Received: 2 June 2021 | Revised: 2 August 2021 | Accepted: 18 September 2021

DOI: 10.1002/hbe2.291

EMPIRICAL ARTICLE

WILEY

How do Older Adults feel about engaging with Cyber-Security?

Benjamin Morrison | **Lynne Coventry** | **Pam Briggs**

Department of Psychology, Northumbria University, Newcastle upon Tyne, UK

Correspondence
Benjamin Morrison, Department of Psychology, Northumbria University, Newcastle upon Tyne NE1 8ST, UK.
Email: benjamin.a.morrison@northumbria.ac.uk

Funding information
Engineering and Physical Sciences Research Council, Grant/Award Number: EP/P011454/1

Abstract

Older adults are increasingly a target for cyber-attacks; however, very little research has investigated how they feel about engaging in protective cyber-security behaviors. We developed and applied a novel card-sorting task to elicit how older adults feel about protective cyber-security behaviors and to identify the factors that impact their confidence in executing these behaviors. Nineteen task-assisted interviews were conducted with UK older adults. A thematic analysis revealed that older adults see protective online behaviors as important, but their reasons for disengagement fell into three categories: I do not want to (essentially, because the costs outweigh the benefits), I do not need to (e.g. because it is not my responsibility), and I am unable to (which includes heightened anxiety about doing something wrong). Underlying confidence around engagement with protective behaviors was a function of three factors: personal competence (related to good computer self-efficacy and relevant past experience), support (having a good network for information and advice), and demand (the effort of keeping up to date with the latest advice). Ultimately, we found that older adults are keen to protect themselves but are lacking appropriate support and we discuss implications for developers, researchers, and policy makers. This paper explores older adults' perceptions of common cyber-security behaviors. We introduce an effective card sorting methodology for security elicitation in older adults. We apply this to identify reasons as to why older adults may not engage in security behaviors as well as identifying a number of reasons why older adults actively avoid engaging in security behaviors.

KEYWORDS
aging, card sorting, cyber-security, emotion, HCI, older adults, online behavior, privacy, psychology, security self-efficacy

1 | INTRODUCTION

Older adults are the fastest growing population among computer and internet users (Friemel, 2016) and use technology for a number of reasons; from convenience activities such as banking (Van Boekel et al., 2017), shopping (Vroman et al., 2015), maintaining communication (Juárez et al., 2018), through to facilitating self-care and health management (Portz, 2017). Older adults recognize the benefits that technology provides for staying independent for longer, and many are keen to continue using technology well into older age (Betts et al., 2019; Morrison et al., 2020; Seifert & Schelling, 2018).

Like all users, older adults are at risk of cyber-attacks; however, they are specifically sought out by cyber criminals (Munanga, 2019). While much of the existing technology research surrounding older

adults has focused on adoption (Berkowsky et al., 2017; Chiu & Liu, 2017; Mitzner et al., 2019) and attitudes toward technology (Mitzner et al., 2010; Seifert & Schelling, 2018; Vroman et al., 2015), a growing literature base has started to focus on older adults' cyber-security vulnerability and online behavior.

Older adults are susceptible to certain types of attacks such as romance scams (Nicholson et al., 2019a, 2019b; Whitty, 2017) and consumer fraud (Shao et al., 2019). They are also an increasing target for phishing attacks and can struggle to differentiate between genuine and fake emails (Grilli et al., 2020; Lin et al., 2019). There is an argument that older adults, perhaps even more than their younger counterparts, should embrace protective actions, yet we know that older adults tend to exhibit low digital literacy (Schreurs et al., 2017) and low computer self-efficacy (Hunsaker & Hargittai, 2018; Yagil et al., 2016). They also tend to lag behind younger users in terms of awareness and expertise with regards to internet security hazards (Grimes et al., 2010), and they show less knowledge and lower confidence in performing protective behaviors than younger groups (Jiang et al., 2016). They can sometimes struggle with novel authentication systems (Nicholson et al., 2013) and they do not tend to use password managers (Ray et al., 2021). In short, older adults show a reluctance to fully engage with cyber-security behaviors, resulting from combination of low self-efficacy, mistrust, and a lack of awareness.

Older adults often doubt their own technical abilities, and this in turn inhibits their willingness to engage in novel forms of digital interaction (Berkowsky et al., 2017). In particular, they can find the management of online security to be an emotive experience, fraught with anxiety (McDermott, 2012). Yet, to date, very little research has investigated why older adults might fail to adequately protect themselves online, and why they lack confidence in managing their cyber-security (Lebek et al., 2014). Whilst trying to understand general differences in protective security behaviors, Jiang et al. (2016) found that older adults had less knowledge, confidence, and as such performed less security behaviors, than younger populations. If poor confidence undermines the ability of older adults to protect themselves online, then understanding more about the factors which affect self-confidence may be useful. Qualitative investigations are generally useful in this space, but it can be a real challenge to assess security knowledge and awareness in a population that might struggle to explain their competencies, actions and vulnerabilities, given digital literacy levels that are relatively low (Grimes et al., 2010). Interviews are useful, but are often more effective when accompanied by structured tasks involving prompts or provocations of various kinds.

Card-sorting and ranking tasks can be useful in qualitative research, as they increase simplicity for both the participant and the researcher (Pauwels & Mannay, 2019). Within organizational cyber-security research, Nicholson et al. (2019b) demonstrated the utility of a ranking task (the "cybersurvival task"), where employees were given cards, each describing a different protective behavior selected from organizations IT policy, and were asked to rank these in terms of their effectiveness in offering online protection. Their rankings were then compared with expert (CISO) rankings and in this way, misperceptions or points of misunderstanding were highlighted. Although a similar task could prove useful outside of workplace settings, no such tasks exist within the current cyber-security literature base. In addition to the rankings, the discussion around the task provides access to a rich source of qualitative data including underlying assumptions, misunderstandings, and ongoing behaviors which may not be as forthcoming in direct questioning about behaviors.

This study aims to address current gaps in the literature by introducing a novel card sorting task that allows older adults to simply express their beliefs and their confidence in a range of protective behaviors before using this task as a prompt for subsequent interview questions. The ultimate aim was to understand more about the factors that might inhibit older adult engagement with online protective behaviors. The study sought to answer two research questions: (1) why might older adults choose not to engage in protective online behaviors? and (2) what impacts the confidence an older adult has in executing such behaviors?

