Training and Embedding Cybersecurity Guardians in Older Communities.

James Nicholson

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

Ben Morrison

University of Sunderland, Sunderland, UK, ben.morrison@sunderland.ac.uk

Matt Dixon

Northumbria University, Newcastle, UK, matt2.dixon@northumbria.ac.uk

Jack Holt

Newcastle University, Newcastle, UK, j.holt3@newcastle.ac.uk

Lynne Coventry, Jill McGlasson

Northumbria University, Newcastle, UK,lynne.coventry@northumbria.ac.uk; jill.mcglasson@northumbria.ac.uk

Older adults can struggle to access relevant community expertise when faced with new situations. One such situation is the number of cyberattacks they may face when interacting online. This paper reports on an initiative which recruited, trained, and supported older adults to become community cybersecurity educators (CyberGuardians), tasked with promoting cybersecurity best practice within their communities to prevent older adults falling victim to opportunistic cyberattacks. This initiative utilised an embedded peer-to-peer information dissemination strategy, rather than expert-to-citizen, facilitating the inclusion of individuals who would ordinarily be unlikely to seek cybersecurity information and thus may be vulnerable to cyberattacks. We report on ways the CyberGuardians used informal methods to create more aware communities, served as role models for behaviour change and indirectly improved their personal wellbeing. We discuss considerations for supporting CyberGuardians, including implications for sustainability and for replicating this model in other digital contexts, e.g., recognising misinformation or improving mental health.

CCS CONCEPTS •Security and privacy~Human and societal aspects of security and privacy~Social aspects of security and privacy •Social and professional topics~User characteristics~Age~Seniors •Human-centered computing~Human computer interaction (HCI)~HCI design and evaluation methods~Field studies

Additional Keywords and Phrases: Older adults, civic engagement, community, cybersecurity, information sharing.

CHI '21, May 8–13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-8096-6/21/05…$15.00
https://doi.org/10.1145/3411764.3445078

1 INTRODUCTION

It is important for older adults to remain engaged physically, cognitively, and socially as they age [25]. Moving more activity online has the potential to be either a facilitator or a barrier to such engagement [5]. Online technology can facilitate social inclusion through social media, instant messaging and video calling, but some older adults may not feel confident engaging with these technologies. As a consequence, ensuring that older adults are active in both online and face to face communities becomes important for healthy aging.

The number of older people using the internet continues to rise [21], and this uptake will have been further accelerated by the COVID-19 pandemic forcing older adults to physically isolate. Technology is now a necessity for maintaining engagement with the outside world, yet a clear obstacle for engaging with the internet can be not feeling safe online. Older adults typically have a higher fear of crime which can affect the activities they take part in [15]. These fears are not unfounded, as older users are disproportionally targeted by online attackers [1–3] with detrimental effects [1,37]. Older adults generally have more savings – hence being targeted – and may find it hard to bounce back from financial loss associated with cyberattacks as they have fewer external sources of income to rebuild these life savings. This, in turn, can lead to successful scams having a significant adverse impact on their health and wellbeing [2].

As such, it is important to ensure that these older and potentially vulnerable citizens have access to appropriate cybersecurity information so they can effectively protect themselves from online harms. We know that older adults seek cybersecurity information in different ways to younger adults [28]. Specifically, the availability of a provider of information seems to be most important to older adults whereas younger adults will prioritise the provider's expertise [31]. This difference in information-seeking habits can, in part, be attributed to their social networks (e.g. lack of access to knowledgeable individuals) and to problems mastering the cybersecurity language [28]. While training sessions are a preferred method for learning about technical subjects, these can be complicated to develop suitably for this population [4,26,28] and may only reach only a small proportion of those who would benefit from the information.

In this paper, we develop and evaluate a community-driven solution aimed at improving the cybersecurity resilience of older communities while also engaging this population with civic participation. Our aim was to embed knowledgeable sources of information in communities to facilitate the spread of good cybersecurity practices and reduce the susceptibility to opportunistic online attacks while empowering older users to feel confident using online technologies. This was achieved by training 14 older adults to understand cybersecurity best practices and supporting them in sharing that information with their peers over a nine-month period.

The contributions of this paper are:

(1) Firstly, we believe this is the first academic paper to detail a real-world longitudinal evaluation of a community-driven initiative to empower older adults in reducing susceptibility to opportunistic online attacks in their communities, and detailing their preferred methods for doing so;

(2) Secondly, we discuss the sustainability challenges that such community-driven initiatives face;
(3) Finally, we present insights into the recruitment and training for older members of the community to engage with similar community-driven civic initiatives.

2 BACKGROUND

Older adults are the fastest growing population among internet users [14,21] and use technology for a variety of purposes, from maintaining communication [22], through to everyday activities such as online banking [7]. Despite this, there remains a number of issues which may result in online social injustice for older adults, rather than allowing them to receive the many benefits it avails.

2.1 Older Adults and Cybersecurity

Older adults represent a particularly vulnerable online group and are actively targeted by specific cyberattacks such as pension scams [1,24] and romance scams [20] in addition to the range of threats also facing the general population [1,10]. Furthermore, when they are attacked, they are more heavily victimised, losing more money when compared to their younger counterparts [20].

Understanding cybersecurity in this population is essential for ensuring that older adults can protect themselves in an ever-changing technological landscape. Recent research has suggested that one key factor in understanding older adult cybersecurity behaviour stems from their information seeking behaviours [28]. Older adults' cybersecurity information seeking behaviours differ from younger users in one way: older users appear to prioritise the availability of an information source over all other criteria, unlike the general population who prioritise expertise [31]. This difference in source prioritisation may be one of the key contributing factors as to why older users are more vulnerable than the general population when it comes to understanding and protecting against current and future cybersecurity threats. This, therefore, promotes a key question as to how this vulnerability might be mitigated.

Not only is it possible to develop and promote training sessions aimed at older adults, we know that hands on [26], one-on-one [4] and face-to-face [28] sessions are the preferred methods for learning about technical concepts for this population. We also know that they prefer to learn independently or from peers rather than being lectured by experts [26]. These training sessions, however, typically only attract individuals with the motivation to learn more about cybersecurity, something which we have long known is not prevalent in many citizens [44]. Other attempts to improve cybersecurity knowledge and behaviours of older adults have included online learning through web-based surveys and scenario-based apps [6]. Although these methods have been shown to significantly improve cybersecurity awareness and skill levels in experiments, they often struggle with ecological validity and are not widely adopted in the real world or able to create any practical change. It is likely that interventions which lean towards older adults' preferences, such as by prioritising available sources of face-to-face information, will be more useful in promoting active cybersecurity engagement in older adults. However, to date, no existing research has tested the acceptability and feasibility of such initiatives.

2.2 Older Adults and Online Civic Engagement

Social isolation and depression within older adults is expected to become the most prevalent cause of disease burden by 2030 [45] despite aging research establishing the importance of older adults remaining active in their communities [25] to deter some of these long-term effects [35]. However, older adults may struggle to

seek help and build social networks due to emotional reticence [33] or actively disengaging with society [38]. Lack of social support can be a key factor in the transition to social isolation [39].

Civic participation may help to mitigate some of the loneliness experienced by older adults by providing a role and purpose in which they stay engaged to help their communities [36]. Many such initiatives, as well as key services such as banking, post-offices, etc. have begun to move online. While we have seen some of these online initiatives be successful, e.g. in community radio [34], the movement of such initiatives into online settings can introduce a number of implications [5]. Firstly, although recent research has suggested that the internet can be an important tool in facilitating social interaction among older adults [22], it can also have the side effect of excluding some older users who do not possess the knowledge, accessibility, or desire to engage online. More importantly, the movement of such schemes into online settings exposes more older adults to this potentially dangerous online environment.

2.3 Cybersecurity Advocates

It is important for older adults to feel safe when using online technologies. While cybersecurity protective information is typically not sought out by individuals [13], older adults may be more motivated to learn about protecting themselves due to their high fear of crime [15]. It is also well established that stress brought on by fear of cyberattacks engenders an emotion-focused coping response, which can lead to disengagement with cybersecurity behaviours [11] and/or lower interactions with online services.

Routine Activity Theory [9] argues that there are three conditions that drive crime: the presence of a likely offender, the presence of a suitable target, and the absence of a capable guardian. The third role is especially interesting. Guardians have been defined as those that *"keep an eye on the potential target of crime. This includes anybody passing by, or anybody assigned to look after people or property. This usually refers to ordinary citizens, not police or private guards…"* [19]. In the context of cybersecurity, these capable guardians can be identified as those who take it upon themselves to ensure that others are knowledgeable about cybersecurity issues. These individuals, referred to in this research as *Cybersecurity Advocates*, typically take up this role due to interest in the topic in addition to feelings of self-efficacy [17]. While some extrinsic motivators such as monetary compensation can also play a role, these are usually minimal. These individuals are typically IT professionals or university academics who support others with cybersecurity help [16]. Their audience can be described as those they regularly encounter opportunistically, such as colleagues and end users, although on occasion they can engage with the general public [17]. While these Cybersecurity Advocates may play a favourable role in cybersecurity information dissemination, they usually only influence those in immediate proximity of them. This is problematic for populations who typically do not come into contact with these individuals, e.g. older adults, who may only interact regularly with neighbours or selected close others such as family and friends.

