"If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults

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

Lynne Coventry
Northumbria University
Newcastle, UK
lynne.coventry@northumbria.ac.uk

Pam Briggs
Northumbria University
Newcastle, UK
p.briggs@northumbria.ac.uk

ABSTRACT

Older adults are increasingly vulnerable to cybersecurity attacks and scams. Yet we know relatively little about their understanding of cybersecurity, their information-seeking behaviours, and their trusted sources of information and advice in this domain. We conducted 22 semi-structured interviews with community-dwelling older adults in order to explore their cybersecurity information seeking behaviours. Following a thematic analysis of these interviews, we developed a cybersecurity information access framework that highlights shortcomings in older adults' choice of information resources. Specifically, we find that older users prioritise social resources based on availability, rather than cybersecurity expertise, and that they avoid using the Internet for cybersecurity information searches despite using it for other domains. Finally, we discuss the design of cybersecurity information dissemination strategies for older users, incorporating favoured sources such as TV adverts and radio programming.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**.

KEYWORDS

Cybersecurity; digital literacy; information seeking; older adults; social aspects of security.

ACM Reference Format:
James Nicholson, Lynne Coventry, and Pam Briggs. 2019. "If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults. In *CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, Scotland UK*. ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/XXXXXX.XXXXXX

1 INTRODUCTION

Citizens are increasingly exposed to personal cybersecurity threats, yet many people struggle to protect themselves online and usually require external support. This support is typically drawn from online sources, professionals, work colleagues, and/or friends and family [12, 37, 43, 44]. In addition to obtaining support from the aforementioned sources, news reports can play an important role in raising user awareness of cybersecurity threats and appropriate mitigating action [12].

Sources of cybersecurity information are thus diverse, but a digital divide also operates that can affect access to good quality information and advice for certain individuals. Recent work has started to explore these populations. For example, those with lower standards of education will turn to less authoritative sources, typically asking friends and family for guidance rather than seeking expert advice [44]. Older adults also comprise an interesting group, as they are actively targeted for specific cyberattacks such as pension scams [1, 30] and romance scams [25] in addition to threats also facing the general population [1, 8]. They also lose more money from compromises when compared to their younger counterparts [25]. Older adults are unwilling to report cyber incidents which means that they may be even more vulnerable than official figures show [26].

Prior work has briefly suggested that older adults may exhibit different habits from younger adults when it comes to cybersecurity information seeking and awareness [12, 44]. Yet research on the trusted sources of cybersecurity information and advice in the older population is sparse. This is despite the fact that older adults have been found to exhibit high fear of crime [21, 24] – which is likely to translate to online environments [47].

In this paper, we explore cybersecurity information seeking behaviours in older adults. Our aim is to understand what lifestyle and digital literacy factors affect an older adult's ability to obtain and assess good quality information and advice. We explore this through semi-structured interviews with 22 community-dwelling older adults who regularly use the internet for communication and information.

The contributions of this paper are threefold:

(1) Firstly, we believe this is the first paper to address in depth older users' cybersecurity information-seeking behaviours and their decisions about which sources to trust;
(2) Secondly, we introduce a cybersecurity information access framework focusing on older users, describing the cyberliteracy and information resource factors that influence their capacity to find relevant advice and information;
(3) Finally, we show how poor cyberliteracy can affect trust in digital sources, making older adults uncomfortable using the Internet to search for cybersecurity information, even if they use it freely to search for material in other contexts.

CHI 2019, May 4–9, 2019, Glasgow, Scotland UK

ACM ISBN 978-1-4503-5970-2/19/05…$15.00
https://doi.org/10.1145/XXXXXX.XXXXXX

2 BACKGROUND

2.1 Cybersecurity vulnerabilities of older adults

Older adults show a number of distinct cybersecurity vulnerabilities. They are more vulnerable to spam and take fewer defensive actions than younger adults [20], they have a more limited knowledge of computer-based privacy and security threats [20], and they are often more willing to trust those they encounter through digital transactions [19]. If we add to this the fact that some have significant retirement savings, then it is not surprising to discover that older adults are disproportionately targeted for internet crime and fraud [30]. Older adults are also more likely to be more socially isolated [3] and some experience problems with digital literacy. This is important as those with relatively weak social ties and/or poor digital literacy are less able to share in the peer learning that occurs within social networks, are more likely to be more trusting and vulnerable to fraud (e.g. [3]), and less able to assess the quality of advice they receive [53].

2.2 Older Adults and the Cybersecurity Threat

There are two ways to think about the response citizens make to the threats they experience in their everyday lives. The first is to consider the knowledge and interpretation of that threat: how severe it is, how vulnerable or susceptible they are to that particular threat. The second is to consider the extent to which they can mitigate that threat, by taking effective evasive or protective action. These two dimensions are used to explain a wide range of health and other behaviours and form the basis of a number of behaviour change models, one of the most salient being Protection-Motivation Theory (PMT – [48]). PMT is a well-established model that describes the likelihood that people will be able to make an effective behavioural response to a threat. It has been used to account for the uptake of protective behaviours in a wide variety of contexts, including decision to be vaccinated, adoption of a healthier lifestyle and, more recently, cybersecurity [23].

The first element of PMT is the awareness and understanding of threat. In this regard, older adults form an interesting group. It is well known that older adults differ from their younger counterparts in being risk averse, in part because they are more worried about the underlying threats (e.g. [46]). In the cybersecurity context, the lack of expertise in older adults is associated with a higher perception of security threat [18] and the likely response to this elevated threat perception is that older adults sometimes avoid using digital technologies (e.g. [7]).

The literature on older adults' understanding of cyber threats is slight, but there is a parallel literature that shows that older adults exhibit a particularly high fear of crime [21]. Fear of crime is interesting, as it is likely to translate to an online environment, especially in relation to cyber identity threats [47]. Again, we see that a high perceived susceptibility to cyber threat is likely to lead to a defensive response in terms of disengagement with cybersecurity measures [9] and/or lower interactions with online services. We should note, however, a recent study reporting that whilst older adults are aware of cybersecurity attack vectors such as phishing, they somewhat paradoxically report low awareness of their own susceptibility to threats [39] which means that they often fail to understand the ways that their own behaviours put them at risk.

The other element in PMT describes the coping response that can be made in the face of threat. Again, there is extensive literature that shows that the ability to respond meaningfully to threat, coupled with a belief in one's ability to make that response (self-efficacy) is critical. Indeed, recent meta-analyses in the health domain show that the coping rather than the threat elements of the PMT model are those that predict successful behaviour change [55]. In cybersecurity terms, this implies that cybersecurity literacy – knowing which protective responses are effective and having the necessary expertise and confidence to make those responses – is vital. However, older adults tend to have lower levels of digital literacy than their younger counterparts [50] and can struggle to protect themselves online, although some evidence suggests that *well-informed* older users can distinguish between safe and unsafe websites [28].