2 | METHOD

2.1 | Task development

Ranking tasks such as the desert survival task (Lafferty et al., 1974) and NASA's Moon Survival Problem (e.g., Hall & Watson, 1970) have been used in existing organizational based research for the purpose of understanding employees' knowledge and interaction with each other. These tasks typically require users to make decisions and weigh up items to determine their importance. Usually set within the survival context, participants are typically asked to rank items based on how important they would be in aiding their survival. Importantly, such tasks elicit understanding and attitudes in relation to the objects, as the items worth and value are based on the perceptions they hold about each item. Although these tasks were useful for understanding decision making processes and attitudes in occupational settings, they were independent of context, limiting their applicability to settings such as security.

Nicholson et al. (2019a, 2019b) were the first group to create such a task tailored specifically to a security setting. In the cybersurvival task (Nicholson et al., 2019b), employees were shown a set of 20 cards describing protective behaviors (e.g., use a strong password) and were asked to rank these in terms of cyber-security efficacy. Initially, the rankings were done individually, then they were reflected on as part of a workgroup, where people were encouraged to discuss the reasons for their top and bottom choices and where there was disparity between group members. Although this task was effective at aiding the understanding of end-users, its focus remained within organizational settings with items referring to organizational structures such as the "IT department" and "the network." Furthermore, the language used within their task was only appropriate for users with sufficient digital literacy to understand jargon terms such as HTTPS, something which older adults typically find difficult (Cook et al., 2011).

In the task presented within this paper, we developed cards describing nine "protective behaviors," created with as little jargon as possible, and written without any reference to occupational settings, meaning that each behavior could be carried out outside of the workplace. We also asked participants to sort these cards in two ways: first, as with the cybersurvival task, we asked them to conduct a simple ranking from most to least effective. This meant they were required to consider the value of each security behavior in relation to others and in relation to what they perceived to be the main threats. Second, we asked them to rate their confidence in executing each of these actions, as a measure of self-efficacy for each behavior, something known to affect the extent to which people will engage in cyber-defensive actions. To facilitate this, we developed a board layout where the effectiveness ranking was on the *y*-axis and the confidence ranking on the *x*-axis (see Figure 2).

The prompt cards were produced based on two sources of advice on how to protect yourself online. The first was the UK Government's CyberAware website, designed to be accessible by the general public. The second source came a published study on popular cyber-security behaviors (Ion et al., 2015) which was also used in designing the cybersurvival task. The final set of cards for this task can be seen in Table 1.

A game board was created with two axes (initially unlabeled). The *Y*-axis was then labeled "most effective at keeping me safe online" (top) and "least effective at keeping me safe online" (bottom) and participants were asked to place the cards representing each security behavior (outlined in Table 1) in rank order between these two extremes based on their perception of how effective these behaviors were at keeping them safe online. After all cards had been placed, each card was discussed in sequence from most to least effective, outlining the participants' understanding of the behavior and the reasons for the ranking. Following this task, two axes labels were added onto the *X*-axis. At the left-most extreme of the board, a card entitled "Not at all confident I could do this safely" was added, and on the far right, a card labeled "very confident I could do this safely." Participants were then asked to adjust each of their ranked cards along this *x*-axis and again were invited to discuss the reasons for their decisions. An overview of the card sorting task can be seen in Figure 1.

TABLE 1 Final set of security behaviors used in card sorting task

Behavior
Have software protection
Keep your device secure
Guard against phishing emails
Use strong passwords and keep them safe
Back-up data
Update software
Use public Wi-Fi safely
Maintain good online/browsing behaviors
Be aware of fake websites

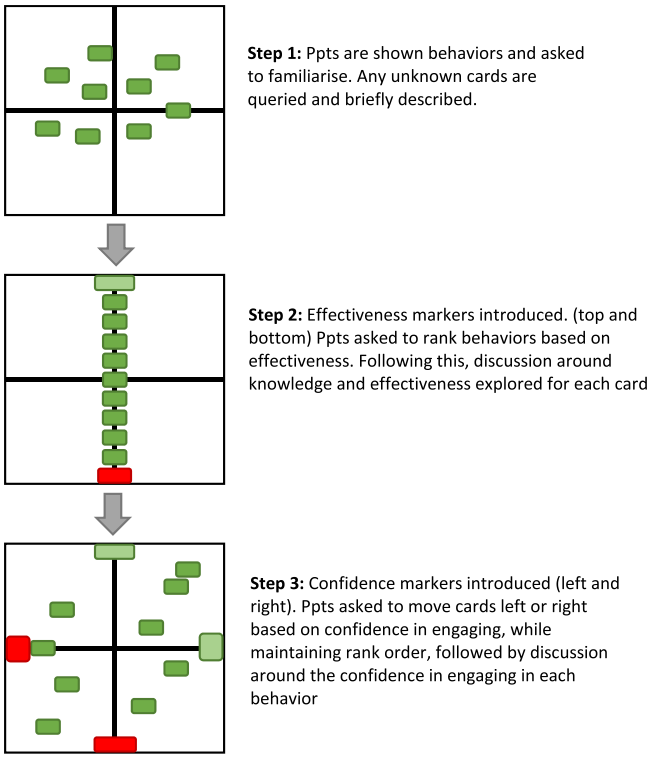

FIGURE 1 Visual representation of the card sorting task

2.2 | Participants

Nineteen older adult participants were identified predominantly through opportunity and snowball sampling (aged between 62–78 years old $m = 68.79$) from the North East of the UK during May 2019. We did not specify a target number of participants prior to conducting the study, due to the difficulty in establishing such figures in qualitative research (Levitt et al., 2018). Rather, we ceased recruitment and data collection at the point which "no new themes or information arose" (Guest et al., 2006), often termed data saturation. The number of participants is in line with other qualitative studies in the area of cyber-security (Durrant et al., 2017; Fujs et al., 2019; Olivier et al., 2015). Table 2 provides an overview of the demographics of participants who took part.

