NOT-EQUAL

EPSRC Network+: Social Justice through the Digital Economy

Pilot Projects: Application Form

We are seeking funding proposals from shortlisted candidates for Not Equal's first call for pilot projects. For full guidance please see details of the call on the Not Equal website.

Pilot research projects can be between 6-8 months in length. We expect to fund up to 12 pilot research projects of up to £40k (80%FEC) for this first funding call.

Please submit this form before the deadline of **5pm, 30th April 2019** to notequal@ncl.ac.uk.

Applicants will be advised on the outcome of their proposal by the 30th May 2019.

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

1. SUMMARY

Please provide a summary of your proposed research project (<300 words).

This project aims to support older users in becoming cybersecurity guardians (or CyberGuardians) for their local community and to organically train other older users in this practice, thus making available sources knowledgeable as well. CyberGuardians will serve as points of contact for cybersecurity queries for peers in their local communities, and research is needed to understand the most appropriate training methods for older adults and to understand what support is needed for them to carry out the job effectively. We will develop and design age-specific cybersecurity training sessions based on perceived cybersecurity threats identified by participants and literature.

Understanding cybersecurity threats and defences is essential for citizens to effectively protect themselves from the ever-changing technological landscape. Recent work has reported that older adults' cybersecurity information-seeking behaviours differ from younger users in one key area: Older users appear to prioritise the availability of the information source over all other criteria, unlike the general population who prioritise expertise. This difference in source prioritisation suggests that older users may be more vulnerable than the general population when it comes to understanding and protecting against current and future cybersecurity threats, despite being one of the fastest growing demographics in the adoption of internet-enabled technologies.

We will train older volunteers (55+ years) to become our CyberGuardians over several weeks through dynamic workshops that will inform them about relevant cybersecurity threats and countermeasures based on the demographic's threat models. Importantly, participants will also be informed on more practical aspects including cybersecurity information seeking to ensure the sustainability of this approach.

We will then monitor the effectiveness of our CyberGuardians in action throughout the remainder of the project using digital diaries and interviews to understand what support CyberGuardians need in order to effectively perform their guardianship.

2. HOW DOES YOUR PROPOSAL ALIGN WITH THE THEMES AND OBJECTIVES OF NOT EQUAL?

Please describe how your proposal helps understand, explore or develop practical responses to social justice issues within the digital economy; and how does your proposal enhance a cross-disciplinary way of working. Please also indicate which of the Not Equal challenge areas your proposal focuses on e.g. Algorithmic Social Justice, Digital Security for All and Fairer Futures for Business and Workforce (<500 words).

This proposal focuses on the Digital Security for All theme. Our pilot will focus on the specific demographic of older users, who typically struggle to understand the ever-changing landscape of cybersecurity threats and defences without the proper support. In fact, older users are often targeted by attackers and this results in them losing more money than the general population when scammed (Hughes, 2018).

However, if the pilot is successful it could set a blueprint for the development and support of CyberGuardians across different communities and demographics. While many working age adults keep up to date through security training at work, those without access to such programmes (or who are part of organisations with poor training programmes) face similar issues to older users.

Our proposed programme of empowering older users to become CyberGuardians for their local community means that many more older adults should have approachable and knowledgeable *like-minded* individuals who can help with relevant cybersecurity issues, as well as educate them on how to become more cyber aware. This latter point is important, as we know that people are more likely to seek and accept information from individuals that they can identify with (e.g. Wash & Cooper, 2018), while the label of being a CyberGuardian will enhance messenger effects (e.g. Dolan et al., 2012).

By partnering with the University of the Third Age (U3A) and the Old Low Light, we are potentially reaching over 400,000 members of the general population nationwide. We hope that by training and empowering members of the community to take on the role of CyberGuardians even more older users will have access to reliable cybersecurity information and advice.

References:

Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., & Vlaev, I. (2012). Influencing behaviour: The mindspace way. *Journal of Economic Psychology*, *33*(1), 264-277.

Hughes, T. (2018). More fraudsters are scamming senior citizens through technology – and it's costing them millions. https://www.usatoday.com/ story/money/personalfinance/2018/03/17/more-fraudsters-scamming-senior- citizens- through- technology- and- its- costing- them- millions/428406002/

Wash, R., & Cooper, M. M. (2018). Who provides phishing training?: Facts, stories, and people like me. In *Proceedings of CHI 2018*.