2.3 Cybersecurity skills and the general population

To interact effectively in the digital world, digital literacy skills need to be developed. Digital literacy refers to a multiplicity of literacies associated with the use of digital technologies and incorporates not only having the ability to use the technology, but associated cognitive, social, and emotional issues [33]. While younger people are perceived as being digital natives, in fact digital literacy is reliant on other factors including culture and university education [2]. Older adults in general understand their limitations with regards to digital literacy, and therefore rely on family and peers for support [50]. It is important to note that digital literacy also includes developing the ability to select and use the necessary tools to complete activities online while protecting oneself from harm in digital environments [33].

While digital literacy training may be provided for those in education or work [2], not much is known about where older users obtain their cybersecurity information, or the reasons behind these choices. However, prior work has hinted that older adults exhibit different habits to those of younger adults when it comes to cybersecurity awareness and information seeking. For example, there appears to be a difference in sources of cybersecurity advice between users aged 18-39 and those 40 and over – where family and friends are sought more by the latter [42]. Indeed, older users also appear to hear about security news predominantly on television, unlike younger adults who generally have various sources such as online articles and social media [12].

The sources of cybersecurity information for the 'general population' are plenty and diverse. Public media, security prompts, professionals, colleagues, friends, and family are all important sources information and advice [42, 44], although patterns of use across these sources differ. Broadcast news media are more likely to act as key sources of information on topical threats, such as large-scale security breaches that carry personal data implications, or ransomware attacks that affect public resources [56]. Social media and other personal networks also have a role in communicating immediate or novel threats [12]. For day-to-day threats, personal contacts – such as work colleagues, friends, and family – are more likely to offer advice about personal cybersecurity protection and

within these networks, those with IT expertise, are particularly important [36, 37, 44].

Different information sources employ different tactics for information dissemination. Experts tend to describe the specific attack vectors (e.g. phishing, viruses, malware) using a more technical language. Non-experts tend to focus on who is initiating the attack (e.g. hackers) using everyday words to talk about computer security concerns, while newspaper reports focus on sensational rather than 'mundane' attacks [41]. Yet, news articles typically drive everyday discussions about security [11], which means that citizens are more likely to talk about large-scale attacks rather than focus on their own everyday problems.

Users must assess what information and advice to accept and what to reject [44]. Yet, the sheer volume of information is in itself problematic, with many users experiencing 'security fatigue' [17]. Inevitably, social processes come into play [37] and behavioural norms perpetuate in this space. For example, simply having friends and family adopt a particular security tool makes it much more likely that an individual will go on to explore that tool [10].

Recently, *cybersecurity advocates* have been identified as security professionals who can offer security expertise in the language of everyday use [22]. This is in contrast to *Digital Champions* proposed by *digitalunite.com* or Barclays bank's *Digital Eagles* [1] who skill up non-security experts to serve as points of advice for the general population. These individuals, present across several contexts including industry and higher education, play the role of motivating users to be secure and making cybersecurity less boring. Very little is known about what populations these advocates encompass and inform, or whether these are self-selecting or based on social characteristics or demographics.

With this in mind, we endeavour to understand where older users obtain their cybersecurity information and, crucially, why they prioritise those sources.

3 METHODOLOGY

The study consisted of semi-structured interviews with older internet users that focussed on the construction of a sociogram (see Figure 1) and discussions about information gathering amongst and outside that social group.

The primary purpose of the sociograms – a graphic representation of social links that a person has – was to place participants in the right state of mind for critically thinking about their interactions and information-seeking behaviours. Prior work has found that simply asking participants about experiences often leads to erroneous and incomplete recalls [29]. Thus, by priming participants about their support network prior to discussing their information-seeking behaviours, we hoped to improve the accuracy of their recalled interactions. Sociograms were constructed using the methodology of *McNeill et al.* [31] and this process typically lasted 10-15 minutes.

All interviews took place at the University and lasted on average 90 minutes, but the overall length was guided by the participants (range: 70 minutes to 120 minutes). As a consequence, the precise topics discussed varied on a per-participant basis depending on their experiences.

[1] https://www.barclays.co.uk/digital-confidence/eagles/

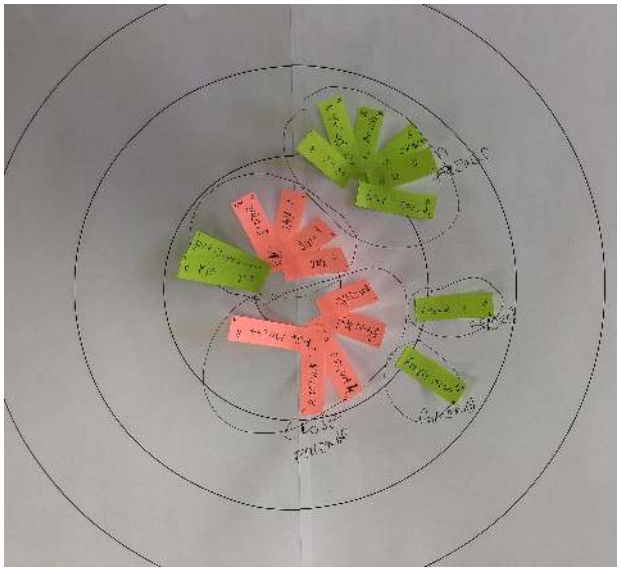

Figure 1: Example of a sociogram created by a participant. Pink sticky notes indicate very close people while green ones indicate close acquaintances. People placed in the small inner ring indicate those that the participant feels closest to.

All participants were offered a £20 shopping voucher for their time. This study was approved by the Faculty's ethics committee.

3.1 Participants

We recruited a total of 22 participants for the interviews. Our sample consisted of 15 females and 7 males, with a mean age of 72 years (S.D. 7.39 years) and was made up of community-dwelling internet users who were both socially well connected and more socially isolated in order to elicit information about a wide range of communicative experiences.

Participants were recruited using emails and communications broadcasted by organisations and charities working with older adults. Some participants were recruited via word of mouth and snowball sampling. Recruitment criteria included adults aged 65 or over (largely to avoid individuals who could still get sources of information and advice from workplace training) with experience using the internet.

The interviews were advertised as 'interactive interviews' to discuss sources of information, lasting up to two hours. Potential participants were not told initially about the focus on cybersecurity information to prevent self-selection bias, but once participants agreed to take part they were given more information before consent to taking part was sought.

3.2 Procedure

All interviews were carried out face-to-face and on a one-to-one basis by a postdoctoral researcher with expertise in cybersecurity. Participants were briefed upon arrival and were encouraged to ask questions both before commencing the study and throughout.

Participants were also told that all questions and activities were voluntary, therefore if they were uncomfortable answering anything they could simply refuse.