2.3 | Procedure

Ethical approval for this study was granted by a School of Psychology, University of Northumbria Ethics Committee. Following consent procedures, participants were introduced to the task board (see Figure 1). The set of protective behavior cards (Table 1) was then placed in front of the participant, and they were asked to familiarize themselves: indicating whether there were any behaviors they did not understand. The researcher responded to any unknown cards with minor clarifications designed only to aid comprehension, using as little detail as possible to avoid any unintended bias. The participant was then asked to sort the cards in order of how effective they believed they were at keeping them safe online. Following the ranking, the researcher briefly

TABLE 2 Participant demographics

Participant	Age	Sex	Pre-retirement occupation
P1	74	F	Worked in a range of retail roles
P2	78	F	A range of roles retail roles including a bookshop
P3	73	F	Teacher in a range of artistic disciplines
P4	67	F	Social worker
P5	66	F	Worked for a charitable funder
P6	68	F	Social worker
P7	71	F	Mental health nurse
P8	61	F	Chemical manufacturing engineer and manager
P9	72	M	Medical secretary
P10	72	F	Medical receptionist
P11	71	F	Legal secretary
P12	61	F	Teacher
P13	65	F	Teacher married to P12
P14	67	M	Teacher
P15	62	F	Teacher
P16	65	F	City Council worker (Library and Intranet)
P17	68	F	Salesperson for labeling marketing company
P18	75	M	Head of Computing (School) Married to P6
P19	71	M	Teacher

discussed each card with the participant from most effective to least effective. For each card, the interviewer asked for a brief explanation of the action on the card and whether or not they engaged in that behavior (and their reasons). After all cards had been reviewed, participants were asked to retain their original rank order, but to move the cards left or right based on how confident they would be in engaging in those behaviors, with the least confident behaviors placed toward the left-hand side of the board and the most confident toward the right-hand side of the board. For each card, they were asked why they chose that position and what factors might impact their confidence in carrying out the behavior. It was made explicit to participants during the second part of the sorting task (the confidence sort) that the positioning of the cards was based not on whether they *currently* carried out the behavior or not, but instead, *how confident they would be* in carrying out the behavior if they were asked to do so. Discussion once again started at the top card and proceeded toward the bottom card, after which a photograph was taken to note the final order. A visual representation of the task can be seen in Figure 1 and completed participant examples can be seen in the Figure A1. Interviews were subsequently transcribed and analyzed according to the analysis procedure (outlined further ahead).

3 | RESULTS AND DISCUSSION

3.1 | Ranking task—protective effectiveness versus efficacy

A visualization of the overall outcome of the ranking task is shown in Figure 2. This was calculated by assigning a score of 9 to the behavior seen as the most effective protection and a score of 1 being assigned to the behavior seen to be the least effective. We calculated confidence scores by overlaying a 10×10 grid over the completed task, allowing us to calculate the mean confidence for each of the behaviors. Note, however, that this we are not intending this visualization to be used as a quantitative dataset given the limited number of participants in the study. It is however useful to demonstrate for our participant group, what the overall pattern is in relation to both perceived efficacy of actions and user confidence.

Figure 2 indicates that this sample saw having software protection, using strong passwords and keeping their devices secure as the most effective protective online behaviors. Generally, confidence ratings were high, with participants showing the greatest confidence in password use and keeping their devices secure.

3.2 | Interview analysis procedure

Data were analyzed using Braun and Clarke's (2006) Thematic Analysis approach. This approach, used widely in qualitative research, consists of six steps; familiarization with the data, generating initial codes, searching for themes, reviewing themes, defining and producing themes, and finally, producing a report. A further description of these stages, alongside recommended guidance for their conduct, is outlined within the Braun and Clarke's (2006) paper.

Familiarization was achieved through the interviewer conducting the interviews, transcribing the data, and reading and rereading finalized transcripts. No software tools were used in the data analysis. Instead, thematic analysis was conducted by hand. Transcripts were

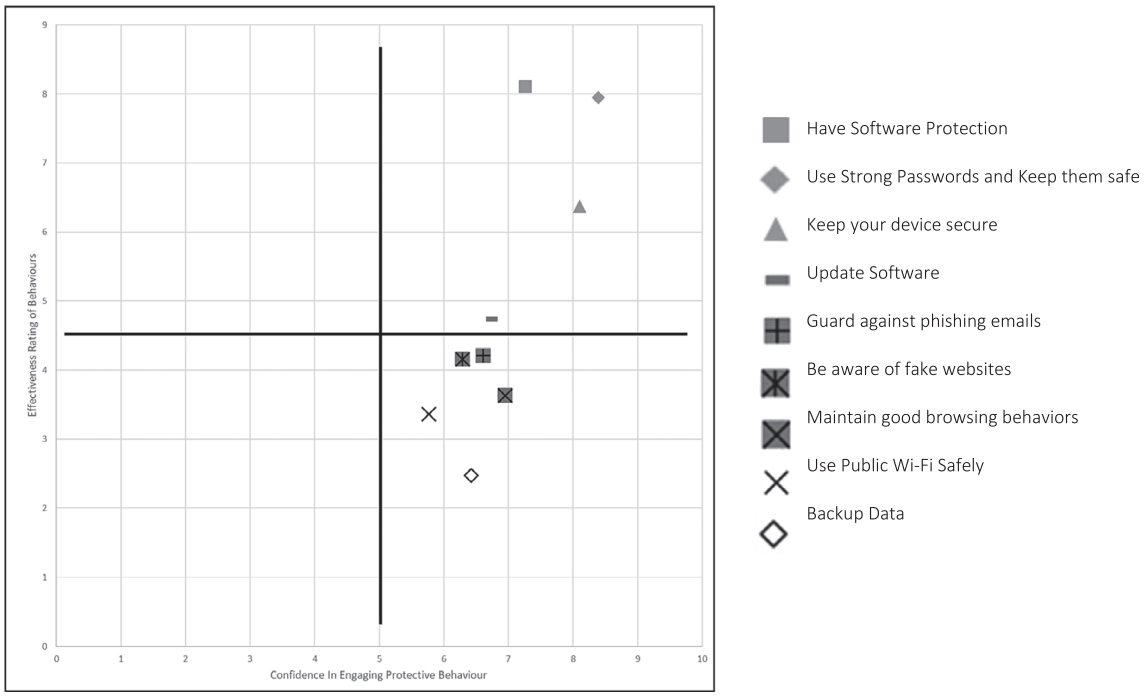

FIGURE 2 Visual representation of mean placement of cards

printed and coding was conducted in paper form, using brief margin-based descriptions with interesting extracts highlighted. Extracts were then cut out and grouped, after which they were further grouped into early themes. The interviewer then worked with the two other authors to review the themes. Each theme was scrutinized for relevance of quotes as well as appropriateness of subthemes, with revisions agreed where necessary. In the following sections, we discuss how these maps relate to the qualitative data and answer each of our major research questions.

3.3 | RQ1: Why do older adults choose not to engage in protective online behaviors?

