhanced using their own examples to improve the appeal to their age group. The glossaries were also distributed to attendees as were used as interactive prompts. Encouragingly, some advanced content (e.g. password managers and two-factor authentication) was kept for the training sessions, indicating that the CyberGuardians were confident with these newly-introduced gold standard tools.

Jane and Joe relied solely on the digital copies of the slides and the recorded video sessions to prepare their materials for their training session. They both felt that there was no need to independently source any additional materials.

Eighteen people attended the training session and the feedback, including verbal, from feedback sheets, and later through email was very positive, with 12 attendees intending to (or having already) change their passwords as a result. In fact, one attendee explained that after the training they were able to spot a suspect email and put into practice what they had learned from attending this training event: *"Looking at addresses of emails, for example an email came from the president of an organisation I belong to saying 'I have something for you to do immediately' I looked at the address, I looked at the email, and I thought 'this is not my friend, she would not address me in that manner' and neither was the address at the top the one that you would expect to find. So just double checking the addresses and the content… I really question everything now." (Session Attendee)*

Session attendees also commented that Jane and Joe kept reinforcing the phrase, *"If in doubt, leave it out"* which offered good advice when being unsure about an email: The best course of action being to ignore while also easy to remember which is essential for the older generation. Eliciting urgency from users is a key technique used by scammers, thus ensuring that users remain calm is a key strategy for avoiding becoming victims of fraud [7].

Importantly, the CyberGuardians enjoyed the experience and have put plans to continue delivering training sessions to other peers, suggesting that this could be a sustainable model: *"I enjoyed it. It was very satisfying to do the session that we did and get the feedback that we did and I feel that we have actually done a reasonable job in putting it across. That was good." (Jane)*

Implications for Cybersecurity Training

Jane and Joe's experiences highlight two key aspects to consider when designing cybersecurity training sessions for older users: flexible materials and encouraging teamwork.

The materials provided (including the session videos) were adequate and enabled the CyberGuardians to adapt to their own training style and to tailor them for their audience who they knew well. It is key to support CyberGuardians with flexible materials from the outset that can be adapted to their needs, as other CyberGuardians who have chosen alternative methods of spreading cybersecurity knowledge have not requested additional aids or materials and have instead relied on verbal instruction.

It was also clear from the case study that working with a partner can increase confidence – not just in disseminating information, but also to encourage people to try something 'scary' like attending cybersecurity training. As Joe explained: *"Being a team made the difference to what we were prepared to do"*. This is perhaps an aspect of the recruitment material that can be adapted to encourage citizens to identify partners or groups that they can attend with and later disseminate their knowledge.

Finally, working with non-academic partners familiar with this age group was invaluable for pitching the training sessions at the adequate level and engaging the participants in the first place. However, it is crucial that as academic institutions we do not dictate how citizens disseminate cybersecurity information, but rather that we trust and support them to use their own methods.

Acknowledgements

This work was funded by the CyberGuardians project through the EPSRC NetworkPlus on Social Justice through the Digital Economy (EP/R044929/1), UK.

We would also like to thank Mike Martin for his continued support and our project partners the University of the Third Age (U3A) Whitley Bay and the Old Low Light Heritage Centre.

References

[1] AgeUK. 2015. *Only the tip of the iceberg: Fraud against older people*. AgeUK. Retrieved August 7, 2018 from https://www.ageuk.org.uk/documents/en-gb/for-professionals/consumer-issues/age%20uk%20only%20the%20tip%20of%20the%20iceberg%20april%202015.pdf?dtrk=true

[2] AgeUK. 2019. Older person becomes victim of fraud every 40 seconds. Retrieved March 12, 2020 from https://www.ageuk.org.uk/latest-press/articles/2019/july/older-person-becomes-fraud-victim-every-40-seconds/

[3] Nabat Arfi and Shalini Agarwal. 2013. Knowledge of Cybercrime among Elderly. *International Journal of Scientific & Engineering Research* 4, 7: 1463–1468.

[4] Sarah Coates, Priya Tanna, and Eleanor Scott-Allen. 2019. *Overview of the UK population - August 2019*. Office for National Statistics. Retrieved March 13, 2020 from https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/articles/overviewoftheukpopulation/august2019#the-uks-population-is-ageing

[5] Cassandra Cross. 2017. 'But I've never sent them any personal details apart from my driver's licence number …': Exploring seniors' attitudes towards identity crime. *Security Journal* 30, 1: 74–88. https://doi.org/10.1057/sj.2015.23

[6] National Cyber Security Centre. 2019. Top tips for staying secure online. Retrieved March 31, 2020 from https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

[7] James Nicholson, Lynne Coventry, and Pam Briggs. 2017. Can we fight social engineering attacks by social means? assessing social salience as a means to improve phish detection. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security* (SOUPS '17), 285–298.

[8] James Nicholson, Lynne Coventry, and Pamela Briggs. 2019. "If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI '19), 1–11. https://doi.org/10.1145/3290605.3300579

[9] Norbert Nthala and Ivan Flechais. 2018. Informal Support Networks: an investigation into Home Data Security Practices. In *In Proceedings of Symposium on Usable Privacy and Security (SOUPS) 2018*, 20.

[10] Joseph J Simons, Noah Joshua Phillips, Rohit Chopra, Rebecca Kelly Slaughter, and Christine S Wilson. *Protecting Older Consumers*. Federal Trade Commission.