During the initial 10 – 15 minutes, participants were asked to create a 'friends and family map' (sociogram) to then be used as a probe to help them consider the roles of others in their network. Following the creation of the sociogram, participants were asked about their experiences of internet security problems and further information on how they rectified these problems. Where participants did not have prior experience with a security issue, they were given concrete scenarios of breaches and asked to recount step-by-step how they would approach the situation, leading to information about help sources and sources of advice. Participants were also asked how they heard about cybersecurity incidents and how they kept themselves informed and up-to-date. Finally, participants were asked about their online information seeking behaviours. As the interviews were semi-structured, the order of the topics varied on a per-participant basis depending on their experiences.

3.3 Analysis

All interviews were audio recorded and transcribed. Then, all transcribed data was analysed using framework analysis [45]. Framework analysis is useful for applied research of this kind as it seeks answers to four types of question: (i) Contextual: What is the nature of people's experiences? What needs does the population of the study have? (ii) Diagnostic: Why are decisions or actions taken, or not taken? Why are services or resources not being used? (iii) Evaluative: How effective are existing systems and resources in achieving objectives? And (iv) Strategic: What new services, actions, or resources are needed to overcome the problem? As with other types of thematic analysis, (e.g. [5]) the analysis proceeds in five stages involving familiarization, the identification of a thematic framework, indexing, charting, and interpretation. The first pass was conducted by the first author, and then the research team engaged in the process of 'researcher triangulation' whereby themes and subthemes were vetted by team members [35].

Two members of the research team worked on the data and ensured agreement on the framework and subthemes before they were finalised.

4 RESULTS

We describe our resulting framework in terms of the interplay of two constructs. These are captured in the framework shown in Table 1 and are unpacked below. The first addresses the cybersecurity literacy of an individual and includes both contextual (knowledge and experience) and evaluative (assessment of competence) elements. The second describes the resources that are available to that individual and includes contextual (their social network and available resources), diagnostic (why and when certain sources are used), and evaluative (trustworthiness of those resources) elements.

4.1 Cybersecurity Literacy

We identified four subthemes in relation to cybersecurity literacy: legacy knowledge, interest in I.T., language, and previous experience.

Table 1: Proposed framework capturing the cyberliteracy and resource factors that influence access to cybersecurity information and advice.

Cyberliteracy	Resource
Legacy Knowledge	Social
Interest in I.T.	Community
Language	Commercial
Past Experience	Broadcast Media
	Internet Media

4.1.1 Legacy Knowledge. Legacy knowledge refers to information that has been retained from previous formal or informal employment. This might simply refer to information absorbed from colleague discussions during the workday:

Female 002: "I suppose going back to when I was at work and people would mention things, I mean, we used computers all the time. So then, yes, people mentioning things and something possibly coming onto your computer and like 'what do you think this is?' or just generally just by talking to people I think."

In such cases, we should note that that 'shadow security' practices operate in organisations, such that employees develop group norms that are not always appropriate [27, 34]. In other words, this knowledge may be unreliable.

Cybersecurity information could have also been obtained from the I.T. support team at the organisation. This legacy information can take several forms, including communications from the I.T. team broadcast to the organisation as a whole, e.g. *"the phishing looks like this, it has hit our system, please don't do it"* (Female 009), or face-to-face information and advice when the I.T. department is local:

Female 005: "I worked in <location> which is where the I.T. department was. So I would have been able to ask them then, but I then got moved out of <location>. So once I moved out of <location> I couldn't really phone them up."

Finally, users adopted knowledge from their organisation's security policies as personal 'best practice', including password composition strategies and templates of phishing emails:

Female 005: "Well, I used to work for the <location> government, so I use their formal, if you will, that I used for them. Which is random letters, so two of which form, next to each other, would form a word... with numbers and, uhm, what are they called... symbols."

It is not surprising that older users hold onto legacy knowledge acquired from the workplace, given organisations' push to ensure employee security compliance [52]. Ultimately, this amassed legacy knowledge influences older users' mental models of cybersecurity. However, legacy knowledge may be inaccurate, as noted above, or simply out of date (e.g. the password composition advice change in 2015 [32]).

4.1.2 Interest in I.T.. Interest in I.T. refers to both the user's own interest in learning more about I.T. as well as the interest of the user's surrounding social group. It partially reflects their motivation to learn more about cybersecurity:

Male 908: "I've always been interested in technology – I've never had any training on it but I've always been interested, uhm, and it's

just reading any relevant articles or subscribing to various information sources about technology of any sort."

This interest in I.T. is sometimes manifested in following up cybersecurity information to understand the threats or solutions in more detail:

Female 903: "It would be something online that I read, perhaps there was a virus with a name and I Googled the name and that's where I got it from. It was one that had affected big firms or a big firm but it said it also had possibility to creep down the line to ordinary people's computers so I was a little worried about that..."

It is important to note here that there is likely to be a knowledge-action gap. In other words, just because a user has an interest in I.T., and therefore is engaged, it does not necessarily mean that they will act more securely [16]. That said, when a user is surrounded by people who understand and discuss I.T. – both physically and digitally – they are more likely to follow the behaviours of the group and absorb cybersecurity information casually, rather than having to specifically seek this information when needed:

Female 003: "...about a month ago my son came 'round and he was looking up something like a hotel and he said mum you haven't downloaded the latest download or update or whatever. He said do you ever update? I said occasionally, and he said you need to update – so he updated it..."

In the quote above, our participant explains how she learned about the value of keeping her devices up to date despite not actively seeking that information. This valuable unsolicited cybersecurity information could be key to preventing future breaches, yet she only learned about it because her son volunteered that information.

Previous work has identified that older users are less likely to hear about security and privacy information through conversation [12], and throughout our interviews it became clear that this statement was true. We learned that most of our older users had a very limited I.T. literate social network where friends *"aren't bothered with computers and that"* (Male 006), thus cybersecurity information was unlikely to be discussed with peers under normal circumstances.

4.1.3 Language. Language is a vital concept in user literacy given that if a user is unable to communicate using the correct vocabulary, then this will affect their ability to obtain new cybersecurity information. Understanding information plays a key role in knowledge-acquisition, given that the use of jargon or unfamiliar language will mean that users will not be able to process new cybersecurity information:

Female 909: "It's just... I don't have the language to understand what they're saying. I think that's a good idea but if I have tried it in the past and they start giving words out I do not know and then end up giving up. I know one should just look them up in the dictionary, but it gets more confusing."

If a user is unable to formulate a recognisable query, they may not receive the appropriate help. Similarly, if a user is unable to comprehend and use the correct cyber language when communicating with others, this might inhibit useful conversations:

Male 902: "So that is a great help to me, but the only downside is that I ring them up and try to explain it but I don't feel that I am explaining myself properly and I'm not sure if they will understand over the telephone."

There is also a relationship between a user's language level and their confidence in communicating about cybersecurity and poor confidence can undermine their ability to act effectively:

Female 911: "Yes. I would feel completely out of my depth looking into that. And I wouldn't have the confidence to go into my iPad and... uhm... I mean I was going to the security settings and things on Facebook – I'm always checking the security settings. But I wouldn't, like, go in and alter anything. I would like to have that confidence to know what I was doing."