Discussions around why older adults choose not to engage in protective online behaviors revealed three overarching themes, that they: do not want to, feel unable to, or feel that there is no need to. Descriptions of themes and subthemes are as follows.

3.3.1 | I do not want to

Participants were reluctant to engage in security practices for several reasons: largely related to the perceived cost (in terms of effort, convenience, and money) associated with more stringent security behavior. The first point they made was that security updates would often cause problems down the line, meaning they would have to relearn aspects of the system. They were unhappy when any changes meant that the layout, look or feel of the interface changed.

> P13: When I get a message on my phone or my laptop, I try to ignore it because when I do that it changes everything around and I don't know where it is, and I have to re-learn that and I don't like that very much so I tend to ignore it…

This finding supports earlier research from a younger US-based population which found that changes to user interfaces (UI) are considered one of the most negative aspects of updating and a driving factor behind refusing future updates (Vaniea et al., 2014). These findings suggest that mandatory security updates might usefully be kept separate from optional feature updates.

Another barrier related to the updating of antivirus software, where participants often felt that purchasing additional software was a requirement, or that seeking out free updates might lead to the accidental purchasing of unwanted packages. Aggressive marketing during the update process was highlighted by some participants.

> P19: When it gets updated the first thing it does, before you can actually do the update, is it tries to sell you the other things that can go along with it. I'm not interested in that but if you happen to make a wrong click you might find that you have bought something you don't want.

This "pushing" of related software eroded trust and led some participants to suspect that antivirus software was as an unnecessary financial cost.

> P17: That's why I haven't got any software protection, because I think that it's a waste of money.

Older adults' purchasing decisions relating to protective software are complex. For many, the costs associated with purchasing protective software are too high and are seen as not justifiable in terms of what is returned in security gains (Coventry et al., 2014). This, however, does not explain why older adults refuse to update free software already installed on their devices. The quotes above, although on the surface suggestive of financial concern, perhaps reflect older adults feelings of low computer self-efficacy (Marquié et al., 2002), with concerns around accidentally agreeing to unnecessary purchases. This may lead these individuals to become particularly vulnerable, especially if access to appropriate support is limited (Nicholson et al., 2019a).

Aside from cost, effort was also a barrier and updating ate into the time they would rather spend doing other things.

> P7: I like to try things, you know, I like to give it a go but eventually it gets frustrating. If you think, it's probably some silly little thing that I'm doing, why am I sat here all day when I could be walking along the beach with the dog? I'll ask somebody else and they can sort it.

As well as general inconvenience, participants discussed how security might have "gone too far," with "unusable" security leading to avoidance and frustration.

> P12: it doesn't accept the fingerprint, it says; you've tried ten times to get in, put your pin number in. So I don't know if between the two of us that we have given up, but's that's the thing, sometimes things are so secure that you think, it's me! And it is my device so why don't you let me in, you know…

> P1: Every time I went into my bank account they never realized my password and I had to keep changing the password, and then they wouldn't recognize it again and I thought… blow this… so I just don't bother any more.

A significant literature has shown that poor usability can adversely affect security behaviors (Fagan & Khan, 2019; Nurse et al., 2011). Some technology acceptance models, such as the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003; Venkatesh & Bala, 2008) (and its newer iterations), recognize usability as a key determinant of technology use, and indeed usability is a known problem for a range of technology acceptance issues (Mitzner et al., 2010; Nägle & Schmidt, 2012; Seifert & Schelling, 2018). Whilst there is now a body of work on "usable security," little is targeted toward older adults.

In relation to ease of use, participants were aware of software such as password managers, designed to make life simpler, but there was a general suspicion about these:

> P15: I'm fearful that 'get that one and they get everything', and I understand that they… the keychain set up is such that theoretically it is a lot better than memory but there is a sort of personal controllability assorted to it.

> P18: I'm reluctant to use these packages that look after your passwords for you because if they get cracked, it's all there.

Ion et al. (2015) reported that those who are more likely to use password managers are also more likely to demonstrate higher levels of expertise than those who do not. In a sample of 18–64 year olds, Fagan et al. (2017) supported these findings demonstrating that those with higher technical expertise were more likely to use password managers. Interestingly, one of the main reasons provided by *non-users* in their study choosing *not* to engage in using password managers was related to security concerns. This study supports these findings in an older adult sample, although due to the qualitative nature of this study, there are limitations to the generalizability of this result. The use of password managers remains a contentious debate as some research suggests that despite expert recommendations, password mangers may still lead to vulnerabilities (Fagan et al., 2017; Li et al., 2014). As such, their use or nonuse may not point directly toward vulnerability; however, understanding the reasons for engagement (or disengagement) with such systems provides insight into older adult's online security motivations.

3.3.2 | I'm not able to

In this theme, we see that many older adults lack faith in themselves in relation to security behaviors. There were several reasons for this; some participants felt that, if left to them, something would go wrong, or simply felt overwhelmed by the demands of maintaining secure passwords or keeping up to date with the latest security advice.

Fear was a critical issue and many of our participants catastrophized the risks they took when attempting to protect themselves online.

> P3: Well there are a lot of things I know that you need to do but because I don't understand them I don't do them. Because I'm always scared that I'm going to push the wrong buttons and do the wrong things, lose everything that's on the program.

> P1: It's… fear of the unknown shall we say. Because knowing my luck everything would go wrong and the

> computer would blow up or something. It stops me playing around with it in case I do something stupid.

Not all participants were worried about data loss; however, one participant discussed how their fear revolved around generating a vulnerability to attack, rather than losing data.

> P10: well someone would say to me, oh well that's alright and I think well I'm not doing it, I don't know… I don't know why… I just don't want to be scammed, I'm very careful about it [laughs]

On several occasions, participants related their own low perceived self-efficacy to the possibility of major losses. One theoretical model which might help to understand this anxiety is the Transactional Theory of Stress and Coping (TTSC) (Lazarus & Folkman, 1987). Grounded in coping theory, TTSC suggests if the stress associated with a perceived threat is low, the individual can engage in "problem-focused" coping, seeking reasonable solutions to solving the problem. If stress is high, however, the individual instead engages in "emotion-focused" coping–coping aimed at making them feel better, leading to denial of the problem and other ways to disassociate themselves from it. Although this model seems useful, as yet there is very little research that has applied the transactional theory of stress and coping to cyber-security.