3 CITIZEN-CENTRED CYBERSECURITY SUPPORT: THE CYBERGUARDIANS INITIATIVE

In this paper we report the findings of a nine-month long community-driven cybersecurity initiative aiming to support older adults in becoming knowledgeable about cybersecurity and to share best practice with their peers. In contrast to traditional training programmes and self-selected Cybersecurity Advocates [16,17], the purpose of this initiative was to embed trained Cybersecurity Advocates into older adult communities to facilitate the spread of best practice to members who are typically harder to reach, i.e. those unlikely to look out for

cybersecurity information or attend training sessions. We also emphasise the sharing of information by peers, which is a method valued by older adults [26]. Throughout this paper, we refer to these trained individuals as '*CyberGuardians*'.

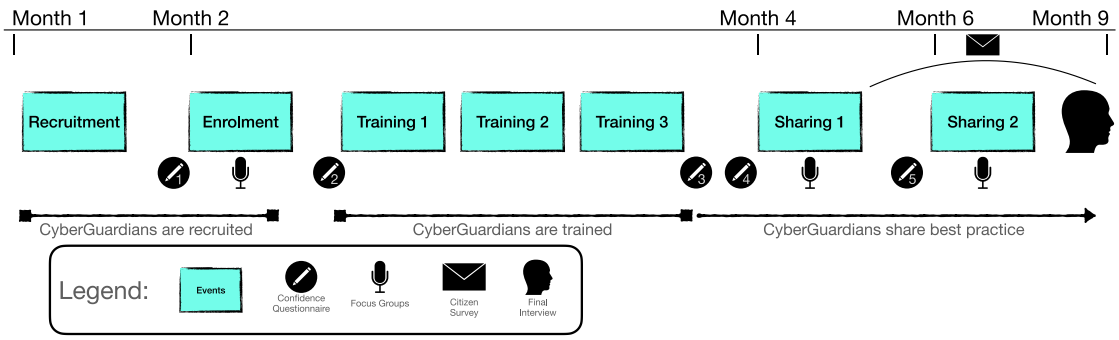


Figure 1: Timeline of the CyberGuardians Initiative including events and data collection points.

The initiative's philosophy highlighted that there is no such thing as being 100% secure – a notion communicated to the CyberGuardians at the start of each training session. However, by enacting the simple behaviours identified from academic research and official government advice (e.g. [1,10,27,28], see Fig 3 for example advice), citizens can reduce the risk of simple opportunistic cyber attacks. It was emphasised during the training sessions that the role of the CyberGuardians was not to force anyone into the adoption of security technologies or behaviour change, but rather to improve citizens' awareness of simple behaviours they could employ for better online protection and peace of mind.

The initiative consisted of several stages in which the CyberGuardians were brought together for the purpose of information sharing, training, and/or data collection (see Figure 1 – we note that the national COVID-19 lockdown restrictions commenced in month 5 of the initiative). We can roughly categorise the initiative as a training phase followed by an active stage, where participants began to share their new knowledge with peers. In total, all 14 older adults who were recruited to become CyberGuardians subsequently completed their training sessions. Following the training, 10 CyberGuardians actively engaged with their roles and participated in subsequent events, focus groups, and interviews. Although the CyberGuardians were not directly financially compensated for their time, they were able to claim back travel expenses and any related expenses (e.g., room hire for workshops, food, etc.). This initiative was reviewed and approved by our University ethics board.

3.1 Project Partners

Throughout this initiative we worked alongside representatives from non-academic partners who work with older adult communities to ensure that our CyberGuardians and their local communities benefitted from the project. This included their involvement in: recruitment, production of training materials (to ensure appropriateness), and offering ongoing support for a number of the CyberGuardians.

Our partners included the University of the Third Age (U3A) Whitley Bay, the local branch of a national volunteer-based organisation aimed at people who have retired and encouraging them to share their knowledge, skills and interests in a friendly environment. The U3A is widely spread across the UK, with over a

thousand groups and a combined 400,000 members covering a wide range of interests from walking dogs, to book clubs and IT classes. Our other project partner was the Old Low Light Heritage Centre, a regional heritage centre that served as an activity centre for residents. This centre is run by volunteers, the majority of whom are older adults.

3.2 Recruitment of CyberGuardians

First, we ran a cybersecurity awareness event aimed at older adults which was advertised through our partners' communication platforms and by email to people who had previously participated in other university projects. At the end of the event, attended by 84 older adults, we described the initiative and invited people to enrol for the 8-month initiative while noting that long-term commitment was not necessary at that stage. Following this event, a workshop was scheduled and attended by interested individuals (n=16). After consent procedures, this workshop sought to gather insights into the possible avenues of cybersecurity training by splitting participants into groups and asking them about their concerns when going online, and to detail any troubling online experiences (either personal or from peers).

Table 1: Participants Who Completed the CyberGuardians Training (Locations within region).

Pseudonym	Age	Gender	Past Occupation	Location
Joe	70-75	Male	Retail	Rural: West
Jane	70-75	Female	Healthcare	Rural: West
Ken	70-75	Male	Pharmaceuticals	Rural: East
Tom	65-70	Male	I.T.	City centre
Kay	60-65	Female	I.T.	City centre
David	65-70	Male	Teacher	City: 60 miles south
Daniel	65-70	Male	Teacher	Rural: East
Terry	70-75	Male	Social Work	Rural: East
Amelia	55-60	Female	Healthcare	Rural: East
Charles	70-75	Male	Finance	City: 15 miles south
Cynthia	70-75	Female	Hospitality	Rural: East
Robert	75-80	Male	Retail	Rural: South
Joseph	70-75	Male	Undisclosed	Rural: East
Claire	70-75	Female	Undisclosed	Rural: East

We recruited 14 older adults aged between 55 and 80 years from the North East of England (see Table 1) for the CyberGuardians initiative. The majority of the CyberGuardians belonged to one or both of our partners' organisations, but only two knew each other before joining the project. They had all retired and came from a variety of occupational backgrounds: retail, IT, social work, teaching, healthcare and pharmaceuticals. They had varying levels of IT knowledge, with two being highly competent and the majority being able to use the internet for everyday tasks, but without in-depth technical knowledge. Throughout this paper, we will refer to our participant CyberGuardians using the pseudonyms in Table 1.

Their primary motivation for joining the initiative was to *"find out how to better protect [themselves] online"* (Jane), although having the opportunity to assist others to stay safe was another common motivator. The two retired IT professionals had seen the concrete consequences of cyber harms in their working lives, and thus understood the importance of cybersecurity behaviours. A number of the CyberGuardians also had personal

experiences of dealing with cybersecurity consequences including knowing elderly relatives and neighbours who had been scammed, but did not report having been victims of any cyber harms themselves.

3.3 Training the CyberGuardians

The content and structure of the training workshops were co-designed with our non-academic partners and with the CyberGuardians themselves during the enrolment workshop. The cybersecurity topics were agreed on after reviewing existing academic literature on older users (e.g. [10,28]), charity reports [1], and official government advice [27]) in addition to the partner insights to develop the training materials. A second face-to-face meeting was arranged with our partners to showcase and discuss the slides, videos, and demonstrations. Minor changes were suggested on the topic of encryption and hashing, with an agreement to use the metaphor of '*juicing an orange*' to make these concepts more relatable.

During the enrolment workshops, CyberGuardians were asked about cybersecurity topics of interest, their experiences with these topics, and any weaknesses they believed they needed further help with. These insights were taken into consideration alongside the aforementioned sources when finalising the contents of the presentations and the ordering of the activities.

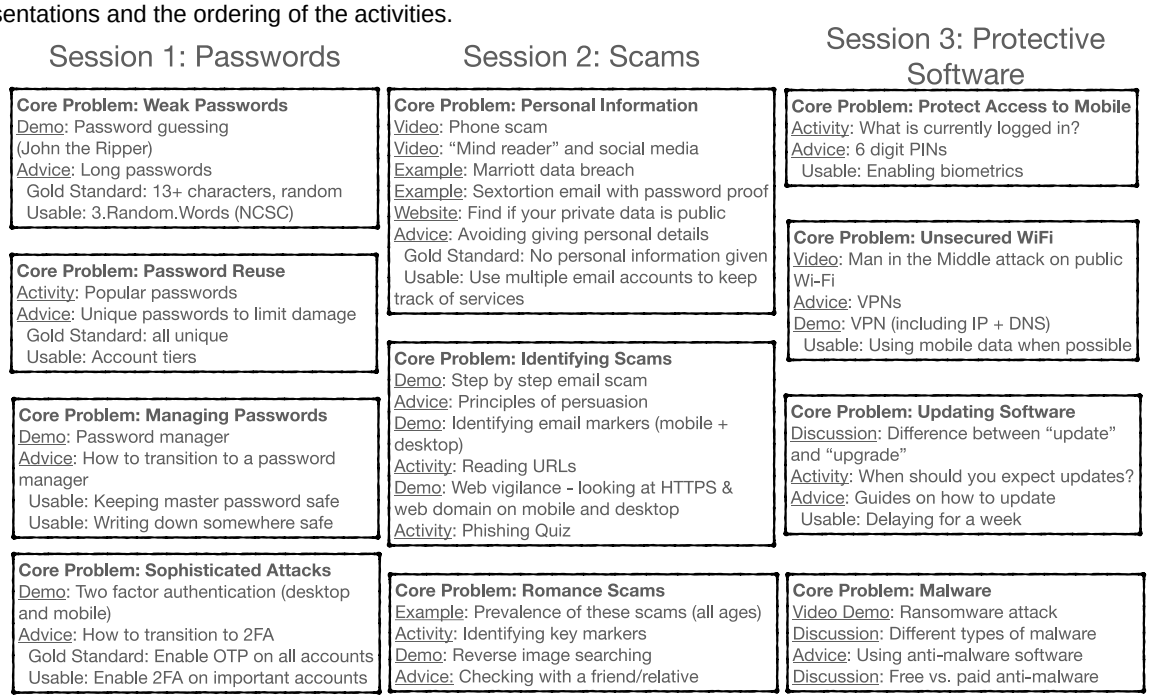


Figure 2: Overview of training topics and activities. CyberGuardians were encouraged to ask questions throughout and at the end of each section.

