NOT-EQUAL

EPSRC NetworkPlus: Social Justice through the Digital Economy

Project Final Review Form

Please submit this form within one month of completing your project to **notequal@ncl.ac.uk**.

GENERAL INFORMATION	
Lead Applicant (PI): Dr. James Nicholson	**Co-Investigators (names and organisations):**
Email address: james.nicholson@northumbria.ac.uk	**Supporting Partner(s):**
Job Title: Lecturer	University of the Third Age (U3A)
Department: Computer and Information Sciences	The Old Low Light Heritage Centre
Organisation: Northumbria University	**Project Title:** Creating and Understanding CyberGuardians in Communities
	Project Reference Number: NE52

1. SUMMARY

Please outline the research challenge and question your project aimed to address, in less than 100 words.

Cyber attacks are on the rise, and as such it is important for citizens to be aware of how they can protect themselves online. There are a number of simple behaviours that citizens can perform to minimize the chances of being compromised by an opportunistic cyber attacks (i.e. those that are easy to perform and therefore common). Older citizens, in particular, are vulnerable to these opportunistic attacks as they typically do not have access to up-to-date and reliable cybersecurity protective information.

We were interested in understanding how older citizens can support peers in sharing reliable cybersecurity information that can prevent opportunistic cyber attacks.

2. APPROACH

Please provide a summary of the approach of your research project, including any deviations from your work plan, the reasons for this and how you addressed any issues.

The fourteen CyberGuardians who were predominantly recruited from our partners, the University of the Third Age (U3A) and the Old Low Light which is a North Shields based charity, completed their formal training in January 2020 through interactive workshops with presentations, live demonstrations (e.g. password cracking) and hands on activities (e.g. phishing test). The topics covered in the training had been identified by the group themselves as well as through existing literature on older users. The training focused on three main areas: password management, scam detection and protective software. 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 encryption as "juicing an orange". This training, along with some initial findings on group-based workshops delivered by the CyberGuardians to older citizens, was documented in a short paper presented at DIS2020 (Nicholson & McGlasson, 2020).

We collected insights from the CyberGuardians on their experiences throughout the different sessions (Welcome meeting, training sessions, and 3 sharing sessions) as well as through an anonymous online questionnaire aimed at the CyberGuardians and all citizens that were helped. A full paper detailing these findings is currently under review.

When COVID-19 hit, and the UK was forced into a national lockdown, the practical elements of the project pivoted from opportunistic information sharing to formal workshop opportunities to disseminate cybersecurity knowledge. This shift resulted in the CyberGuardians helping many older citizens in staying safe online during the COVID-19 phishing increase, and help on using Zoom securely so they could stay in touch with family and friends.

References:

Nicholson, J., & McGlasson, J. (2020, July). CyberGuardians: Improving Community Cyber Resilience Through Embedded Peer-to-Peer Support. In Companion Publication of the 2020 ACM Designing Interactive Systems Conference (pp. 117-121).

3. ACTIVITIES & OUTPUTS

Please list any outputs from your project to be entered in the Not-Equal Researchfish submission. These include events, publications, workshops, webinars, invited talks, media coverage and tools (please include links to open source, git-hubs if relevant) that have resulted from your project.
Please include the following for each entry:

Title: CyberGuardians: Improving Community Cyber Resilience Through Embedded Peer-to-Peer Support
Date: July 2020
Type of Event: Publication
Number of People Reached: ACM Digital Library
Primary Audience: Academic
Key Outcomes/Impact: Initial findings.
Link: https://dl.acm.org/doi/10.1145/3393914.3395871

Title: Sharing is Caring

Date: 4 November 2020
Type of Event: Invited Talk: Swansea University
Number of People Reached: 25 directly
Primary Audience: Academic
Key Outcomes/Impact: Initial findings.

Title: CyberGuardians on BBC Look North
Date: 26 February 2020
Type of Event: Media
Number of People Reached: BBC North East
Primary Audience: Public
Key Outcomes/Impact: Showcasing of work, partner contacted for further information. CyberGuardian featured reported being stopped on the street by strangers (but not being asked for help by strangers).
Link: https://livenorthumbriaac-my.sharepoint.com/:v:/g/personal/james_nicholson_northumbria_ac_uk/EYoiqwwObnRFoyEIsvXe67gBZVXmrIK5WhkZAN_yDCVlbA?e=9696hI

Title: Sharing is Caring: The CyberGuardians Project
Date: November 2020
Type of Event: Publication
Number of People Unknown, but U3A Whitley Bay has approximately 340 members.
Primary Audience: Public
Key Outcomes/Impact: Advertising the scheme, but also reporting on the success so far (820 people helped).
Link: https://u3asites.org.uk/files/w/whitley-bay/docs/partners.report.cyberguardians.pdf

4. INSIGHTS & IMPACT

Please describe the findings of your project and their significance in relation to potential or actual social impact.

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 CyberAdvocates, and this could be the most effective way to spread cybersecurity best practice into the community – both young and old. This approach 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 in changing behaviours since the training appeared to be effective, something which can be traced back to security storytelling amongst peers. 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. which ultimately leads to lower awareness and can facilitate attacks. This is also typical of other difficult subjects (e.g. social isolation, privacy, etc.). This type of initiative has begun to demonstrate how we can generate interest and engage communities in conversation and overall awareness of such topics.

The CyberGuardians discussed Cybersecurity advice and information with approximately 470 unique citizens. Additionally, the citizens who spoke with the CyberGuardians reported discussing this advice and information with a further 350 people. In total, this means the 14 CyberGuardians disseminated good quality cybersecurity information to approximately 820 people in 9 months. While we know that cybersecurity awareness does not guarantee protection from cyber attacks, we have begun to see many of the CyberCitizens improve their password and phishing behaviours (this data is still to be properly analysed) and we have seen evidence of open communications between CyberCitizens and the CyberGuardians, which can only be seen as a good thing: being open about scams and security behaviours that can prevent these means that citizens have peers who they can turn to for help if needed, but perhaps more importantly they can be aware of potential threats that they wouldn't be otherwise.

5. REFLECTIONS & FUTURE DIRECTIONS

Please list the key highlights from your project, summarize any lessons learned from this work and outline any future directions or plans to continue activities beyond this project.

We need more work to understand how to support the CyberGuardians in an online context. While they developed excellent methods for sharing cybersecurity information to peers informally, finding an audience for their online workshops has proved to be more difficult. Of course, this is because people typically do not seek cybersecurity information unless they are in need of help, and in an online context that might mean that the individual does not have access to the internet to seek help. We need to start thinking about ways of recreating informal and relaxed environments online where the CyberGuardians can share their wisdom.

We also need to consider the best ways of expanding the scheme to other older demographics. While we have seen great success with this pilot project, the majority of participants were relatively wealthy old adults who had good social connections. We need to think how best to reach lower SES older adults, and who may not potentially have great social connections.

We would also like to extend the scheme to other age groups (e.g. younger adults) although much research will be needed to understand the social context and how technology can be used to facilitate the spread of good cybersecurity information in these demographics.

Further Information
If you have any further questions regarding this form, please contact notequal@ncl.ac.uk or 0191 2088268.