3. CASE FOR SUPPORT

Please describe your proposed projects, including its aims and objectives. This will include the design and method of your project, context, background literature and data to be collected. Please also indicate why is this research important and for whom (<1000 words).

Background

Understanding cybersecurity threats and defences is essential for citizens to effectively protect themselves from the ever-changing technological landscape. In a recent paper (Nicholson et al., 2019) we reported that older adults' cybersecurity information seeking behaviours differ from younger users in one key area: Older users appear to prioritise the availability of the information source over all other criteria, unlike the general population who prioritise expertise (Nthala & Flechais, 2018). This difference in source prioritisation suggests that older users may be more vulnerable than the general population when it comes to understanding and protecting against current and future cybersecurity threats, despite being one of the fastest growing demographics in the adoption of internet-enabled technologies (Hunsaker & Hargittai, 2018).

Routine Activity Theory (Cohen & Felson, 1979) 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 latter role is especially interesting, and where we will focus from a cybersecurity perspective. 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…" (Felson, 2006) and as such raises an important question: can we shape Cybersecurity Guardians (or CyberGuardians) who will protect everyday users from cyberattackers?

Aims

This project aims to train older users to become CyberGuardians for their local community and to organically train other older users in this practice. Previous work has highlighted the importance of network effects and of having readily available, local sources of information (Nicholson et al., 2019). Section 2 above details the importance of having like-minded individuals promoting good cybersecurity knowledge. Other work details the importance of having Cybersecurity Advocates that translate cybersecurity terms to lay language, and who support the general population with their cybersecurity queries (Haney & Lutters, 2018). Thus, our research question for this pilot project is: "What support do CyberGuardians need for effective guardianship?"

Method

We propose a multi-step process for developing and supporting CyberGuardians: recruitment, training, guardianship, and evaluation.

The initial step will be to recruit older individuals who want to learn more about cybersecurity and who would like to communicate this knowledge to peers. Our partners at the U3A and the Old Low Light – as well as existing relationships with relevant groups like the Elders Council of Newcastle – will be integral in this recruitment process and initial scoping for interest can commence prior to the project start date to prevent unnecessary delays.

The second step will be to ascertain what a likely threat model looks like for older users through a combination of academic literature, organisational reports, news reports, and insights from our participants. The threat model will be used to develop the training for our CyberGuardians, and will be an interesting outcome from this project.

The third step will be to carry out a series of training workshops with the CyberGuardians to ensure that they are knowledgeable about the key issues that members of the community will need help with. These workshops will take place over 4-6 weeks, and will consist of practical troubleshooting, cybersecurity information searching, and some limited theory to ensure that CyberGuardians are able to effectively keep themselves up to date with the necessary cybersecurity topics. Core material to be covered will likely include password hygiene, two-factor authentication, and scam detection, but actual topics will depend on the identified threat models. During these workshops, CyberGuardians will be supported in developing materials and organising information exchange events for members for their community. The methods that CyberGuardians choose for protecting their communities will be an important and interesting outcome from this project.

The fourth step will be a key milestone in the project where CyberGuardians will be encouraged to disseminate cybersecurity knowledge to their respective communities for a period of at least 2 months. They will be asked to keep a record of both individual and group interactions and any follow ups. Specifically, we will want to know who approached them, why, and with what problem. They will also be asked to record any times when they have approached members of the community proactively. This data will be used to evaluate the CyberGuardians' self-confidence and their perceived effectiveness in dealing with others' cybersecurity issues. During this period, the PI and the U3A Events Chair (Mike Martin) will serve as points of contact for CyberGuardians.

The final step will be to interview the CyberGuardians on their experiences – specifically around what worked well and what they would like to improve (both regarding the training and the actual guardianship). At this stage we will also evaluate our initial threat model and determine whether this was accurate in practice or not.

Analysis

The main analysis will consist of the diaries that CyberGuardians keep during their guardianship, as well as the final interviews with guardians. However, the development of the workshop materials, and the development of materials to support CyberGuardians will also be valuable for understanding the methods that older users perceive to be the most effective for communicating cybersecurity information.

References:

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588-608.

Felson, M. (2006). Crime and nature. Sage.

Haney, J. M., & Lutters, W. G. (2018). " It's Scary… It's Confusing… It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. In *Proceedings of SOUPS 2018*.

Hunsaker, A., & Hargittai, E. (2018). A review of Internet use among older adults. New Media & Society, 20(10), 3937-3954.