The training focused on three main cybersecurity topics: password management, scam detection and protective software (see Figure 2). The content was split into 3 three-hour sessions, repeated twice to accommodate participant availability. The sessions consisted of interactive workshops including: presentations, videos (e.g. social engineering), live demonstrations (e.g. password cracking), hands on activities (e.g. phishing

tests), as well as question and answer sessions. Each session concluded with a summary of key habits associated with the training topic (e.g., see Figure 3 for example takeaways for Session 1: Passwords). Feedback from the CyberGuardians emphasised the importance of the demonstrations in helping them understand key cybersecurity advice, in line with previous work highlighting the importance of technical demonstrations for enhancing the understanding of cybersecurity concepts [29].

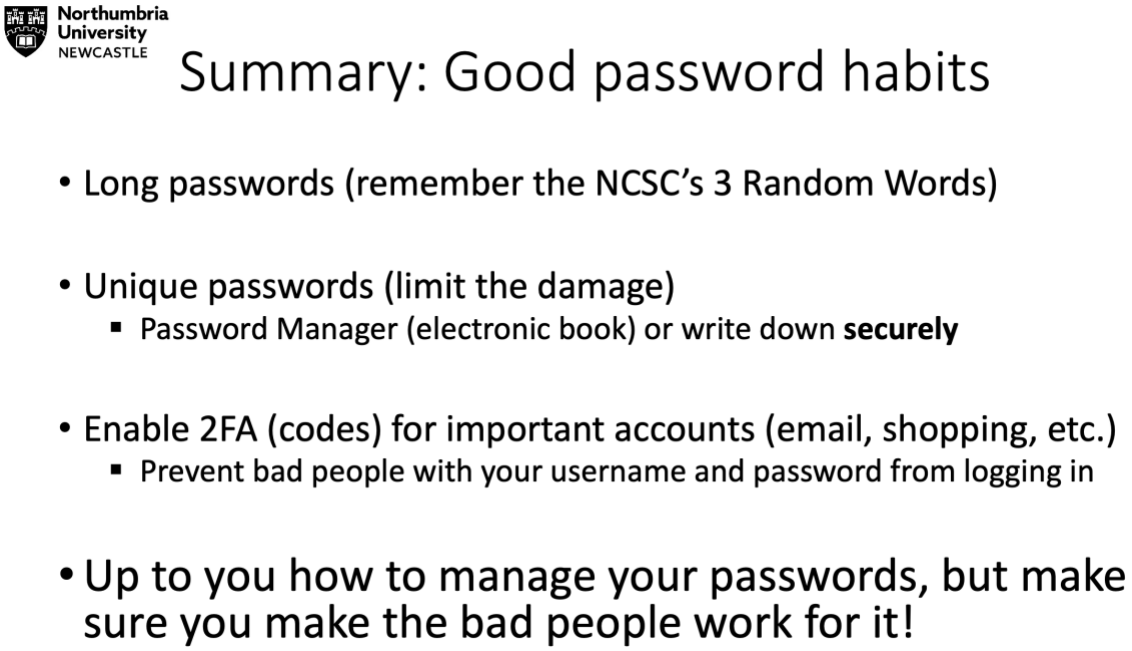


Figure 3: Summary slide from the password management training workshop detailing key habits (from simplest to most complicated). Each of these listed habits was covered in detail with examples and activities earlier in the workshop.

The CyberGuardians were also given paper handouts of the presentations to make notes on key information, as preferred by this age group [26]. All training sessions were video recorded and were made available to the CyberGuardians so that they could watch them again or at a later time if necessary, along with the digital slides. Glossaries of key terms were provided, something which helped to address their concerns about not being able to understand cybersecurity terminology – as highlighted in extant literature [28]. CyberGuardians were also made aware of the key sources of accurate cybersecurity information such as the National Cyber Security Centre (NCSC) website and cybersecurity podcasts in order for them to be able to stay updated with new, current, security issues. The research team also ensured that details of new scams were communicated to the CyberGuardians via email, so that they might disseminate this information to their communities of *CyberCitizens* – or members of the public who received advice or help from the CyberGuardians.

3.3.1 Quality Control of Security Advice

To ensure that good cybersecurity practice was shared by CyberGuardians we highlighted a range of possible advice, from "gold standard" (e.g. using a password manager), to simple guidance that can

substantially improve poor practice (e.g. using three random words for creating password [27]) during the training. The research team was available at any time to answer any questions, and a number of CyberGuardian-led sessions were monitored by the team and project partner for quality control. The research team also carefully analysed the survey responses from all participants in order to spot any miscommunications in advice. In general, the CyberGuardians adopted Ken's mantra of *"If you don't know just say you don't know but I'll take a note, find out and get back to you"*.

On the other hand, the advice that was passed on by CyberCitizens to other people in the community cannot be verified. There is a risk that such information could mutate with sharing [18], but we suggest that generating more awareness around cybersecurity threats and protections is a positive outcome within communities that typically are not aware of – or do not discuss – such topics.

3.4 Data Collection and Analysis

We obtained a wealth of insight from the CyberGuardians' behaviour through a range of qualitative and quantitative sources. See Figure 1 for a timeline of when the data was collected.

3.4.1 Qualitative Data Collection

The qualitative data that was collected included group discussions between new CyberGuardians during their initial recruitment workshop, and from two sharing sessions post-training (one in person and one online). This data details their expectations for the initiative and the challenges that they anticipated, as well as reporting on what had worked well following training. We also conducted interviews with each of the CyberGuardians towards the end of the nine-month period to explore their experiences of taking part. CyberGuardians were asked to keep track of their interactions with community members who received advice or help (named '*CyberCitizens')* using a journal with pre-defined questions. They were further asked to log their preparation and reflective thoughts within this journal. Finally, a number of CyberGuardians audio recorded their delivery of formal cybersecurity sessions to groups of CyberCitizens. We used these recordings to better understand the communication techniques employed by the CyberGuardians and to determine the types of questions that CyberCitizens posed. In addition to the qualitative data collected from the CyberGuardians, we conducted interviews with 13 CyberCitizens to better understand their motivations for engaging with the CyberGuardians, their experiences of doing so, and any resultant changes in their cybersecurity behaviour. CyberCitizens were selected based on their availability and were recruited by emails sent by our project partners and the CyberGuardians themselves.

3.4.2 Quantitative Data Collection

The majority of quantitative data reported here came from an anonymous online survey that was distributed to both CyberGuardians and CyberCitizens. This survey was passed on to CyberCitizens by the CyberGuardians within two weeks of their interaction. The purpose of this survey was to approximate how many people had benefited from the information (i.e., "how many people have you shared this information with") and to understand whether any cybersecurity behaviours as a result of the interaction. Other questions enquired about what aspects were deemed the most important following these discussions.

The CyberGuardians were required to fill out a confidence questionnaire following the initial workshop, before each training session, before each sharing session, and prior to their final interviews (see Figure 1). The purpose

of this questionnaire was to understand what key cybersecurity knowledge the CyberGuardians retained at different stages, but also to measure how their confidence in key cybersecurity skills (e.g. password composition, scam detection, and sharing this information with members of the general public) changed throughout the duration of the initiative.

3.5 Methodological Limitations

We collected a range of data throughout the nine-month period. While this data was invaluable in understanding the mechanics and outcomes of this novel method, we were only able to collect insights from CyberGuardians and known CyberCitizens who were willing to engage with us. This, in practice, means that the responses we report may be skewed towards positive experiences as individuals who did not see the value, or did not follow through with changes, may not have been inclined to complete a survey or agree to an interview.

Many interesting insights were challenging to capture first-hand, so we had to rely on a triangulation of CyberGuardians and CyberCitizen feedback. For example, informal interactions with family or peers (e.g., during a family meal) were particularly difficult to capture as CyberGuardians did not always remember everyone they had passed on cybersecurity knowledge to and did not record such interactions in their journals. These discrepancies were clear when comparing the journal entries and the final interviews, where CyberGuardians remembered smaller interactions that they had either forgotten to write down, or simply did not believe were interesting to the research team as they were short informal chats with known people. In the future, we should consider how we can capture these interactions seamlessly without inconveniencing both CyberGuardians and CyberCitizens.