The sense of being overwhelmed or unable to cope was a strong theme. This was often discussed in relation to password behavior:

> P19: My biggest worry is you have got something and you can't remember your password and you can't get into it.

> P13: My big failing is that most of my devices have the same password and I know that if somebody found that, all of my bank accounts and all sorts would have the same… [sighs] I should change them… but I wouldn't remember them.

This fear of forgetting was present in a number of participants and even those who were aware of the latest password advice found that the fear of forgetting new passwords was a deterrent:

> P16: I think possibly because I haven't got onto the strongest recommended type of password. I don't know why I haven't really… it's a bit silly isn't it? It's ridiculous really isn't it? When you think well that is a stronger password, why aren't you using it? But it's probably the fear of forgetting is what it is… But then I would have to write it down wouldn't it? Somewhere… so I don't know…

> P3: Well I could do that… (use three random words) but I would have to write them down though which then negates it doesn't it?

Woods and Siponen (2018) present the argument that password memorability is an "imperative" issue. They argued that users can typically remember more passwords than they believe they can, but also noted that they lack perceived control over their memory, lack the motivation to remember, and do not understand how their memory works. That said, most of their sample were aged late 40s or younger 50s. Older adults who report not being able to remember passwords, may in fact be telling the truth and certainly there are marked age differences in password recall (Nicholson et al., 2013), but there is relatively little evidence with older adults under-researched in password security research (Vu & Hills, 2013).

The decision to write down passwords, something which had previously been considered poor password practice (Adams & Sasse, 1999; Duggan et al., 2012) has now become an acceptable and even necessary trade-off for a number of participants, who had devised a range of strategies to ensure that passwords remained secure, typically writing passwords as prompts or in an encrypted format:

> P5: The difficult with passwords you see, is you're supposed to have lots and you're not supposed to write them down but that isn't actually possible, unless you have got some sort of photographic memory or something you know… So you have to find some sort of way that you think to have lots of sorts of passwords and be able to access them without giving them away, and I'm fairly confident that the way I do it you would actually have to know what the main words were before you get very far at all…

> P17: Because I can't remember them (passwords) that's why. But I haven't got them written down as they are, I know what they are but nobody else would know.

Our findings here support earlier work which demonstrates that older adults are prone to writing and storing passwords, and supports the notion that the reason for this is due to fears of forgetting them (Merdenyan & Petrie, 2018). This is in marked contrast to younger adults who typically prefer to remember passwords, regardless of whether they are asked to write them down or not (Boothroyd & Chiasson, 2013). Conversely, it may be that older adults value greater password security more than younger adults, something which is suggested by earlier password sharing literature (Whitty et al., 2015).

Finally, some participants simply felt that they did not have the knowledge of *how* to protect themselves.

> P4: Well, I wouldn't know where to start (Updating Software) and I wouldn't know when, sometimes I can remember, like at work you were meant to switch off your computer and it would update and whatever, I think mine possibly does that, I've not used it for a long time and my phone does updates but I wouldn't know how to updating something, do you know what I mean? Well not without automatic anyway.

Such issues have typically been discussed in terms of a "digital divide," although many recent researchers recognize that there has been a blurring of the boundaries in technology inequalities between older and younger adults, a term described as a "gray divide" (Friemel, 2016). Akin to the findings of Schreurs et al. (2017), this study found that modern day older adults are keen to learn, but at times are embarrassed by their limited knowledge. This sense of shame is a genuine barrier to progress and future research might focus on ways to empower older adults in this space. Increasingly, older adults are leaving the workplace with greater levels of digital literacy, and as such are blurring the lines of the gray divide further.

3.3.3 | I do not need to

In this final section, we turn to those adults who simply do not see security as their problem, either because they feel that threats have been exaggerated, or because they believe that their devices are already equipped with the necessary protective software. In both cases, we find some interesting mental models around exposure to threat:

> P17: I just feel it's in the house and it's secure in the house, nobody can use it apart from me

> P7: It's unlikely that they are going to do that (ransomware attacks) to individuals unless you are somebody with some status or some money, what benefit is there? There is nothing that I've got that anybody would want.

A wealth of previous literature has demonstrated that people typically demonstrate an unrealistic optimism for internet events, seeing themselves as less likely to become a victim than others, and more likely to have positive experiences than others (Campbell et al., 2007; Cho et al., 2010). Wash (2010) also found mental models relating to attackers targeting "Big Fish" in home computer security as did Redmiles et al. (2016), with participants considering themselves not to be at risk. One issue with this previous literature however, like many areas of security research, is that findings are based heavily upon younger cohorts. The findings here suggest that similar unrealistic optimism biases, and similar "big fish" mental models, may also be present in older adults.

The second issue—feeling that security was not their responsibility—was typically accompanied by a rationale that described their "role" and that of others in the device ecosystem. Sometimes these others were household members, but sometimes they were the device or software manufacturers:

> P6: If it was on my computer at home, I wouldn't be confident. It has got the protection, but I would leave that to my husband to do, it's not my responsibility.

> P18: Norton now have got warnings of possibly fake sites or ones to be a bit wary of, but they should really protect you against I would think all threats, that's what we pay them for.

> P6: Whoever provides your computing services, it is also their responsibility to you as a user and presumably their knowledge and expertise is in protecting their users

Interestingly, one participant likened engaging in security protection to how they manage their car.

> P10: Update it? Erm… I just don't know what I'm doing so I don't do it. It's like the car, I never sort of mess about with the engine, it's not my problem.

This delegation of responsibility may be seen as a way that users can resolve anxieties around wanting to remain safe whilst online, while knowing that they do not have the knowledge or understanding to manage their security safely. Relying on trusted others, whether this be a relative or a paid professional was seen as an acceptable way to detach from the responsibility of having to engage in such behaviors.

> P5: Cyber safety and whatever… simply because I don't understand it and I know I don't, so if somebody I trust has put software protection on my machine then good, but I don't take any ownership in a sense if you see what I mean.

Detachment from security responsibility poses a dangerous issue for cyber-security vulnerability and has been seen in recent workplace based literature (Nicholson et al., 2019b). The reliance on trusted others does not always mean that those others may be available and the reliance on software does not imply that all threats will be detected. Effectively, dismissing personal responsibility can mean that users do not learn, and they do not require any resilience in the longer term.

3.4 | RQ2: What impacts the confidence an older adult has when engaging in protective online behaviors?

The second research question related to the confidence that older adults have in relation to protecting themselves online. Following analysis, three major themes were identified which were seen to impact upon older adults' confidence in protecting themselves online: personal, support, and demand factors.