Nicholson, J., Coventry, L., & Briggs, P. (2019). "If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults. In *Proceedings of CHI 2019*.

Nthala, N., & Flechais, I. (2018). Informal support networks: an investigation into home data security practices. In Proceedings of *SOUPS 2018*.

4. NOVELTY OF PROPOSAL

Please explain the novelty of the proposed research project (<150 words).

This project takes the novel approach of training members of the community to be 'experts' who will in turn help other community members, rather than the traditional model of having academic or industry experts attempt to disseminate relevant information to individuals (on a one-to-many basis).

Here, we are looking at the process for developing and supporting CyberGuardians, who will be in a better position to understand the local threat models and will be able to help like-minded individuals in preventing and assisting with cybersecurity incidents.

This pilot will give us insights into the challenges and opportunities that arise from training and supporting CyberGuardians, and can lead to more effective methodologies for improving the process for both older users and other demographics.

5. NON-ACADEMIC PARTNERS

Please explain how your non-academic partners will engage with the project e.g. in-kind time, use of facilities, etc. (<150 words)

We propose working with our established partners the University of the Third Age (U3A: https://www.u3a.org.uk/) – a nation-wide organisation aimed at encouraging lifelong learning amongst older adults and consisting of 10,000 local regional members and over 425,000 members nationally (all older adults) – and the Old Low Light in North Shields (http://oldlowlight.co.uk/), a volunteer-run community organisation consisting of approximately 2,000 volunteers, the majority of whom are older adults.

Both organisations will facilitate the recruitment of participants for the role of CyberGuardians, and will also help advertise the availability of these CyberGuardians to the community once they have been trained. By having two well-regarded organisations endorsing our CyberGuardians, we anticipate that older users will feel confident in engaging with both the programme and the individuals.

6. DELIVERABLES AND SOCIAL IMPACT

Explain the outcomes and deliverables of your project as well as the expected social impact. Please ensure this answer is suitable for a lay audience (<300 words).

The purpose of this project is to empower regular members of the community to become reliable sources of information for cybersecurity queries. In this pilot, we will be testing this programme with older adults. We propose to do this by training willing older volunteers to become CyberGuardians who will then serve as the point of contact for members of their community, as well as train other willing volunteers. The tasks for CyberGuardians will include one-to-one help (for example being approached by someone with a security question), as well as group events (for example presentations or workshops run by CyberGuardians to demonstrate and help others). This means that older internet users will have **approachable**, **available**, and **knowledgeable** peers who can support them through the scary and confusing world of cybersecurity.

To this end, the question we are trying to answer is: "What support do CyberGuardians need for effective guardianship?"

This project will publish the materials used to train CyberGuardians, a video documenting the process (including interviews with CyberGuardians), and any materials that were developed for the CyberGuardians.

7. WORK PLAN

Please outline the work-plan for your proposed research/activity (<200 words).

We will recruit older individuals through our partners who want to learn more about cybersecurity and who would like to communicate this knowledge to peers (Months 0-1).

Month							
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Recruitment & Threat Model		*Train CyberGuardians*		*CyberGuardians at Work*		*Interviews*	
Develop a threat model for older users through published resources and insights from our participants to inform the training materials for our CyberGuardians.		Train CyberGuardians over 4-6 weeks to ensure that they are knowledgeable about the key issues that members of the community will need help with. During these workshops, CyberGuardians will be supported in developing materials and organising information exchange events for members for their community.		CyberGuardians will be encouraged to disseminate cybersecurity knowledge to their respective communities for a period of at least 2 months. They will be asked to keep a record of both individual and group interactions and any follow ups.		Interview CyberGuardians on their experiences – specifically around what worked well and what they would like to improve (both regarding the training and the guardianship). At this stage we will also evaluate our initial threat model and determine whether this was accurate in practice or not.	

8. HOW WILL YOU COMMUNICATE THE FINDINGS OF YOUR RESEARCH TO THE PUBLIC?

Please outline your dissemination plans e.g. events, networking with local support groups, creating vlogs, writing blogs, etc. (<200 words).

Our main dissemination event will consist of a short presentation open to the general public describing the project and the main findings (e.g. processes for establishing and supporting CyberGuardians, insights into threat models, etc.) which will also be livestreamed (and later available on demand) to anyone interested. This free event will be advertised via the Old Low Light and the U3A, as well as through word of mouth. Following the presentation, viewers will be encouraged to ask questions (including those watching via stream) and the research team will answer these.