4 GENERAL FINDINGS

The findings are structured as follows: first we discuss the characteristics of CyberCitizens. We then go on to report on the methods that the CyberGuardians chose for sharing cybersecurity best practices with their communities. Finally, we present insights from the deployment that can help improve similar initiatives in the future. Insights from the CyberCitizens are presented throughout the findings.

4.1 CyberCitizens

The CyberGuardians (n=13 completed the anonymous survey) reported discussing cybersecurity behaviours and best practice with approximately 470 unique citizens (average per Guardian: 34) over the course of the nine months. While we have taken into consideration workshop participants (i.e., people that multiple CyberGuardians may have counted), it is still possible that some CyberCitizens may have encountered multiple CyberGuardians independently. Equally, as previously established, many informal interactions may have gone unrecorded due to the CyberGuardians failing to register these in journals and notes. As such, establishing an accurate reach for the information is challenging, and a clear limitation of such initiatives.

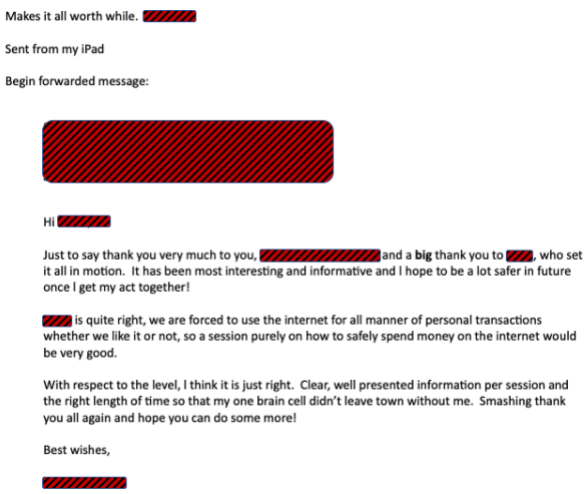
Additionally, the citizens who responded (n=113/470) reported sharing this cybersecurity advice with approximately 350 other people (average per person: 3). Once again, it is very challenging to assert whether these were unique people, and whether the integrity of the advice was maintained in retransmission. It is also possible that some of the basic tips could have been passed on to others in the community so the reach could be considerably higher than reported here.

The CyberCitizens were predominantly older adults, although advice reached a small number of younger people (approximately 4% were under the age of 40). The age range of CyberCitizens was 12 to 89 years old, with 60% of respondents being in the 70-80 age category and predominantly female (59%). 113 CyberCitizens completed the survey, with the majority being those who engaged in formal interactions (e.g., workshops or arranged one-to-one sessions). However, 37% explicitly reported being friends or family of the CyberGuardian and having interacted on an informal basis.

The two most common reported takeaways from conversations with the CyberGuardians were the need to be "aware" when dealing with online communication (87%) and the need to have unique and strong passwords (83%). The importance of password managers, data backups, awareness of phone scams, and two-factor authentication made up a more modest 32% of comments. Nearly half of our respondents (44%) reported changing at least one password, with 73% making a commitment to improve their behaviours.

"I usually have one password for everything. But it's literally every possible website I have one password. But now I have two!" (CyberCitizen)

Of course, cybersecurity behaviours can only be considered a spectrum, and while the CyberGuardians were able to persuade some Citizens to adopt best practice, others, like the one above, focussed on improving their behaviours one step at a time. She later explained how she changed her email password to a different code once hearing about how passwords are guessed by computer programs very quickly.



Makes it all worth while. [redacted]

Sent from my iPad

Begin forwarded message:

[redacted]

Hi [redacted]

Just to say thank you very much to you, [redacted] and a **big** thank you to [redacted], who set it all in motion. It has been most interesting and informative and I hope to be a lot safer in future once I get my act together!

[redacted] is quite right, we are forced to use the internet for all manner of personal transactions whether we like it or not, so a session purely on how to safely spend money on the internet would be very good.

With respect to the level, I think it is just right. Clear, well presented information per session and the right length of time so that my one brain cell didn't leave town without me. Smashing thank you all again and hope you can do some more!

Best wishes,

[redacted]

Figure 4: CyberCitizen feedback received by Ken and forwarded to the research team.

The large majority of respondents reported improving their awareness of online scams (80%), although this is something which is difficult to quantify. A specific example of heightened awareness came from a CyberCitizen who attended a formal workshop session.

"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." (CyberCitizen).

While the majority of interactions were set up by the CyberGuardians or the CyberCitizens themselves, we did see instances where citizens who were aware of the CyberGuardians brokered conversations with other citizens. For example, one CyberCitizen set up a three-way meeting with a CyberGuardian and invited their friend because *"this guy was just using the same password for everything"* (CyberCitizen). This then resulted in the CyberGuardian explaining the importance of good passwords and discussing techniques on how to create and manage them.

The feedback received from CyberCitizens was unanimously excellent. Feedback was received via email (see Figure 4), via formal feedback sheets after events (n=21), through the online survey (n=113), and directly through selected phone interviews (n=11). CyberCitizens emphasised the importance of having *"easy to understand advice"* that is *"interesting and informative"*, while having *"accessible"* knowledgeable peers encourages their engagement with the content.

4.2 CyberGuardian Confidence

The CyberGuardians completed the same questionnaire asking them to rate their confidence on a number of different cybersecurity topics on 5 different occasions over the 9-month period. Here we report on the baseline measure (taken before their first training session) and their final questionnaire 8 months following the training. This questionnaire consisted of eight questions on different cybersecurity behaviours and asked respondents to select their confidence level on a 5-point Likert scale (1=*Not At All Confident* to 5=*Very Confident*). Participants completed the baseline measure before their first training session, and the final questionnaire 2-3 days before taking part in the final sharing meeting.

We focus on the two key questions that are relevant for a CyberGuardian: 1) How confident are you that you can protect yourself online? and 2) How confident are you in your ability to help others understand cybersecurity issues? As can be seen in Table 2, the confidence of the CyberGuardians appeared to improve over time when we look at those who answered "confident" and "very confident".

Table 2: Confidence Questionnaire Scores (% of participants scoring Confident or Very Confident).

Question	Baseline (n=14)	8 Months After (n=9)
How confident are you that you can protect yourself online?	35.70%	100%
How confident are you in your ability to help others understand cybersecurity issues?	28.5%	87.5%

We were unable to run any parametric statistical tests on these numbers given the small number of participants (we trained 14 CyberGuardians, and 9 completed the final questionnaire), but we can see a positive trend towards these individuals improving their confidence over the course of the initiative.

In the final questionnaire, we asked the CyberGuardians whether their confidence in cybersecurity knowledge has improved by helping others. 62.5% answered that their confidence had improved a lot, while the remaining 37.5% answered that their confidence had improved a little. Overall, we see a positive trend where attending the training sessions and then engaging in sharing that information with peers improved the

subjective confidence of the CyberGuardians. As we report below, their own cybersecurity behaviours also improved during this time period. Here, we acknowledge that only active CyberGuardians completed the final questionnaire, and thus if responses of those who did not engage with the role are taken into consideration the improvement in confidence may not be as pronounced.

4.3 Behaviour Change Role Models

The CyberGuardians reported a range of methods for sharing cybersecurity best practice, however they consistently ensured that they improved their own behaviours before communicating with CyberCitizens. The most common improvement was changes to passwords to make them more unique and strong – typically employing the three random words approach [27]. For example, Ken documented the process that took him *"15-20 hours to change passwords on 120 sites"* before eventually adopting a password manager. Other CyberGuardians took further measures, like Amelia, who focused on making sure her router was secure from unauthorised access by guests, and Charles, who took it upon himself to create offline backups of all his files. All CyberGuardians became more aware of potential phishing scams, as demonstrated by regular email correspondence with the research team forwarding messages they had received, or that CyberCitizens had forwarded onto them (e.g., see Figure 5).

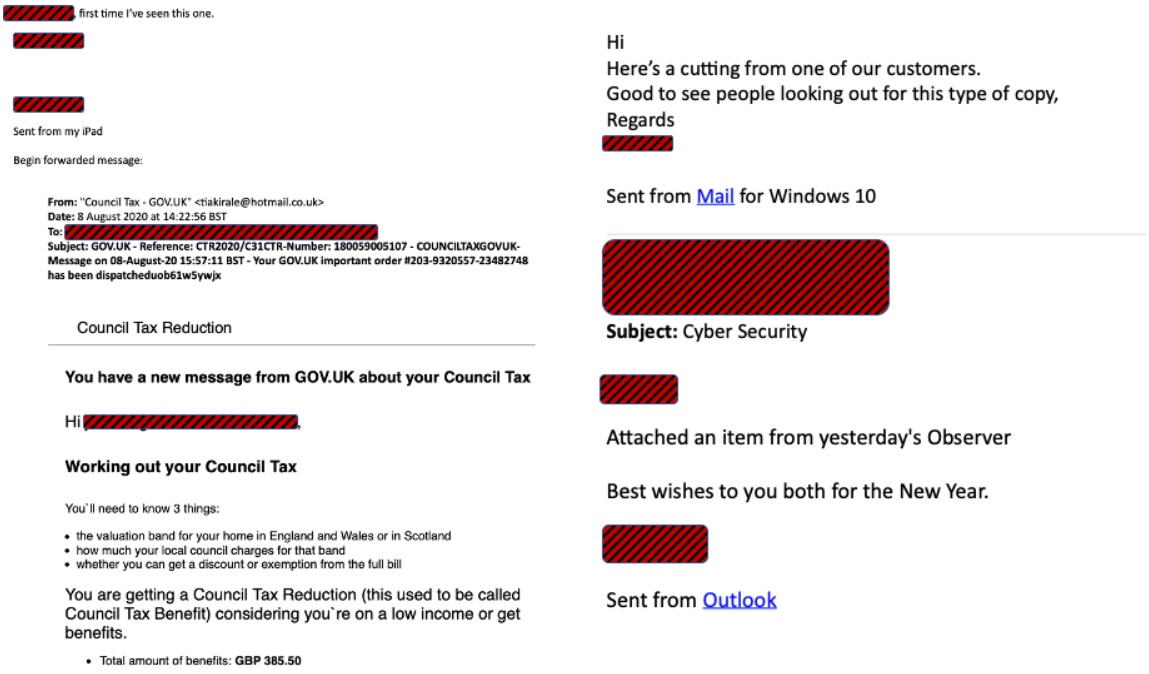


Figure 5: Email correspondence with CyberGuardians. Left: A CyberGuardian sharing a new phishing message with the research team and the other CyberGuardians; Right: Another CyberGuardian passing on an email received from a Citizen to the research team.