3.4.1 | Personal factors

"Personal factors" describes the individual-level characteristics or competencies that impacted confidence. Perhaps unsurprisingly, low levels of perceived computer self-efficacy were critical.

> P4: Because I don't understand techy things, I tend to avoid them at all costs, whereas I think some people are better at sitting down and playing with things

> P15: You know, you're just wary of it and I know from friends who are very computer savvy, there are times when I say hang about, I don't quite know what I'm doing here and because of that I couldn't say I'm confident.

Note that beliefs about low computer self-efficacy are not always justified and older adults often underestimate their actual computer knowledge (Marquié et al., 2002). However, perceived computer self-efficacy is important for short term (Czaja et al., 2006) as well as long-term technology adoption (Mitzner et al., 2019) in older adults.

A related issue is the extent to which participants felt that they had any control over the situation. The more perceived control they had, the more confident they were about engaging in those behaviors.

> P15: (when asked why strong passwords were more effective than updating software): Because that is something that is down to me, I can control it.

> P3: Well I always think of financial things, like banking, but I never do banking online, mainly for that reason… [Interviewer: What reason?]. Mainly because I'm worried about not being in control of it.

Locus of control is a well-researched concept and has previously been used in information security research to help understating why people may or may not engage in security behaviors (Workman et al., 2008). It is believed to be "crucial" in encouraging information security policy compliance (Ifinedo, 2014) and the findings here support earlier information systems literature and the suggestions of Bada et al. (2019) who posit that promoting feelings of control should be considered when developing future security awareness campaigns.

Finally, there is a kind of virtuous circle such that engaging in protective behaviors promotes confidence which leads to further engagement.

> P8: If I'm doing something all of the time, I tend to feel a lot more confident about what I'm doing.

Unsurprisingly, there is a significant literature which shows that prior experience of conducting a task leads to greater feelings of comfort within those tasks (Chung & Monroe, 2000; Hicks et al., 2000). We know that "past behavior is the best predictor of future behavior" not least because of the confidence generated by repeated success (Ajzen, 2011). This posits an interesting question when we consider the extent to which security processes should be made manual or automatic as the latter is clearly low-demand but does not support learning in any sense.

3.4.2 | Support factors

Support factors relate to the kinds of support network available to an individual, both formal (e.g., via professional support) and informal. The relationship to confidence is interesting here, because some participants suggest they would use their support networks as an opportunity to learn and gain greater confidence, whereas for others, support was simply a matter of someone else "fixing" a problem, which meant that they remained dependent upon others and were happy about this, providing that they trusted the competence of the other.

Many of our participants rejected that dependence, and sought to learn, believing that they *could* complete a range of security behaviors, if they were shown what to do.

> P1: if I was going to set up a password on my phone, I would be happy if somebody showed me, I am the kind of person where if somebody could show me how to do it, I am quite happy, then I will try it on my own but I won't try it without somebody to advise me what to do.

> P7: (when asked about backing up) I have probably forgotten it all now, but if he had just sat down with me for a short while and talked to me about it for a few minutes then I am pretty sure that I would be able to get on and do it.

Participants also reflected that they would feel comfortable carrying out tasks such as engaging in protective online behaviors if they had instructions that they could follow.

> P5: I'd be confident to work it out or to following the instructions, I wouldn't be confident doing it off my own back, but yeah…

> P12: I think I would manage it if I had the information on how to do it.

The findings here support recent literature (Betts et al., 2019) which suggests that older adults have a "thirst for knowledge" relating to technology and have a desire for digital technology sessions to teach them the essential digital literacy skills they require. Martínez-Alcalá et al. (2018) demonstrated that not only can older adults benefit from digital literacy training, but also suggested a "blended workshop" platform by which this learning can be particularly effective. In a UK sample, Fletcher-Watson et al. (2016) demonstrated the acceptability and feasibility of a 6-week training course in digital literacy aimed at older adults, finding almost 100% attendance throughout the course, and a large increase in reported self-efficacy following the course. Similarly, recent work by Nicholson et al. (2021) has demonstrated the effectiveness of a security training intervention designed at empowering older adults to provide support to peers in the community.

Support structures, such as those referred to above, were not always available to some of the older adults interviewed. Some participants discussed how they paid for professional help and relied on this for technical support. The trust that they had in these individuals was key.

> P5: I don't think I have any confidence in my ability to use software protection, but I think I have bought good software protection and I suppose one of the reasons I am more confident in that is that it is out of my hands, it is something that was recommended to me by someone I trust, so I don't feel like I have any input in that, but I'm confident in it.

> P4: I just prefer, if I know somebody who is confident to do it, that I trust and know, rather than somebody I don't, if they have a shop in a local village or something… it's like buying something isn't it, you wouldn't buy something from a market trader if he wasn't there every week, but if he was you could always go back.

Previous literature by Nthala and Flechais (2018) found five factors considered by older adults when assessing a source of support: perceived competence, trust, availability, cost, and closeness of the source. In this study, trust was an important factor for participants who did not have access to readily available support. Interestingly, some participants described their paid IT help as "friends," due to having known and relied upon them for a long period of time, even though any assistance was still charged at full price and as a paying customer. Delegation of security responsibilities may provide some cover for those who can afford it, however this leads to two key issues: (1) many cannot afford such support and (2) even in those who can afford support, many attacks are social-engineering based and as mentioned above, pre-established protection can only protect an individual so-far. Delegating responsibility is likely to lead to an "it's not my responsibility" mentality, something which is less favorable than the promotion of personal security.

Reliance upon friends and family produced more mixed results, with less learning and poorer long-term effects upon user confidence.

> P7: when I got it my son came around and said "oh, I'll set this up" and he set it up and I said thank you, and then he did it and buggered off and so I have to phone him up and say "well, what do I do about this?"

> P3: You see my husband always set everything up, I've got virus protection that he put on it for me, but it worries me that it's going to run out and I won't be able to do it myself.

Again, we see that older adults are keen to be *shown how* to protect themselves. Although previous literature has demonstrated that receiving some intergenerational support can be useful for older adults: sometimes even improving self-efficacy (Damodaran & Sandhu, 2016), the method of its delivery is important to its success. When older adults rely on younger members of the family, who may be particularly impatient (Xie, 2007), the device may be taken from them and the task completed without any education, leaving the individual unprepared when the situation arises again (Sandhu et al., 2013) and promoting dependence on those who can provide support, something which is problematic when these individuals are not readily available. Policy makers can help here, by providing accessible information for older adults, but more importantly, cocreating and codesigning alongside older adults when implementing strategy designed to promote technological learning.