The language situation for cybersecurity is not dissimilar to that in the health domain where specialised language alienates the general population and confuses their understanding of key terms, resulting in calls for simplifying the language used by professionals and the media [51].

4.1.4 Past Experience. Finally, past experience refers to how both positive and negative experiences shape an older user's perceptions of cybersecurity and affects their motivation to seek additional information. Bad experiences can affect cybersecurity hygiene (e.g. updates) and thus open them up to vulnerabilities and poor mental models:

Male P901: "...the latest update really slowed it down and I was really not happy. Because before the latest update I was still doing the job which I needed to do faster and with some efficiency and if something would upset that why on earth would you need to do that when you don't need it, you know? And that is why I am really cautious ever since then."

In effect, this bad experience changed his updating habits for the worse – opening him up to new cybersecurity vulnerabilities. Indeed, it has previously been reported that changes to the software's user interface can render previous experience useless [54], thus dissuading older users to update software on a regular basis.

When users hear about the experiences of others, it can also create mistrust:

Female 906: "I don't do online banking and I won't do online banking because I don't think, no matter how safe they say it is, I don't believe them. Because things keep happening, the NHS happened, the TSB fiasco happened, and my bank is TSB. Uhm, so I don't do anything like – there's no financial anything on my computer except for doing – for buying things and I do that because it's cheaper..."

As Female 906 articulates above, this lack of trust arising from bad experiences can be problematic by disengaging users rather than encouraging them to seek solutions. However, conversely, good experiences can work as gateways to more experimentation:

Female 007: "For a long time, I wouldn't buy anything online because I didn't trust any payment method. Even when people would say if it had a little lock on it, it should be alright. I just didn't like buying anything over the internet at all. But, since I've got the Kindle and I'm fanatical on reading books, I buy a lot of books. And, so I've started, uhm, very occasionally, I'll buy something other than a book"

Finally, taking up new roles can introduce older users to new technology, and, with it, new cybersecurity threats:

Female 903: "Well I'm a completely self-taught computer user, I've never been to any classes. At the point I joined I had just taken on editing a magazine, I'm only the editor I don't actually write it but I have to put it all together and in order to do this, I bought the latest

Word and I had to learn how to use it and until then I had really only used the internet, I suppose, for emails."

The role of past experience is thus vital and well recognised in the learning community. Good early experiences can facilitate the adoption of technology for older users but poor experience can alienate users for good, particularly older users who have established non-technical patterns of interaction in their daily lives [4].

4.2 Information Resources

Under normal circumstances, cybersecurity information was not actively sought by older users – this occurred almost exclusively when the need arose to fix problems. It was more common for this information to be obtained passively throughout normal daily activities.

We identified five themes describing the information resources an individual might draw upon in the cybersecurity context: Social, Community, Commercial, Broadcast Media, and Internet Media.

4.2.1 Social Resources. Social resources consist predominantly of family and friends close to the user. In many cases, social resources tend to be the first point of call for cybersecurity information and advice. While users may not expect their social resources to provide the required information or to fix the issue, they serve as a sense-making and sanity check first stop before continuing on their information-seeking journey:

Female 903: "Uhm, again, I would probably ask <son 1> first – if he said – he might say 'ignore it', you know, it's just not true... but he might say 'oh dear, you know, someone has got into your computer why don't you ask <son 2>' and if <son 2> didn't know I would take it round to my computer repair people to see if they knew what to do."

Older users turn to family and friends for cybersecurity knowledge, and in theory will prioritise people who have some experience using I.T. This includes people who are currently working in I.T., those that have previously worked in I.T., those who use computers, and young people:

Male 001: "<name> specifically, he knows so much about computers, he has set them up for his firm and what have you. So he is computer literate I would say..."

While older users generally prioritise the skills of their social resources in that order, ultimately it comes down to availability and what social resources are at hand to deal with queries. This means that in practice, an older user may end up approaching someone with less expertise within their social circles simply due to the fact that they are able to obtain an answer more promptly:

Female 903: "I would probably first of all ring <son 2> and say 'the tablet is doing so and so' âĂŞ and he would nearly always say 'well, switch it off and switch it on' and I would do that and if it didn't work, he would say either 'you can ring <son 1>' or 'I'll look at it when I come around some time'. So I might then send a message to <son 1> saying 'my tablet is doing this and that', and he might know the answer or he might not."

This is an important consideration, as even older users with access to I.T. experts may default to the least appropriate person simply due to being local or contactable. While the intent of older users reflects that of the general population [37] – in that competence of source is valued over other factors including trust, availability, cost, and closeness – in practice they prioritise the availability of source given their limited relevant social options and given their limited literacy. Again, we see a parallel with the development of a local, non-expert 'shadow security' culture within an organisation, where colleagues that work in the immediate vicinity develop their own norms and beliefs [27].

In addition to providing direct knowledge, social resources also play the role of brokers. That is, an older user may approach a friend or family member with the aim of obtaining a recommendation for someone else to provide the desired information or help:

Male 006: "He's a social friend, really. I might, uhm, mention in passing, I've got a problem I would ask him... but no, I wouldn't discuss computers with him, really... But if I've got a problem, because he's got his own business and he's got to be up to date, he knows people who, uhm, to sort things out for him, so I ask his advice on people, that's what I do."

Social resources can also serve as an encouragement for older users to engage with new technology, either actively or passively (e.g. [40]):

Female 905: "So I had an Australian friend come, and she had an iPad and she said how fantastic it was and it was driving her poor husband barmy because she was on it all the time. But I got interested and she persuaded me that it was a good idea so I went and bought one. We went together and bought it."

While it is a positive outcome that older users are encouraged to take up new technology, it is important that they are appropriately briefed about new cyber threats and countermeasures. A particular problem occurs when well-meaning friends introduce individuals to new threats, for example, by gifting second-hand devices:

Female 005: "Well, it was my brother's cast off, he gives me so much of his cast offs. So, he was there, but he's one of these, he says 'it is very intuitive, you work it out'. So, every now and then I'll be, 'I cannot get' or 'what do I do?' "

This highlights an important issue associated with hand-me-down devices: the lack of ongoing support and the assumption that the recipient is able to make sense of the device. This issue is explored further in Commercial Resources (see subsection 4.2.3).

4.2.2 Community Resources. Communities can be considered an extension of the social resource or they might be formal organisations and informal interest groups. In both cases, older users can be exposed to cybersecurity information, and provide an opportunity for information dissemination and advice seeking. These communities can also serve as brokers for older users to find peers or professionals to remedy problems:

Male 902: "...I was a member of an organisation at the time and she said that this was someone – the firm that she used, and it was geographically close to me..."