Following the training, most CyberGuardians became more engaged with cybersecurity, as demonstrated by frequent correspondence with the research team forwarding useful cybersecurity information (e.g. from

newsletters) or examples of scams (see Figure 5). However, these CyberGuardians explained that they had not changed their information seeking habits, but that instead they appeared to be more aware of scams and cybersecurity news since taking part in the training.

"I think since, I am generally thinking about scams and there has been a lot in the media in the past 12 months. Unless, I'm just more aware so maybe there was that. Since there was [initiative], I am more aware of it" (Joe)

When discussing this phenomenon with one of our project partners, he recalled several examples of when CyberCitizens had contacted him with news articles and newsletters themselves, suggesting that simply discussing cybersecurity with local peers can lead to a more informed and aware community.

"The CyberGuardians are also far more proficient in explaining how to recognise scams on the phone and online: I am really surprised how confident they are about talking about this subject now. It is encouraging that all the CyberGuardians stuck with the training through all the workshops, and the enthusiasm demonstrated to spread their new knowledge amongst their peers after the sessions and is still just as strong after a few months of implementation" (Project Partner)

Our project partner emphasised the importance of the ways the CyberGuardians can empathise, communicate, and influence their peers, further strengthening the impact of the initiative.

4.4 Methods for Sharing Cybersecurity Best Practice

The CyberGuardians reported success in spreading cybersecurity best practice and observing behaviour change in CyberCitizens. These changes in behaviour were supported by anonymous surveys completed by CyberCitizens. However, as with all behaviour change interventions, not all CyberCitizens accepted advice or changed existing behaviours.

"You can only lead a horse to water – you can give them the information but whether they do anything about it is up to them" (Tom)

Most CyberGuardians were pragmatic about this, recognising that their role was not to *"sell anything to them"* (Joe), but rather to help them make an *"educated choice"* (Daniel).

4.4.1 Opportunistic Information Sharing

The majority of CyberGuardians reported that raising cybersecurity as a subject in everyday conversations was an effective way of conveying information to peers. For example, Terry started conversations about passwords with other grandparents in the school yard while waiting for grandchildren, while Ken raised it at the pub while with friends. This method appears to be one of the most effective for communicating with CyberCitizens and subsequently driving behaviour change, something which is not surprising given that we know that most people learn about cybersecurity in an opportunistic manner, rather than actively seeking information [13]. Terry's acquaintance changed a number of his passwords after three conversations in the school yard, while Ken's friends began to forward him potential scam emails.

In addition to behaviour change, we observed how opportunistic cybersecurity discussions could lead to the spread of cybersecurity awareness and best practice amongst CyberCitizens. For example, Terry came across an acquaintance who had just received a text message from her mobile phone provider alerting her about a missed payment. Terry identified this message as a phishing message and advised her to call her mobile provider directly on a trusted number to verify the content of the message. This was indeed a phishing message,

and she immediately communicated this to friends who were on the same mobile network. This informal information sharing and attack prevention has been picked up by one of our project partners as a key aspect of this initiative.

"…they seem to be more efficient, the informal meetings or informal sessions with people that they just been at the same venue or the same walk, and they just got into a conversation about security or the internet or whatever... I think they tend to like that informal contact, when they're not under any sort of pressure, you know, they're in a social situation as well at the same time so they can open up without being guarded" (Project Partner)

Our project partners regularly reflected on how everyday CyberCitizens are more open to learning about cybersecurity tools and behaviours under social and less structured situations, and how this method gets the information across to people who would otherwise not be exposed to this knowledge.

"I wouldn't sign up to go to security events or training or anything like that. I don't have the time or the interest, to be honest. That is why it was great to talk with Ken about it, otherwise I would have no idea!" (CyberCitizen)

This resonates with previous work demonstrating that informal environments can be ideal for fostering learning in communities [42], thus creating these informal environments is of great importance and something to consider in the future.

4.4.2 Workshops with Groups

While initially most of the CyberGuardians shared best practice with close friends and family, some chose to share their knowledge in group sessions. For example, 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 (for more details on their preparation and use of materials for workshop delivery see [30]). This practice of using group workshops to disseminate advice to peers was later adopted by other CyberGuardians following the first sharing session and were delivered online due to the national COVID-19 Lockdown. On average, workshop sessions were delivered to 15 citizens per session, with a total of 103 citizens attending formal workshop sessions over the course of the nine months.

Preparation for these larger-scale workshops was time intensive, with the CyberGuardians reporting spending an average of 3 hours per session modifying the presentation materials to suit their audience. This poses an interesting question around what the most effective use of a CyberGuardian's time might be – the delivery of material to a large number of willing people (e.g., workshop) or more informal one-on-one conversations that may reach citizens who are typically not exposed to such information.

4.4.3 Social Media

Most of the CyberGuardians decided to share cybersecurity best practice with peers via person-to-person interaction, be it within a physical setting or online through videoconferencing. This was due to a combination of them not using social media regularly or at all. They also believed that peers who would most benefit from this advice would not be on social media, or would not believe the advice from a social media source.

The two more technically competent CyberGuardians used social media to spread relevant cybersecurity information to friends and family. One of them (Tom) initially tried face-to-face contact with members of his community by developing and distributing a poster campaign around his local library. After failing to get any response to this campaign, he switched to Facebook as a method for disseminating cybersecurity best practice

to others. Following this switch, there was evidence of his advice being cascaded out by friends and family into the wider community and beyond (see Figure 6). The messages predominately came from the materials provided to the CyberGuardians by the research team, which were then reframed and tailored to their audience.

4.4.4 Online Communications

All of the CyberGuardians were comfortable using email for everyday communications (verified by recruiting via email). As a result, it is not surprising that most of the CyberGuardians used email to pass on security tips and warnings about the latest scams to friends, family, and other CyberGuardians. It should be noted, however, that this form of information spreading only became commonplace once Covid-19 Lockdown restrictions were imposed on the country which prevented CyberGuardians from meeting others in person.

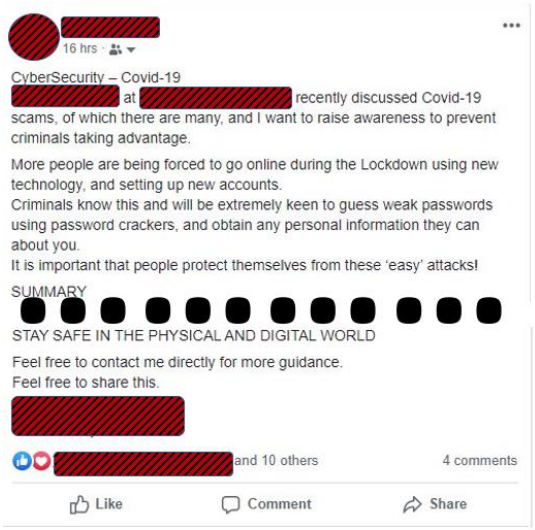


Figure 6: Example Social Media Post by Tom, Sharing Cybersecurity Advice.

Interestingly, email communications were only reported with individuals or groups that the CyberGuardians were already familiar with. Targets for email updates included existing interest groups, people who had previously attended cybersecurity workshops sessions, and fellow CyberGuardians. Phone calls were attempted, however these had mixed reactions from the CyberGuardians due to the difficult nature of communicating complex information without having any visual indicators and no established rapport.

4.5 Technical Knowledge

Throughout the nine-month period, it became clear that having technical knowledge and/or having worked in an IT intensive role was **not** a pre-requisite for being a successful CyberGuardian. As previously mentioned, we did not recruit CyberGuardians based on their IT technical knowledge, although coincidentally two participants had an IT background. Having good IT knowledge, and having a reputation for such, could present an opportunity to share cybersecurity best practice, as previously reported [16]. For example, Tom was regularly asked to help fix IT issues by peers and he used these opportunities to offer advice.