3.4.3 | Demand factors

The final theme related to task demands, where we identified two key factors: the simplicity of the process and the demands of staying up to date. Regarding the first issue, our participants described Apple devices as relatively simple when engaging in behaviors such as updating.

> P16: I think Apple is easier than the laptop, I think I'm probably more confident with the phone and the iPad then I am with the laptop which isn't an Apple.

> P19: See I think one of the reasons I like the iPhone and the iPad is that when it comes to loading new software it's easy. It's absolutely easy whereas the laptop, it's not as straightforward and sometimes causes problems

Simplicity is important in understanding *why* information security advice is followed (Redmiles et al., 2016) and underlies engagement with a range of protective behaviors including adoption of two-factor authentication (Holmes & Ophoff, 2019). Ease of use builds confidence and increases intention to engage in protective online behaviors and is thus a key factor for the design of future systems.

A second demand factor related to the need to keep up to date with the latest advice. Participants referred to "the padlock" (signifying https security) and explained how the advice they receive around threats such as this has previously changed, forcing them to relearn to stay safe.

> P16: I think that things change all of the time, and so I'm always slightly wary of what I'm doing, like the padlock, before I was like, oh I have to look for the padlock but now I'm thinking, well that doesn't actually mean very much so I think there are always things to learn.

In addition, participants referred to the digital vigilance required to stay safe online, and the possible repercussions of falling into a "false sense of cyber-security."

> P18: Because in a moment of relaxed state of mind you could, if you were doing a search or even a link to it that would pop up on a google search or something like that, if it looks genuine and if you're not actively thinking make sure this is not a fake website, it could easily happen and draw you in.

Here we see the relationship with an emerging literature on "security fatigue" (e.g. Stanton et al., 2016). Whilst most of the literature on security fatigue relates to younger, often "working-age" adults, it may be particularly difficult for retired older adults, who lack workplace support. In work, they might have received relevant updates, but outside of this setting have to be more self-reliant when trying to navigate the often-inconsistent communications from businesses and government. Several participants discussed inconsistencies and misconceptions such as those relating to https/padlock security throughout the study, something which has also been found in similar work in a US older adult sample (Frik et al., 2019). These suggest that future campaigns should focus on establishing easily digestible messages or the promotion of mental models, which highlight the changing nature of threats and make older adults more resilient to changes in security advice.

The possession of good, functional mental models is likely to be particularly effective (Redmiles et al., 2016). Those older adults with good mental models of how attackers work are more likely to be motivated and better able to engage with protective behaviors. To take passwords as an example: those older adults who have some understanding of brute force attacks may appreciate the need for increased entropy in their own password compositions (e.g., Frik et al., 2019). For some less tangible protective behaviors, such as updating, the relevant mental models are likely to be more complex, possibly leading to lower salience and lower engagement. Previous security literature has determined that mental models, and the metaphors that represent these models, differ between experts and nonexperts (Camp et al., 2007), although it has been argued that any usable mental model is better for security than nothing at all (Wash & Rader, 2011).

3.4.4 | Language miscommunication and misinterpretation

Technical language is a known barrier in digital literacy and understanding (Cook et al., 2011; Nicholson et al., 2019a). Naturally, this was reflected in this study, and eloquently outlined by Participant 14.

> P14: it's the understanding process, I also think much of IT now is couched in terms…. Which people don't understand, it's jargon and it's designed to confuse, rather than inform.

When asked about updating for example, our participants would often take this to mean the act of taking out new subscriptions, upgrading to better packages or renewing existing payment-based packages, rather than the installation of free software downloads. This confusion was present in roughly half of the participants interviewed.

> P5: I update it every year, I pay for a new one every year

> P1: I update it every two years, I have an ongoing… it was every year but now it's every two years, it's not due to be renewed until next April.

Another participant knew the word "update," but having stopped to think for a second, demonstrated a lack of understanding of updating in an online setting.

> [Interviewer: So updating software, what does it mean to update software?] P4: Well it's self-explanatory! … I have no idea really?

It is easy to understand why jargon is problematic and although messages and awareness campaigns are increasingly targeted toward older adults, the messages sent by policy makers and the interpretation of those messages by older adults can sometimes be incongruent. The inability to express a problem using the correct terminology is also a source of shame in older adults, leading to decreased self-confidence and reluctance to talk to professionals about issues that may be pressing.

4 | GENERAL DISCUSSION

This study set out to explore older adults' thoughts and feelings toward protective cyber-security behaviors, facilitated by a newly developed card sorting elicitation task. This study was successful in identifying several findings which extend existing human factors cyber-security knowledge into older adult samples, as discussed throughout the findings section. Furthermore, this study has identified a number of important issues where existing literature is currently scarce, some of these relate to issues likely to be exacerbated in older adults, such as the stress of engaging with cyber-security. Others, provide clear direction for future research and subsequent policy development.

One key finding of this study was that cyber-security can be an emotive experience for older adults. Our participants frequently discussed feeling anxious, stressed, or fearful about trying to manage cyber-security. We see older adults using strategies such as writing down passwords to resolve their fear of forgetting passwords, some refusing to engage in security behaviors in-case they cause more harm than good, and others who recognize the need for cyber-security, yet defer responsibility to others because they are too nervous to take action themselves. In some cases, older adults will disengage entirely from cyber-security activity, showing signs of denial (e.g., refusing to believe they might be a target) or simply hoping that protection comes from an unspecified other source. Such responses reflect a larger psychological literature in which denial can emerge when people have no

realistic means of coping with stressors in the environment (Lazarus & Folkman, 1987; Lee et al., 2016).

A small and recent body of literature (for example: Lawson et al., 2016; Stacey et al., 2021; van Schaik et al., 2020) has begun to focus on the impact of emotion on cyber-security. There has recently been a call for better research tools that are able to disentangle the relationship between emotion and cyber-security (Renaud et al., 2021). Organizational security research appears to be leading the way in this regard, for example D'Arcy et al. (2014) have used existing psychological models to draw relationships between emotion and cyber-security behaviors. They drew upon existing technostress literature and coping theory (Lazarus & Folkman, 1987) to understand how employees responded to information security requirements and developed a security related stress scale. They noted that greater levels of security related stress were associated with noncompliant security behaviors, again an indication of processes of denial operating in this space. Although this is promising, for our understanding of the impact of emotion on cyber-security behavior, very little work has been conducted outside of workplace settings. This is problematic as security stress, fear, and anxiety are likely to exist outside of workplaces and are perhaps even amplified in older adults who have lower digital literacy and limited access to technological support (Nicholson et al., 2019a, 2021).