Special interest groups can happen both formally within organisations and also informally outside, with both offering an outlet for those interested in I.T. to discuss and learn more about the subject, including cybersecurity:

Female 903: "Yes I used to belong to their I.T. group and this was one of the things we were told about, that passwords, that crooks relied on people being lazy about their passwords and would be easy prey at the slightest opportunity."

Being part of a community means older users have 'colleagues' who may be able to help with issues that arise:

Female 904: "She gave it to me and said 'here, it may need charging up'. I didn't have a clue so luckily there was a fella in the charity shop who was a wiz with computers and things like this, so <name> set it up for me and he set it up so it would be easy for me."

Again, here we see the opportunistic nature of information seeking in older users and how having a community available supports their information needs.

Community-organised courses also contribute to older users' I.T. and cybersecurity information. Despite their value, however, older users explained their difficulties in finding relevant courses, and specifically how finding courses that were pitched at the right literacy level – and at their age group in particular – were very difficult to find:

Female 905: "Well, I have looked but, see, the thing is, I haven't found anywhere that I can get lessons for my age group – you know, because it's not as easy as you think it is, just go and do a class when you reach a certain age."

While the content of courses is important, the mode of delivery is equally important. Older users reported having attended face-to-face courses, and while acknowledged that online courses may be more convenient due to time constraints, they would most likely not complete online courses, supporting previous work on factors for disengagement with formal learning online [14].

Female 911: "A course probably. If it was online and I was doing it myself, I wouldn't do it... I think it would be too complicated and I think it would be too dry. I think I would start it, but, whether I would finish it would be a different proposition."

Ultimately, communities and events facilitated by communities give older users an outlet for improving their cybersecurity knowledge. In fact, these can be seen as replacements for the workplace information exchange with the caveat that experts providing the advice are likely to be less trained than those in the workplace.

4.2.3 Commercial Resources. Commercial resources consist of entities with expert knowledge on cybersecurity. These resources consist of large national stores, local shops, and professional freelancers, while covering both setup support and aftersales support:

Female 008: "I wanted the personal touch. Somebody who knows a little, knows enough about whatever you're doing, doesn't have to be a computer expert, but knows enough about your bid to be able to sort you out and if there's a problem I can go to the local shop, I like to support local businesses anyway, and I just wanted to spend £250 because I don't intend to be working for a lot longer."

The quote above emphasise the expectations that older users put on commercial resources, explicitly the requirement for local after-sales support. The quote also emphasises older users' need for availability, once again prioritising availability over expertise as with social resources.

That said, it is also important to highlight the official structures that are put in place by these commercial resources. The best example is Apple, who provide a range of user-friendly structures for users and are heavily utilised by older users when required. These structures include telephone, web, and face-to-face professional support, as well as a clear focus point for troubleshooting:

Female 911: "Because, I find them really good. I found them very helpful. You can ring them up, they give you an appointment straight away. Um, and if there's any problems going on, generally, we tend to know about them first. Obviously, with people going in so they will be able to say I'll look it's this or it's that or maybe do something over the phone, as well, that I could put it right."

Perhaps it is not surprising that older users rely heavily on commercial resources when available, given their predisposition to seek – and trust – advice from professionals [13] in other contexts. However, we should bear in mind that older adults have limited financial resources and, as we have seen, do not always buy their devices new. This means access to good quality information and advice can be restricted. Financial limitations play out in other cybersecurity decisions, such as the way older adult users may choose to install free antivirus software:

Male 006: "So, I try not to pay – I'm on my pension, that type of thing. And I don't believe in spending money unnecessarily. But, I'm quite happy with Avast. It's very intrusive and it's always got pop-ups, but you can limit them."

Sometimes these money-saving measures directly led to security issues, with one prominent example detailing her experiences of being compromised due to not paying to renew her antivirus software:

Female 960: "Because I hadn't paid anything. It was well past the first three months or whatever it had free, so I had at that point yes... being a tight wad..."

Financial constraints are not exclusive to older users, but we should perhaps start to consider that some older users share commonalities with low socioeconomic status groups and recognise that finances can limit their access to commercial and professional resources.

4.2.4 Broadcast Media Resources. Broadcast Media resources consist of television, radio, magazines, newspapers, and, to a lesser extent, the internet. Cybersecurity information is usually absorbed passively via the news (specifically via headlines), general interest programming, and television adverts:

Male 001: "Well I get a daily paper and if something was in the paper you know I would be aware of it, assuming that the headline was big enough to catch your attention - I don't read every paragraph."

Radio is a particularly interesting medium in this age group, and one that has been neglected in other studies describing the role of broadcast media [12, 42, 44]. Older users report relying heavily on radio information as they can listen over long periods whilst carrying out other tasks:

Female 002: "I mean, I do have Radio Four on quite a lot during the day when I'm indoors or even possibly out in the garden – I'll have my earphones plugged in and not particularly discriminating what I'm listening to. So, I don't put myself out to listen to those programmes, but frequently I don't turn them off."

Television advertisements are another interesting resource, given that few older consumers – especially those 65 and over – watch content 'on demand' [38]:

Female 009: "When you look on a TV we are all told about looking for the symbol for safe websites, aren't we – you look for the safe address... Well, it's the TV adverts, isn't it – it's regularly in the advertising slot between the programmes..."

The segmentation of the media is interesting. We already know that older adults are heavily reliant on the media for cybersecurity awareness [12], but we see here the different qualities of print, radio, and broadcast media. Returning to our discussion of threats earlier, news media can be sensationalist, focussing on major threats rather than everyday events (e.g. [41]) thus it is not surprising that exposure to television news has been shown to increase fear of crime [49]. On the other hand, TV ads are more likely to take a campaign focus, describing the kinds of coping strategies that might keep people safe online. We would also suggest here, that older adults' reliance on radio – and in fact a self-reported preference for radio – could be better exploited in order to supply older users with relevant and important cybersecurity information.

4.2.5 Internet Media Resources. The Internet is a particularly interesting resource when it comes to older users. Whilst younger users turn primarily to the internet for security information, and information more generally, (e.g. [12, 15, 42, 44]), older users appear to be more reserved when it comes to seeking security information using this resource and tend to avoid using the internet for this purpose:

Female 002: "I've got an induction hob where I live now and its not got a manual – what am I supposed to do with this! And the underfloor heating has a Honeywell control that there are no instructions for, so I've had to go online and look up things like that. So I will use it – but if it's something about something that's on the internet then usually I will ask questions first and that would be definitely a second resort."

This aversion is also true for social media, a resource that many of our participants avoided altogether. Those that did engage with social media used it predominantly for keeping in touch with family and did not report seeking cybersecurity information on these platforms, although may have come across this information while browsing.