"I mean, my brother in law, when he brought his laptop over, he was having a problem finding - I think someone had sent him videos on WhatsApp but he couldn't find them - it might have been on his phone - but that was the problem he came with but then of course you have to get into the phone and that's my usual route in as soon as you put in the password, I talk about how secure it is" (Tom)

While this can be a promising avenue for offering cybersecurity advice, in circumstances such as this one it is likely that the citizen is already suffering from an incident. This highlights the importance of ensuring that CyberGuardians are lay members of the community, so that the advice can be pre-emptive as well as remedial.

Our other tech savvy CyberGuardian Kay – who had experience of building sophisticated IT networks for the public sector and commercial companies – highlighted an issue that she had faced. At times she found it challenging to communicate using the right language that citizens could understand.

"Sometimes I know things well enough to function myself but I can't actually pass that on in a good way to somebody else and I think it's really important if you are going to do the CyberGuardian training that you are clear and able to put over what you're trying to say because you could actually make things worse if you complicate things for people" (Kay)

This difficulty communicating technical concepts with lay users is not surprising given that many older users struggle to understand the cybersecurity language [28], and signposts to the need for recruiting lay users for such initiatives.

4.5.1 Training as a Journey for Relatability

Most of the CyberGuardians began the training knowing very little about the subject. For example, Ken was initially worried that he was going to be *"the dummy in the class"* during training because he was *"not a great technophile, having come to the (computer) party late"*. However, he became an active CyberGuardian who participated in both formal and informal information sharing with CyberCitizens, predominantly relying on slipping cybersecurity into casual conversations such as when people ask him what he has been doing lately.

"I think it's finding the right level to come into the conversations, I don't tend to advertise and push it saying I've been on this course. Some people say you have an interest – so people ask but I tend not to push. Well I don't think I am – I prefer to be asked rather than push it" (Ken)

Ken's approach included using his own experiences of changing behaviours to motivate others to do the same. For example, Ken freely admitted to CyberCitizens that he used the same password for all his online accounts before his cybersecurity training – something that his peers could relate to. Other CyberGuardians also used their own experiences of the training and subsequent behaviour change to establish a rapport with the citizens they helped.

"[Ken] told me how he'd done it, and he kept a list hidden away somewhere very safe for the first few weeks, just in case. Now it's not a problem, but that list was reassuring while he got used to it. I think it's those helpful hints that make it a lot easier to make the jump… and I can ask him again if I get in trouble!" (CyberCitizen)

This sharing of experiences and techniques was particularly effective and allowed for citizens to feel understood. Consequently, the CyberGuardians were able to provide usable advice that was likely to be accepted due to their nature as personal security stories [40].

4.6 Wellbeing

4.6.1 Community Wellbeing

Lifelong learning has been identified as key in improving community wellbeing amongst older adults [25]. In this case, having ready access to individuals who could provide cybersecurity support could be beneficial for older citizens in relation to their overall wellbeing. Scams can be traumatic for older people [1], thus, being able to prevent these incidents could contribute to the general wellbeing of older members in the community.

"It's a really great service, you know? If they were not around I probably would have just left it alone" (CyberCitizen).

The CyberCitizen above goes on to explain how she followed up on some smaller queries due to having access to knowledgeable others. However, had support not been accessible, this could have developed into a security incident. In addition to facilitating conversations about cybersecurity that typically are not openly discussed [41], the ability of this project to pre-empt cybersecurity incidents is a valuable aspect of the CyberGuardians initiative.

4.6.2 CyberGuardians' Wellbeing

In addition to benefitting the community, it was clear that the CyberGuardians saw a personal benefit beyond their initial desire to learn more about protecting themselves online. In many cases we saw how CyberGuardians reported feeling good about helping others especially when their advice led to cybersecurity habit changes from the people they helped. This aligns with previous work looking at Cybersecurity Advocates, which highlights the importance of cultivating self-worth by helping others as a key motivation for continued engagement [17].

"…It's good to learn for yourself and good to help other people be more security savvy and safe." (Terry)

Most of our CyberGuardians reported befriending their fellow CyberGuardians – people in similar social circles that they may have recognised previously, but did not know very well. The CyberGuardians formed their own working groups – predominantly based on their residential locations – and used these as a support group for reinforcing key concepts amongst themselves (e.g., discussing scams) and motivating one another to continue sharing cybersecurity best practice. In essence, the CyberGuardians formed a community of practice [43]. For example, four CyberGuardians met regularly to share their experiences of the initiative and discuss any news or threats that citizens in their communities should be aware of. This is in line with previous research exploring how members of the general population make sense of cybersecurity information [12], and in maintaining motivation as a Cybersecurity Advocate [17], although this had not been observed with older users previously.

"I think being part of a group of similarly aged people, some of whom are more IT aware than I am and less so. A varied group but, being able to see that and be part of that. Some people are perhaps less familiar and they are less IT aware. I think that is quite important in the training that you are sharing it with a group who didn't have all of that when they were growing up. So for us, it is something we didn't just assimilate through our teenage years, it's something that came along later on and to be sharing that with people in this situation is one of the most helpful things." (Jane)

Amelia further benefitted by using the initiative to make friends with the CyberCitizens as well. She had recently relocated to the area and had no family or a social network nearby. During the COVID-19 Lockdown

period, she scheduled online ‘catch ups’ with her CyberCitizens and talked about *“non-cybersecurity things”* providing further evidence of the initiative contributing towards good wellbeing for those involved.

4.6.3 Supporting CyberGuardians

Although we observed many instances of improved wellbeing through the CyberGuardians initiative, it is important to note how inadequate support can also adversely affect mental wellbeing. David was the furthest participant and travelled approximately 60 miles to attend the training with plans to help people in his local community. Once the training concluded however, he spoke with family and friends which proved to be *“a mixed bag”*. Specifically, David approached a few citizens with advice but found some resistance to his advice, in particular around being proactive and changing passwords. David did not have any CyberGuardians locally to discuss these struggles with, and ultimately ceased offering cybersecurity advice to friends and family due to decreased confidence in his skills.

“I feel disappointed with myself because it was something I was thinking of doing and wanting to do. When I did try, back in [home city] I felt light years away from your expertise in Newcastle.” (David)

During the final interview, David admitted the need for a support network and how having access to other CyberGuardians would have benefitted both his confidence and his practice. Thus, it is important to consider how best to support CyberGuardians that may not be co-located, either through appropriate recruitment (e.g., a “buddy” system) or proactively throughout the duration of the initiative. However, further work is needed to better understand the most effective methods to form and support CyberGuardian working groups (as described in 4.6.2). For example, most CyberGuardians were very clear that they did not wish to be forced into groups and would prefer for these to happen organically, while on the other hand others like David were unable to form a group and benefit from best practice sharing with peers.

Several CyberGuardians discussed the possibility of developing a website to host CyberGuardians materials and to facilitate both internal and external communication. Having a central location where CyberGuardians can communicate with each other, and access all resources, can ensure that as many CyberGuardians as possible are benefiting from best practice sharing. Additionally, having all resources publicly available was seen as an ideal solution to reduce the personal effort involved (e.g., they can direct CyberCitizens to the website for the resources, rather than emailing these). The creation of this online ‘hub’, while of particular benefit to remote CyberGuardians, could also facilitate the training and interactions of CyberGuardians when they are unable to be co-located, but more research is needed to understand the design characteristics of such a platform.

5 DISCUSSION

This paper demonstrated the acceptability and feasibility of a community-driven information sharing initiative where older adults were able to learn about cybersecurity best practice and share that effectively with their peers to create more secure communities. While we have focused on the context of cybersecurity given the well-documented issues that older people face (e.g., [1]), this blueprint can be used for other digital contexts, and extended to non-digital contexts. This approach is particularly effective where “expert” information is needed and citizens may not be aware where that information resides, or may need help putting specialised information into context, or where open discussions about a specific subject are uncommon. In the digital context this includes topics such as privacy and mis- or dis- information. Other contexts include mental health or sexually transmitted diseases (both a growing concern in older adult communities, e.g., [8,45]).

Here, we summarise the key findings in relation to effective message dissemination, discuss issues that should be considered for the sustainability of similar initiatives, and present general guidelines for recruiting and training these Guardians who can then share best practice information about an array of topics.

5.1 Spreading Cybersecurity Best Practice in the Community

Through a 9-month real-world deployment, we observed a number of key insights into how older CyberGuardians conducted their information sharing with peers. Unsurprisingly for this age group, face-to-face sharing was preferred, but some digital sharing took place when necessary (e.g., during Lockdown).

Informal opportunistic advice sharing was common amongst all CyberGuardians, and this could be the most effective way to spread cybersecurity best practice into the community – both young and old – and mirrors some prior work suggesting the effectiveness of informal learning environments [42]. This approach also increases the likelihood of reaching older citizens who would otherwise not have access to this information – i.e., those that are less inclined to attend training sessions. Specifically, using their own experience of changing behaviours since the training appeared to be effective, something which can be traced back to security storytelling amongst peers [40]. In this case, however, CyberGuardians fulfilled the roles of peer and authority simultaneously, and this gave them a meaningful role in society which had positive impacts on their mental wellbeing.