This project will also publish the materials used to train CyberGuardians, a video documenting the process (including interviews with CyberGuardians), and any materials that were developed for the CyberGuardians.

The details of the scheme and main findings will be published in the quarterly national U3A magazine and on the U3A website. We will also approach local media about documenting the process and possibly distributing the video of the presentation.

9. EXISTING FUNDING

Will any existing funding be used on this project (e.g. PhD funding)? If so, please provide information on these and how they will be used on the project.

No existing funding will be used on this project.

10. TRACK RECORD OF APPLICANTS

Please indicate any previous relevant experience, qualifications and publications of the lead applicant and team (<200 words).

Dr. James Nicholson has been publishing human-centred cybersecurity research at prestigious international venues since 2008. His PhD work focused on developing and evaluating inclusive authentication systems and since then has carried out research benefitting older users, including being part of the EPSRC-funded project Cybersecurity Across the Lifespan where he has published on older users' information seeking behaviours (Nicholson et al., 2019).

James has also been involved in developing and delivering educational cybersecurity and privacy workshops to members of the U3A since 2017. To date 5 workshops have been completed to overwhelmingly positive feedback (and have been oversubscribed). There are plans for further workshops on other cybersecurity topics in the next 8 months.

Mike Martin is a self-taught IT support volunteer for U3A Whitley Bay and Northumbria Region, as well as the Old Low Light heritage centre. For the last 5 years he has been running monthly computer and iOS help sessions. He has also organised Cybersecurity Workshops with other organisations, such as Northumbria University, for members of both organisations.

11. BUDGET BREAKDOWN

Please provide a detailed budget breakdown and justification for your budget - for example: salary grade, point, duration and %FTE: specified journeys or conferences; identified items and quantities of consumables (<300 words)

We require £4,000 to cover participant expenses – both for CyberGuardians (e.g. cost of hiring a venue, travel to help users, etc.) and for regular participants (e.g. attending an event hosted by a CyberGuardian).

We also require £3,000 in consumables for this project. We will host a website where materials will be available for our CyberGuardians, and where CyberGuardians can record their experiences of dealing with community members (Diary). We will also need to design materials for the training of CyberGuardians, and any materials that CyberGuardians need to support their guardianship (e.g. handouts, posters, flipcharts, videos, etc.). The specifics of these materials will only be known after running a few training sessions with the CyberGuardians.

We require a research assistant (starting grade 5.1) for 4 months full time. The researcher will help with the design of the training and supporting materials for CyberGuardians. During a separate stint, the researcher will also interview and analyse the final data collection after the guardianships are over. It is estimated that the researcher will be active from November 2019 – Dec 2020 and from March 2020 – April 2020.

PI at 10% of grade 6.3 (projected for a September 2019 start) will serve as a point of contact for CyberGuardians during their guardianship and will supervise all aspects of the project.

11. TOTAL PROJECT COST

Please list in GBP under the headings - Overall cost, Staff, Travel and Other

	Costs (80%)	**Costs (100%)**
Staff (directly allocated investigators)	£2,594.40	£3,243.00
Staff (directly incurred RA)	£9,471.64	£11,839.55
Non-Staff Costs: Consumables (directly incurred)	£2,400	£3,000
Non-Staff Costs: participant costs (directly incurred)	£3,200	£4,000
Non-Staff Costs: Estates (RA's only)	£866.80	£1,083.50
Non-Staff Costs: Indirect (RA's only)	£13,349.60	£16,687.00
Overall Cost*	**Total Not Equal Funding Requested: £31,882.45**	Total for information only: £39,853.06

Directly allocated and Incurred Posts

Role	Post	Start Date	Period on Project (months)	% of Full Time	Scale	Increment Date	Basic Starting Salary	Super-Annuation and NI (£)	Total cost on grant-80% FEC (£)	Total cost on grant-100% FEC (£)
Investigator	PI	01/09/2019	8	10%	6.3	01/08/2020	£38,085	£10.560	£2,594.40	£3,243.00
Researcher	RA	01/11/2019	4	100%	5.1	01/08/2020	£28,048	£7,223.84	£9,471.64	£11.839.55

*Please note you are able to claim for RA time and RA relevant FTE related costs, PI/Co-I time and other non-staff costs. You are not able to claim for FTE related costs attributed to PI/Co-I time.

Further Information

If you have any further questions regarding this call for proposals, please contact notequal@ncl.ac.uk or Kate Kelly (Not Equal Project Manager) on 0191 2088268.