There appear to be two main reasons why older users avoid using the internet for security information seeking. The first reflects the language barriers reported earlier (see subsection 4.1.3). This is similar to eHealth literacy, where older users report not feeling very confident when evaluating online advice [53]. The second is simply a lack of trust about the quality of cybersecurity advice available online. Older users seemed sceptical of anything they read that may in fact compromise their devices and services:

Female 009: "I Google quite a lot, uhm, I probably haven't Googled I.T. security and I think I would be sceptical about what I was seeing because I'm presuming that people who are anti-I.T. security who want to breach it will also be on the same search. 'Join me, I will protect your computer' – but who are you? So I have a scepticism about it...".

This scepticism reflects recent observations that users are becoming increasingly anxious about cybersecurity notifications. In a recent study, users were reluctant to report a cybersecurity incident, for fear that the notification itself was a form of attack [6]. For older users, particularly those who are more socially isolated and less digitally literate, this level of uncertainty makes it particularly difficult to access good quality advice.

5 DISCUSSION

This paper set out to explore what resources were favoured by older users for obtaining cybersecurity information, and crucially to understand the reasoning behind these choices. Below we present a summary of our main findings, followed by reflections on our cybersecurity information access framework, and finally recommendations for disseminating cybersecurity information to older users.

5.1 Summary of Findings

Our study finds that older adults who are regular internet users do not feel confident using the internet for finding security information or for troubleshooting security/technical situations. This is despite using the internet for a variety of other purposes, including seeking help in other domains. This paradox can be partially explained by a language disparity, where some older users are unable to articulate their problems or understand the information on offer. As a consequence, older users turn to family members or friends for advice and help, using a more opportunistic rather than strategic approach.

Unsurprisingly, older users did not seek cybersecurity information unless there was a proactive need, yet we show how information can be absorbed under the right circumstances to help mitigate future issues. Specifically, cybersecurity information can be absorbed from communities and from courses (e.g. [28]), but older users need to have a general interest in I.T. to be exposed to these in the first place. An interest in I.T. is also important for a user's social resources in order to facilitate information sharing. However, generally more older users are able to absorb cybersecurity information from listening to the radio, a less well documented resource in the literature.

Finally, we found that older users were introduced to new cybersecurity risks by friends and family. This happens when they received hand-me-down internet-connected devices without accompanying appropriate support, reflecting a pattern described in previous work [40]. In these cases, older users lacked any source of commercial support – an important resource for older users who owned new devices – and instead relied much more heavily on social and community resources. This was the case both for the initial setup of the device (e.g. making sure the factory reset was done properly) as well as for follow up queries. This is potentially a very important and underexplored cybersecurity issue.

5.2 Differences between Older and Younger Users

Younger adults typically rely on online news sources for information on topical cybersecurity threats [12], while we found that older users rely on broadcast media – more specifically radio.

For day-to-day threats, younger adults rely predominantly on work colleagues or contacts with IT expertise [42, 44] or perceived to be competent [37] with the subject matter. Meanwhile our older users prefer to rely on family members or commercial resources. Unlike younger users, older users are highly opportunistic when information seeking from social and commercial resources and they prioritise sources who are available immediately – even if they are less qualified to address the issue.

Younger users have been shown to benefit from cybersecurity champions and advocates [22] for motivation and translation and this approach may be fruitful for older adults. While friends and family would appear to act as cybersecurity advocates for older users, it is yet to be determined whether those social ties have the expertise to effectively take on those roles.

5.3 Identifying Vulnerable Older Users

In this paper, we presented a cybersecurity information access framework which details the cyberliteracy and information resources necessary for information seeking and consumption amongst older users. This framework presents four themes for Cyberliteracy (Legacy Knowledge, Interest in I.T., Language, and Personal Competence) and five themes for Resources (Social, Community, Commercial, Broadcast Media, and Internet Media).

In Figure 2 we illustrate the example information resources available to older users, plotting message content in terms of the prevalence of threat information vs. coping advice on the Y axis, thereby taking account of the importance of the threat vs. coping distinction that is found in PMT and other behaviour models. We plot the likely authoritativeness of the information source on the X axis (authoritative vs. unauthoritative). Here we can imagine quadrants representing four different information types: unauthoritative threat, unauthoritative coping, authoritative threat, and authoritative coping information.

While all types of information are important, we know from PMT that an individual's ability to respond to threats is crucial and is critically dependent on their self-efficacy beliefs and knowledge of appropriate coping strategies [23] and thus we identify this quadrant as particularly valuable.

We see that older users who are unable to access authoritative coping information are particularly vulnerable, given they rely on less trustworthy information to prevent or address threats. While having access to this information is an issue, older users must also possess good cyberliteracy skills to make use of these resources, e.g. to judge the trustworthiness of the information and advice, but also to understand the technical language and communicate their needs appropriately. As discussed earlier, there are various reasons why older users may not have access to authoritative commercial resources (e.g. finances, second-hand hardware, lack of awareness) and we should consider ways of shifting information sources towards that quadrant.

5.4 Towards Dissemination of Cybersecurity Coping Information

Older adults prefer face-to-face courses when it comes to learning about I.T. and cybersecurity. However, finding an adequate course – aimed at the right people and at the right knowledge level – is a challenging ordeal. Older users tend to reject online materials despite their convenience, supporting previous work on formal online learning [14]. Our advice would be to support communities (e.g. public libraries as well as private organisations) in organising and advertising courses and events that focus on adequate coping strategies (e.g. aimed at specific user groups, not one-size-fits-all [34]) given older adults' preferences for these type of resources [28]. The branding of these courses is of great importance, as simply focusing on cybersecurity training is likely to limit the general appeal.

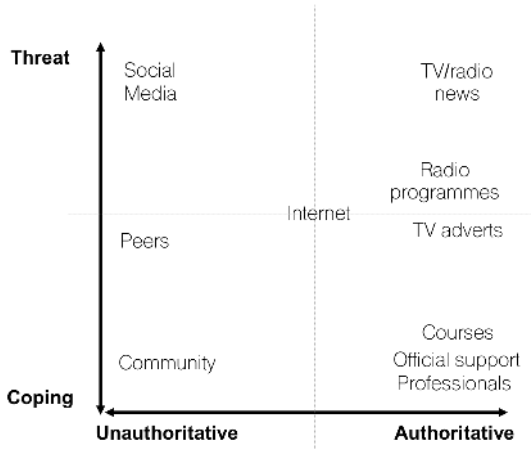

Figure 2: Cybersecurity information resources available to older users, plotted against message strategy (y) and authoritativeness of the information (x).

Our sample learned a great deal about cybersecurity from listening to radio. This was especially true of older users who lived alone. Thus, radio can be a vehicle for dissemination of both cybersecurity threat awareness as well as coping mechanisms. Radio can also serve as a publication vehicle for courses or other sources of information. Once again, it is important to remember that this content should appeal to a general audience who are not necessarily interested in I.T. and may lack digital literacy skills.