Perhaps most importantly, we started to see evidence of cybersecurity chat being normalised within these communities, with CyberCitizens keeping in touch with the CyberGuardians and continuing the cybersecurity conversation. Importantly, we saw how the CyberCitizens discussed this advice with other peers, further spreading the information within the community. People typically do not openly discuss cybersecurity [41] which ultimately leads to lower awareness and can facilitate attacks [9] This is also typical of other difficult subjects (e.g. social isolation [33], privacy, etc.). This type of initiative has started to demonstrate how we can generate interest and engage communities in conversation and overall awareness of such topics.

Finally, we have built on prior work examining older adults' cybersecurity information seeking behaviours which highlights the issues that this demographic faces in accessing available, knowledgeable individuals [28]. The CyberGuardians initiative has presented some preliminary evidence that facilitating access to these individuals can in practice improve the cybersecurity behaviours of older adults. Our work also practically supports well-known theoretical work suggesting that the presence of capable guardians can help deter crime [9] in a digital context. While improved cybersecurity awareness and improved cybersecurity behaviours cannot guarantee the prevention of cyber attacks, they are an important step towards reducing the number of opportunistic online attacks that are successful.

5.2 Sustainability Challenges

5.2.1 Safeguarding

Our project partners played a critical role in the success of the CyberGuardians initiative, from supporting recruitment to, critically, safeguarding both CyberGuardians and CyberCitizens. Given the nature of the community groups we engaged with, our partners were able to assist in the identity verification of CyberGuardians and CyberCitizens. Specifically, their promotion of the initiative served as endorsement of the CyberGuardians' validity and character. Equally, when CyberCitizens contacted our partners for cybersecurity help, any referrals reassured our CyberGuardians of the citizens' belonging to the group (i.e., the community).

Of course, when CyberGuardians approached citizens opportunistically there was no verification process, but these typically involved known people in known environments.

It is important to consider the most appropriate methods for verification of both CyberGuardians and CyberCitizens. It is not difficult to imagine attackers claiming to be CyberGuardians in order to victimise CyberCitizens. This was a clear concern from the CyberGuardians' perspective when discussing the expansion of the initiative but was also a problem from the CyberCitizens' perspective demonstrated by the lack of engagement with opportunistic library posters. As such, in the short-term, community partners will play an essential role in these initiatives for vetting participants, although of course reliance on non-academic partners and services like the UK's Disclosure and Barring Service rely on prior exposure of a criminal background.

Equally, it is important to consider how to safeguard the CyberGuardians from attackers posing as CyberCitizens. This was a concern for some CyberGuardians who agreed to meet with unknown CyberCitizens, and was typically addressed by agreeing to meet in a public trusted space (e.g., at our project partners' premises or at a well-known café). At this point we see both the value and the limitations of an initiative like the CyberGuardians who disseminate cybersecurity information to their communities: value in how members of the community can be comfortably reached and reassured, but equally challenges in expanding the scheme to new communities.

5.2.2 Expansion Considerations

We have demonstrated how the CyberGuardians model can promote cybersecurity behaviour change and improved awareness in communities through informal and relatable help from peers. Additionally, we have supported previous work in demonstrating how general wellbeing of older users can be improved through civic participation (e.g., [34,36]). However, it is difficult to imagine how such an initiative can be organically expanded beyond the CyberGuardians' communities without the significant safeguarding concerns covered above. One of the key motivations, and reasons for success, was making relatable community members available to citizens so they can freely discuss cybersecurity concerns, or to act as pre-emptive best practice sharing. If these CyberGuardians were encouraged to approach members of other communities, they might no longer be relatable and the informal nature of interactions could be disrupted. Additionally, the verification of Guardians and Citizens would be more complex with neither party having any a-priori context of one another, which could lead to pushback from these CyberCitizens.

As such, we posit whether the future for these initiatives lies in identifying non-academic partners in communities of interest who could assist with the recruitment and support of individuals to be trained as CyberGuardians. Of course, this leads to important questions such as how do we identify these communities, and how do we ensure that the appropriate safeguarding is in place?

5.3 Towards the Recruitment and Training of Guardians

It was clear that the success of the initiative was in part due to the endorsement of the programme by an authority. However, it is unclear which authority was the most important in this success. As discussed previously, the endorsement of our partner organisations facilitated the recruitment of the CyberGuardians and the initial retention. On the other hand, a number of CyberGuardians explained how the endorsement from the University played a major role in both their initial involvement and confidence in sharing the cybersecurity information. As Terry explains, they trusted the information from the programme as *"the University is not looking*

to sell you anything". Ultimately, much of the advice that the CyberGuardians were trained on, and shared with their peers, originated from academic research but also the official UK NCSC citizen advice. Some CyberGuardians namechecked the NCSC when sharing information to give it extra weight. Even though CyberGuardians had not expressed an importance for this government accreditation in their initial feedback, clearly this has benefits. The CyberGuardians approach, underpinned by the official advice from the NCSC website, highlights the importance of a trusted source of information and also raises the awareness of this information in CyberCitizens. It is important to consider how best to incorporate such initiatives to ensure both CyberGuardian and CyberCitizen buy in.

Additionally, below we report on other insights obtained through conversations with the CyberGuardians on how to improve both the training sessions and the recruitment for these types of initiatives.

5.3.1 Training

The CyberGuardians were trained on cybersecurity best practices around password management, scam detection, and software protections and were delivered in a platform-agnostic way. However, it was clear that platform was a concern for many CyberGuardians. For example, more than half of the CyberGuardians were Apple users and were concerned about helping Windows and Android users, despite advice being the same (e.g., using three random words for generating strong and unique passwords). One Windows user was uncomfortable with helping an Apple-using citizen due to having never used an Apple product. This was a common concern that should be addressed in the training – either by providing some cross-platform examples (e.g., Android, Mac, iOS, and Windows screenshots of browser URL bars) or re-emphasising that the advice is the same across any device used. In a non-technical context, this could equate to **considering the inclusivity of the advice** to ensure that different peer groups or populations are accounted for. Of course, if possible, this is something that can also be addressed in the recruitment to ensure that all possible viewpoints are covered.

Similarly, the majority of CyberGuardians perceived that their peers were more "tech savvy" than themselves and this belief has persisted throughout the initiative. Believing that others are more knowledgeable than oneself is a known cognitive bias when more expert knowledge is gained [23], and as such it is important to reassure the CyberGuardians that their level of knowledge is more advanced that a typical peer. This can be done through **scenario-based training** where they are asked questions either by the research team, other CyberGuardians, or volunteer CyberCitizens to alleviate some of these concerns and build their confidence on how to respond to some common queries before they begin their active roles. Some **training on communication and presentation skills** may also be beneficial, although more work is needed in this space to understand what this would look like without affecting their relatability. The use of **technical demonstrations** to illustrate risks appears to be an effective method to encourage behaviour change, both for Guardians and Citizens. Equally, providing the Guardians with **base materials that can be edited** appears to be promising, as many Guardians reused these training materials in their sharing. As such, designing these **materials to be simple and shareable**, in addition to signposting to reliable official sources, can facilitate the Guardians in sharing quality information, as well as Citizens passing on that information correctly. It should be acknowledged, that desire or ability to run formal communication sessions is not necessarily required, and less formal sharing of information may be equally effective. More research is required to explore the different ways information can be shared between peers to effect behaviour change.

Finally, it was clear that the CyberGuardians highly valued the social aspects of the training sessions, and the informal conversations prior to sessions and during coffee breaks. In the final interviews, when discussing the potential for training new Guardians online, at the time the CyberGuardians were adamant that the **in-person aspect was essential when first beginning the training to establish a group identity**. As our worlds move increasingly online, and we see group video chats becoming more normalised, it is unclear whether Guardians' views would shift towards the acceptance of these initial sessions being delivered remotely in the future. We require follow-up research to understand whether there have been attitude shifts resulting from the change in social norms, particularly considering the ways in which we can offer opportunities for these embodied social interactions online.

5.3.2 Recruitment

We also note that while being an ex-IT professional can be an advantage in some ways (e.g., opportunities to discuss best practice when asked to fix issues), not having previous knowledge of cybersecurity but having established networks and/or willingness to help others can be equally, if not more, important. When recruiting future Guardians it will be important to **ensure that their desire to help others, and their existing network is adequate rather than focusing on existing topic knowledge**. An existing network is not essential as having a role and purpose may give older adults who have become isolated an opportunity to re-engage with their community. Additionally, using their own learning experiences can be effective for encouraging behaviour change in citizens.

The primary motivation for the CyberGuardians attending the initial training sessions was so that they could learn how to protect themselves online. However, the role within the community can help towards having a sense of purpose and re-engaging with the community which provides additional wellbeing benefits [25]. Thus, **it is important to be clear about what the personal benefits of such initiatives could be** (e.g., [32]), both as individuals, but also longer term for the community.

6 CONCLUSIONS

As more older adults engage with online activities, it is important that they embrace online technology in a safe way. We have reported on a community-driven initiative where 14 older adults were trained to become CyberGuardians and help their peers become more knowledgeable about cybersecurity threats and protections. We have shown how training older citizens as CyberGuardians, regardless of technical knowledge, can result in cybersecurity behaviour change for both the CyberGuardians and the CyberCitizens they interact with, while also having positive effects on their overall wellbeing. We have also seen how such initiatives can normalise the discussion of difficult and technical concepts (in this case cybersecurity) within communities and have suggested how such Guardians can be recruited and trained for other cyber-topics such as disinformation or privacy. In addition, we believe this approach could be extended to non-technical issues which are difficult to discuss, such as poor mental health or sexually transmitted diseases among older citizens.

ACKNOWLEDGMENTS

This work was funded by 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. Lucy R. Betts, Rowena Hill, and Sarah E. Gardner. 2019. "There's Not Enough Knowledge Out There": Examining Older Adults' Perceptions of Digital Technology Use and Digital Inclusion Classes. *Journal of Applied Gerontology* 38, 8: 1147–1166. https://doi.org/10.1177/0733464817737621
5. Michael T. Bixter, Kenneth A. Blocker, and Wendy A. Rogers. 2018. Enhancing social engagement of older adults through technology. In *Aging, Technology and Health*, Richard Pak and Anne Collins McLaughlin (eds.). Academic Press, San Diego, 179–214. https://doi.org/10.1016/B978-0-12-811272-4.00008-7
6. Carlene Blackwood-Brown, Yair Levy, and John D'Arcy. 2019. Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective. *Journal of Computer Information Systems* 0, 0: 1–12. https://doi.org/10.1080/08874417.2019.1579076
7. Leonieke C van Boekel, Sebastiaan TM Peek, and Katrien G Luijkx. 2017. Diversity in Older Adults' Use of the Internet: Identifying Subgroups Through Latent Class Analysis. *Journal of Medical Internet Research* 19, 5. https://doi.org/10.2196/jmir.6853
8. Centers for Disease Control and Prevention. 2018. *Sexually Transmitted Disease Surveillance 2017*. U.S. Department of Health and Human Services. Retrieved from https://www.cdc.gov/std/stats17/2017-STD-Surveillance-Report_CDC-clearance-9.10.18.pdf
9. Lawrence E. Cohen and Marcus Felson. 1979. Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review* 44, 4: 588–608. https://doi.org/10.2307/2094589
10. 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
11. John D'Arcy, Tejaswini Herath, and Mindy K. Shoss. 2014. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems* 31, 2: 285–318. https://doi.org/10.2753/MIS0742-1222310210
12. Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. 2014. The Effect of Social Influence on Security Sensitivity. In *In Proceedings of Symposium on Usable Privacy and Security (SOUPS) 2014*, 15.
13. Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I. Hong. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18), 1:1-1:12. https://doi.org/10.1145/3173574.3173575
14. Thomas N. Friemel. 2014. The digital divide has grown old: Determinants of a digital divide among seniors: *New Media & Society*. https://doi.org/10.1177/1461444814538648
15. Chris Hale. 1996. Fear of Crime: A Review of the Literature. *International Review of Victimology* 4, 2: 79–150. https://doi.org/10.1177/026975809600400201
16. Julie Haney M. and Wayne G. Lutters. 2018. "It's Scary…It's Confusing…It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *In Proceedings of Symposium on Usable Privacy and Security (SOUPS) 2018*.
17. Julie M. Haney and Wayne G. Lutters. 2019. Motivating Cybersecurity Advocates: Implications for Recruitment and Retention. In *Proceedings of the 2019 on Computers and People Research Conference* (SIGMIS-CPR '19), 109–117. https://doi.org/10.1145/3322385.3322388
18. Ann Henderson-Sellers. 1998. Climate Whispers: Media Communication About Climate Change. *Climatic Change* 40, 3: 421–456. https://doi.org/10.1023/A:1005384523305
19. Meghan E Hollis, Marcus Felson, and Brandon C Welsh. 2013. The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. *Crime Prevention and Community Safety* 15, 1: 65–79. https://doi.org/10.1057/cpcs.2012.14
20. Trevor Hughes. More fraudsters are scamming senior citizens through technology — and it's costing them millions. *usatoday*. Retrieved September 16, 2018 from https://www.usatoday.com/story/money/personalfinance/2018/03/17/more-fraudsters-scamming-senior-citizens-through-technology-and-its-costing-them-millions/428406002/
21. Amanda Hunsaker and Eszter Hargittai. 2018. A review of Internet use among older adults. *New Media & Society* 20, 10: 3937–3954. https://doi.org/10.1177/1461444818787348
22. MA Rodrigo Juárez, Víctor M. González, and Jesús Favela. 2016. Effect of technology on aging perception: *Health Informatics Journal*. https://doi.org/10.1177/1460458216661863
23. Justin Kruger and David Dunning. 1999. Unskilled and unaware of it: how difficulties in recognizing one's own incompetence lead to inflated self-assessments. *Journal of personality and social psychology*. https://doi.org/10.1037/0022-3514.77.6.1121
24. Nigel Martin and John Rice. 2013. Spearing High Net Wealth Individuals: The Case of Online Fraud and Mature Age Internet Users. *International Journal of Information Security and Privacy (IJISP)* 7, 1: 1–15. https://doi.org/10.4018/jisp.2013010101
25. Sharan B. Merriam and Youngwha Kee. 2014. Promoting Community Wellbeing: The Case for Lifelong Learning for Older Adults. *Adult Education Quarterly* 64, 2: 128–144. https://doi.org/10.1177/0741713613513633
26. Tracy L. Mitzner, Cara Bailey Fausset, Julie B. Boron, Anne E. Adams, Katinka Dijkstra, Chin Chin Lee, Wendy A. Rogers, and Arthur D. Fisk. 2008. Older Adults' Training Preferences for Learning to Use Technology. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 52, 26: 2047–2051. https://doi.org/10.1177/154193120805202603
27. National Cyber Security Centre. *Password Guidance: Simplifying Your Approach*. National Cyber Security Centre. Retrieved September 20, 2018 from https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach
28. 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
29. James Nicholson, Yousra Javed, Matt Dixon, Lynne Coventry, Opeyemi Dele-Ajayi, and Philip Anderson. 2020. Investigating Teenagers' Ability to Detect Phishing Messages. *IEEE EuroUSEC 2020*: 10.

30. James Nicholson and Jill McGlasson. 2020. CyberGuardians: Improving Community Cyber Resilience Through Embedded Peer-to-Peer Support. In *Companion Publication of the 2020 ACM Designing Interactive Systems Conference* (DIS' 20 Companion), 117–121. https://doi.org/10.1145/3393914.3395871
31. 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.
32. Jake Pywell, Santosh Vijaykumar, Alyson Dodd, and Lynne Coventry. 2020. Barriers to older adults' uptake of mobile-based mental health interventions. *DIGITAL HEALTH* 6: 205520762090542. https://doi.org/10.1177/2055207620905422
33. John Martyn Ratcliffe, Paul Galdas, and Mona Kanaan. 2020. Men and loneliness in the 'west': A critical interpretive synthesis. *Research Square*. https://doi.org/10.21203/rs.3.rs-17584/v1
34. Arlind Reuter, Tom Bartindale, Kellie Morrissey, Thomas Scharf, and Jennifer Liddle. 2019. Older Voices: Supporting Community Radio Production for Civic Participation in Later Life. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI '19), 1–13. https://doi.org/10.1145/3290605.3300664
35. Joanne Rodda, Zuzana Walker, and Janet Carter. 2011. Depression in older adults. *BMJ* 343. https://doi.org/10.1136/bmj.d5219
36. Thomas Scharf, Bernard McDonald, and Ann Marie Atkins. 2016. Promoting civic engagement in later life through the Touchstone Programme: a resource and research guide. *Galway: Irish Centre for Social Gerontology*.
37. Joseph J Simons, Noah Joshua Phillips, Rohit Chopra, Rebecca Kelly Slaughter, and Christine S Wilson. *Protecting Older Consumers*. Federal Trade Commission.
38. Vera Toepoel. 2013. Ageing, Leisure, and Social Connectedness: How could Leisure Help Reduce Social Isolation of Older People? *Social Indicators Research* 113, 1: 355–372. https://doi.org/10.1007/s11205-012-0097-6
39. Jingyi Wang, Farhana Mann, Brynmor Lloyd-Evans, Ruimin Ma, and Sonia Johnson. 2018. Associations between loneliness and perceived social support and outcomes of mental health problems: a systematic review. *BMC Psychiatry* 18, 1: 156. https://doi.org/10.1186/s12888-018-1736-5
40. Rick Wash and Molly M. Cooper. 2018. Who Provides Phishing Training? Facts, Stories, and People Like Me. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (CHI '18), 1–12. https://doi.org/10.1145/3173574.3174066
41. Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. 2020. "We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (CHI '20), 1–12. https://doi.org/10.1145/3313831.3376605
42. Anne Weibert, Konstantin Aal, Nora Oertel Ribeiro, and Volker Wulf. 2017. "This is My Story...": Storytelling with Tangible Artifacts among Migrant Women in Germany. In *Proceedings of the 2017 ACM Conference Companion Publication on Designing Interactive Systems* (DIS '17 Companion), 144–149. https://doi.org/10.1145/3064857.3079135
43. Etienne Wenger. 1998. Communities of Practice: Learning as a Social System. *Systems Thinker* 9, 5: 10.
44. Alma Whitten and J D Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium*, 15.
45. World Health Organization. 2004. *Global Burden Disease Report*. World Health Organization. Retrieved September 14, 2020 from https://www.who.int/healthinfo/global_burden_disease/GBD_report_2004update_part4.pdf