Finally, encouraging commercial providers to assist users with approachable and flexible information and support may be an indirect way of influencing older users' cybersecurity hygiene and facilitate their information seeking. As characterised by Apple users, older users are keen to use reliable commercial resources when available, which also creates new opportunities to freelance experts. Another approach could entail reaching out into the social network to find those with appropriate cybersecurity information, using these as cybersecurity advocates [22], although identifying who the key individuals are will require further exploration.

6 CONCLUSION

A series of interviews with internet users aged 65 and over revealed how good quality cybersecurity information is not easily available to all and has shown that a number of avenues for dissemination of good quality information exist. These include taught courses (for those interested in I.T.), radio programmes, television adverts, professional services, and expert friends.

We have also highlighted how older users are sceptical about using the internet for finding cybersecurity information and advice, despite this being an excellent resource for certain sorts of information. Their reluctance is partly explained by low confidence and a sometimes-poor grasp of the language of cybersecurity. Hence, different mechanisms are needed to help older users with cybersecurity protection and advice, perhaps taking advantage of media that they favour.

Finally, we have shown that older users prioritise their information resources based on the immediate availability of those resources, rather than on cybersecurity expertise. This can lead to the dissemination of poor-quality cybersecurity information and result in a heightened vulnerability to cyberattacks. Those unable to access authoritative sources of coping information are particularly vulnerable.

ACKNOWLEDGMENTS

The work presented in the paper was funded through the Cybersecurity Across the Lifespan (cSALSA) project (EP/P011446/1) from the Engineering and Physical Sciences Council (EPSRC), UK.

REFERENCES

[1] AgeUK. 2015. *Only the tip of the iceberg: Fraud against older people.* Technical Report. AgeUK. 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] Murat Akçayar, Hakan Dündar, and Gökçe Akçayar. 2016. What makes you a digital native? Is it enough to be born after 1980? *Computers in Human Behavior* 60 (July 2016), 435–440. https://doi.org/10.1016/j.chb.2016.02.089

[3] Linda M Alves and Steve R Wilson. 2008. The effects of loneliness on telemarketing fraud vulnerability among older adults. *Journal of elder abuse & neglect* 20, 1 (2008), 63–85.

[4] Yvonne Barnard, Mike D. Bradley, Frances Hodgson, and Ashley D. Lloyd. 2013. Learning to use new technologies by older adults: Perceived difficulties, experimentation behaviour and usability. *Computers in Human Behavior* 29, 4 (July 2013), 1715–1724. https://doi.org/10.1016/j.chb.2013.02.006

[5] Virginia Braun, Victoria Clarke, and Gareth Terry. 2014. Thematic analysis. *Qual Res Clin Health Psychol* 24 (2014), 95–114.

[6] Pam Briggs, Debora Jeske, and Lynne Coventry. 2017. The Design of Messages to Improve Cybersecurity Incident Reporting. In *Human Aspects of Information Security, Privacy and Trust (Lecture Notes in Computer Science)*, Theo Tryfonas (Ed.). Springer International Publishing, 3–13.

[7] Rajarshi Chakraborty, Jaeung Lee, Sharmistha Bagchi-Sen, Shambhu Upadhyaya, and H. Raghav Rao. 2016. Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems* 83 (March 2016), 47–56. https://doi.org/10.1016/j.dss.2015.12.007

[8] 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 (Jan. 2017), 74–88. https://doi.org/10.1057/sj.2015.23

[9] 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 (Oct. 2014), 285–318. https://doi.org/10.2753/MIS0742-1222310210

[10] 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.

[11] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2014. Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation. In *In Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*. ACM Press, 739–749. https://doi.org/10.1145/2660267.2660271

[12] 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)*. ACM, New York, NY, USA, 1:1–1:12. https://doi.org/10.1145/3173574.3173575

[13] Julie M. Donohue, Haiden A. Huskamp, Ira B. Wilson, and Joel Weissman. 2009. Whom do older adults trust most to provide information about prescription drugs? *The American Journal of Geriatric Pharmacotherapy* 7, 2 (April 2009), 105–116. https://doi.org/10.1016/j.amjopharm.2009.04.005

[14] Rebecca Eynon and Ellen Helsper. 2011. Adults learning online: Digital choice and/or digital exclusion? *New Media & Society* 13, 4 (June 2011), 534–551. https://doi.org/10.1177/1461444810374789

[15] A. Farooq and S. R. U. Kakakhel. 2013. Information Security Awareness: Comparing perceptions and training preferences. In *2013 2nd National Conference on Information Assurance (NCIA)*. 53–57. https://doi.org/10.1109/NCIA.2013.6725324

[16] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Marian Harbach. 2016. Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes. In *In Proceedings of Symposium on Usable Privacy and Security (SOUPS) 2016*. Usenix Association.

[17] Steven Furnell and Kerry-Lynn Thomson. 2009. Recognising and addressing 'security fatigue'. *Computer Fraud & Security* 2009, 11 (Nov. 2009), 7–11. https://doi.org/10.1016/S1361-3723(09)70139-3

[18] Vaibhab Garg, Lesa Mae Lorenzen-Huber, L Jean Camp, and Kay H. Connelly. 2012. Risk communication design for older adults. *Gerontechnology* 11, 2 (2012). /paper/Risk-communication-design-for-older-adults-Garg-Lorenzen-Huber/505aebb268aa5a1516571125b4e75e3982e960bb

[19] Galen A. Grimes, Michelle G. Hough, Elizabeth Mazur, and Margaret L. Signorella. 2010. Older Adults' Knowledge of Internet Hazards. *Educational Gerontology* 36, 3 (Feb. 2010), 173–192. https://doi.org/10.1080/03601270903183065

[20] Galen A. Grimes, Michelle G. Hough, and Margaret L. Signorella. 2007. Email end users and spam: relations of gender and age group to attitudes and actions. *Computers in Human Behavior* 23, 1 (Jan. 2007), 318–332. https://doi.org/10.1016/j.chb.2004.10.015

[21] C. Hale. 1996. Fear of Crime: A Review of the Literature. *International Review of Victimology* 4, 2 (Jan. 1996), 79–150. https://doi.org/10.1177/026975809600400201

[22] 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*. USENIX Association.

[23] Bartlomiej Hanus and Yu "Andy" Wu. 2016. Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management* 33, 1 (Jan. 2016), 2–16. https://doi.org/10.1080/10580530.2015.1117842

[24] Billy Henson and Bradford W. Reyns. 2015. The Only Thing We Have to Fear Is Fear ItselfÃćÂĂÅäand Crime: The Current State of the Fear of Crime Literature and Where It Should Go Next. *Sociology Compass* 9, 2 (Feb. 2015), 91–103. https://doi.org/10.1111/soc4.12240

[25] Trevor Hughes. 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/

[26] Sophie Nicholls Jones. 2018. Seniors too ashamed to report financial fraud, say experts. https://www.cpacanada.ca/en/news/canada/2018-06-15-seniors-too-ashamed-to-report-financial-fraud

[27] I. Kirlappos, S. Parkin, and M. A. Sasse. 2014. Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security. In *In Proceedings of Workshop on Usable Security*. http://dx.doi.org/10.14722/usec.2014.23007

[28] Victoria Kisekka, Rajarshi Chakraborty, Sharmistha Bagchi-Sen, and H. Raghav Rao. 2015. Investigating Factors Influencing Web-Browsing Safety Efficacy (WSE) Among Older Adults. *Journal of Information Privacy and Security* 11, 3 (July 2015), 158–173. https://doi.org/10.1080/15536548.2015.1073534

[29] Richard Philip Lee, Ben Thompson, Paul Whybrow, and Tim Rapley. 2016. Talking About Looking: Three Approaches to Interviewing Carers of People With Rheumatoid Arthritis About Information Seeking. *Qualitative Health Research* 26, 9 (July 2016), 1229–1239. https://doi.org/10.1177/1049732315599373

[30] 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 (Jan. 2013), 1–15. https://doi.org/10.4018/jisp.2013010101

[31] Andrew R. McNeill, Lynne Coventry, Jake Pywell, and Pam Briggs. 2017. Privacy Considerations when Designing Social Network Systems to Support Successful Ageing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 6425–6437. https://doi.org/10.1145/3025453.3025861

[32] National Cyber Security Centre. 2015. *Password Guidance: Simplifying Your Approach.* Technical Report. National Cyber Security Centre. https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

[33] Wan Ng. 2012. Can we teach digital natives digital literacy? *Computers & Education* 59, 3 (Nov. 2012), 1065–1078. https://doi.org/10.1016/j.compedu.2012.04.016

[34] James Nicholson, Lynne Coventry, and Pam Briggs. 2018. Introducing the Cybersurvival Task: Assessing and Addressing Staff Beliefs about Effective Cyber Protection. In *In Proceedings of Symposium on Usable Privacy and Security (SOUPS) 2018*. 16.

[35] Lorelli S Nowell, Jill M Norris, Deborah E White, and Nancy J Moules. 2017. Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods* 16, 1 (2017), 1609406917733847.

[36] Norbert Nthala and Ivan Flechais. 2017. "If It's Urgent or It Is Stopping Me from Doing Something, Then I Might Just Go Straight at It": A Study into Home Data Security Decisions. In *Human Aspects of Information Security, Privacy and Trust (Lecture Notes in Computer Science)*. Springer, Cham, 123–142. https://doi.org/10.1007/978-3-319-58460-7_9

[37] 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.

[38] Ofcom. 2017. *Box Set Britain: UK's TV and online habits revealed*. Technical Report. Ofcom. https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2017/box-set-britain-tv-online-habits

[39] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. 2017. Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 6412–6424. https://doi.org/10.1145/3025453.3025831

[40] Sebastiaan T.M. Peek, Katrien G. Luijkx, Maurice D. Rijnaard, Marianne E. Nieboer, Claire S. van der Voort, Sil Aarts, Joost van Hoof, Hubertus J.M. Vrijhoef, and Eveline J.M. Wouters. 2016. Older Adults' Reasons for Using Technology while Aging in Place. *Gerontology* 62, 2 (2016), 226–237. https://doi.org/10.1159/000430949

[41] Emilee Rader and Rick Wash. 2015. Identifying patterns in informal sources of security information. *Journal of Cybersecurity* 1, 1 (Dec. 2015), 121–144. https://doi.org/10.1093/cybsec/tyv008

[42] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2016. How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior. In *In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM Press, 666–677. https://doi.org/10.1145/2976749.2978307

[43] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2017. Where is the Digital Divide?: A Survey of Security, Privacy, and Socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, New York, NY, USA, 931–936. https://doi.org/10.1145/3025453.3025673

[44] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. 2016. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *In Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE, 272–288. https://doi.org/10.1109/SP.2016.24

[45] Jane Ritchie, Liz Spencer, and Liz Spencer. 1994. Qualitative data analysis for applied policy research. In *Analyzing Qualitative Data*. Taylor & Francis, 173–194. https://doi.org/10.4324/9780203413081-14

[46] David R. Roalf, Suzanne H. Mitchell, William T. Harbaugh, and Jeri S. Janowsky. 2012. Risk, Reward, and Economic Decision Making in Aging. *The Journals of Gerontology: Series B* 67B, 3 (May 2012), 289–298. https://doi.org/10.1093/geronb/gbr099

[47] Lynne D. Roberts, David Indermaur, and Caroline Spiranovic. 2013. Fear of Cyber-Identity Theft and Related Fraudulent Activity. *Psychiatry, Psychology and Law* 20, 3 (June 2013), 315–328. https://doi.org/10.1080/13218719.2012.672275

[48] Ronald W. Rogers. 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology* 91, 1 (Sept. 1975), 93–114. https://doi.org/10.1080/00223980.1975.9915803

[49] Daniel Romer, Kathleen Hall Jamieson, and Sean Aday. 2003. Television News and the Cultivation of Fear of Crime. *Journal of Communication* 53, 1 (March 2003), 88–104. https://doi.org/10.1111/j.1460-2466.2003.tb03007.x

[50] Kathleen Schreuers, Anabel Quan-Haase, and Kim Martin. 2017. Problematizing the digital literacy paradox in the context of older adults' ICT use: Aging, media discourse, and self-determination. *Canadian Journal of Communication* 42, 2 (Jan. 2017), 1–34. https://ir.lib.uwo.ca/fimspub/137

[51] Sue Stableford and Wendy Mettger. 2007. Plain Language: A Strategic Response to the Health Literacy Challenge. *Journal of Public Health Policy* 28, 1 (April 2007), 71–93. https://doi.org/10.1057/palgrave.jphp.3200102

[52] S. Talib, N. L. Clarke, and S. M. Furnell. 2010. An Analysis of Information Security Awareness within Home and Work Environments. In *2010 International Conference on Availability, Reliability and Security*. 196–203. https://doi.org/10.1109/ARES.2010.27

[53] Bethany Tennant, Michael Stellefson, Virginia Dodd, Beth Chaney, Don Chaney, Samantha Paige, and Julia Alber. 2015. eHealth Literacy and Web 2.0 Health Information Seeking Behaviors Among Baby Boomers and Older Adults. *Journal of Medical Internet Research* 17, 3 (March 2015). https://doi.org/10.2196/jmir.3992

[54] Kami E. Vaniea, Emilee Rader, and Rick Wash. 2014. Betrayed by Updates: How Negative Experiences Affect Future Security. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2671–2674. https://doi.org/10.1145/2556288.2557275

[55] Kim Witte and Mike Allen. 2000. A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. *Health Education & Behavior* 27, 5 (Oct. 2000), 591–615. https://doi.org/10.1177/109019810002700506

[56] Yixin Zou, Abraham Mhaidli, H., Austin McCall, and Florian Schaub. 2018. "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *In Proceedings of Symposium on Usable Privacy and Security (SOUPS) 2018*. USENIX Association.