As noted above, a critical issue in understanding the impact of stress is the extent to which people believe they can cope. Here, too, our work is interesting in that we have provided a model that shows which factors impact user confidence in cyber-security engagement. Confidence is a critical construct here, and it becomes important to understand the way that a "virtuous circle" of learning could be established in the older adult community such that people would develop greater skills and confidence in their ability to cope with the ever-changing cyber-security landscape. In this regard, there are some interesting developments, such as the "cyberguardians" initiative of training older adults as ambassadors to propagate cyber-security knowledge in their community (Nicholson et al., 2021). We know that the ability to develop a repertoire of problem-focused coping strategies can be key in this area and increasingly researchers are focusing on ways to make cyber-security engagement less onerous (van Bavel et al., 2019).

4.1 | Implications for developers, researchers, and policy makers

4.1.1 | Researchers

In this study, we developed a novel card ranking task, designed to increase the breadth and depth of conversation around difficult concepts (Vaportzis et al., 2017). Building upon existing similar research designs used in this field (Nicholson et al., 2019b), we decided to produce a biaxial chart with prompt cards to facilitate conversation. This task proved useful in promoting conversation, with the prompt cards providing a starting point for discussion. Furthermore, the process of forced ranking (in assessing protective effectiveness) pushed participants to challenge their understanding of each of the concepts, before making judgment decisions based on their underlying mental models. Although we did not set out to specifically investigate mental models, the task developed here, and its precursors, may be particularly useful for accessing such mental model representations in future research (Nicholson et al., 2019b) as users are forced to think about how threats work to consider how effective protective behaviors might be.

Although we were most interested in the factors impacting security confidence, we also included the effectiveness dimension included in existing research (Nicholson et al., 2019b). As mentioned above, this served a number of purposes; first, it allowed us to provide a visualization of the sample's perceptions of security behavior effectiveness (see Figure 2). It is interesting to consider the factors that might impact this distribution, such as the nature of security-based campaigns or workplace training. For example, users are typically reminded about antivirus and passwords, but are less often prompted about ransomware and the protective nature of backing up. Given the sample size, and indeed the qualitative nature of this research, we are limited to the conclusions that we can draw from this part of the task, however future research applying this task is likely to benefit from incorporating effectiveness ratings for this reason.

The second part of the task: the ranking based on confidence, highlighted the need for further research into the impact of emotion and self-belief on cyber-security behaviors, something discussed above. We know that older adults can become anxious about engaging in online protective behaviors; however, we still know relatively little about how this anxiety manifests and influences behavior in the moment, something which lends itself to experimental research. The task used here does however show promise for future research seeking to elicit security knowledge. Participants gave positive feedback relating to their experience of engaging in the task and outlined how it forced them to question their understanding of security practices. They also suggested that doing so led to eye-opening realizations about how their behavior (or lack thereof), was likely to influence their vulnerability. Participants were able to use the prompts to see connections between protective behaviors, realizing how protective practices are important across the board, rather than through one or two specific actions. Herein lies a further strength of the task presented here in comparison to how existing ranking and card sorting tasks have been used.

Tasks such as the moon landing task (Hall & Watson, 1970) and desert survival task (Lafferty et al., 1974) rely heavily on quantitative methods, by measuring the concordance of rankings against those of experts. Nicholson et al. (2019b) also focused on the quantitative component of the task, but showed, in addition, that the group discussion around the card-sorting task acted as a useful knowledge elicitation tool, generating a rich discourse around security knowledge and attitudes. We have exploited card sorting as an elicitation tool here, adding to a sparse literature on the security experiences of older adults. However, the task could be used in qualitative, quantitative, or mixed methods research in the future. Our task provides a nonworkplace alternative to the cybersurvival task that can address similar research objectives. Additionally, by adding a second axis, our task could be used to assess security confidence in alternative

settings, for example in relation to the effectiveness of training. Indeed Nicholson et al. (2019b) suggest that such card sorting tasks may be useful for awareness training purposes, and since participants enjoyed the realizations that taking part provided, within training settings the task may be an effective way to help to demonstrate to trainees the discordance between what they see as effective, versus how they rate their own ability.

Older adults are a diverse population with a wide array of digital skills and abilities. Future research needs to acknowledge this variance in both the abilities of users and the kinds of support they require to facilitate safe Internet access. Future work may benefit from the mapping of interindividual variability using persona case studies (Dupree et al., 2016) in order to understand the various trajectories we might see in older adult samples. Persona cases, although a popular technique in user-centered design (Faily & Flechais, 2011), are less often seen in cyber-security literature. Such cases could be useful in understanding the various motives which drive users toward, or away, from security.

For some of our participants, the delegation of cyber-security responsibility was key. Future research could help us understand perceptions of security responsibility and the factors that give rise to a false sense of cyber-security in older adults. It would also be interesting to understand the impact of an individual's perceived personal responsibility in relation to cyber-security, and how this might influence susceptibility to social-engineering type attacks. Understanding this process further would allow us to determine whether we should promote stronger support mechanisms, or promote personal responsibility for security, something which is likely to be a contentious issue between security researchers.

4.1.2 | Developers

This study supported earlier findings that software updates are often avoided for the simple reason that they will lead to interface changes that require some "relearning" (Vaniea et al., 2014). This suggests a need to reimagine the update process; making clear when security updates are necessary and allowing the option to reject updates that significantly change the user interface in favor of simple security updates. Alternatively, developers could gradually introduce changes to allow for an adjustment period.

Aggressive marketing during the update process was also outlined as an issue (see Section 3.3.1). Although this may be an effective nudge toward better security, it may be better for developers to produce guidance that would allow purchasers the opportunity to gauge why each function is important. Doing so is likely to reduce confusion and avoidance, promote trust, and possibly increase the likelihood of users opting for higher levels of protection. Future research could also investigate what features different age groups prefer, based on their threat protection mental models, to determine if and how this influences protection package buying behaviors.

The simplicity of a device was reported as a factor which reduced the demands associated with updating devices, as well as other security processes such as two factor authentication. Developers and researchers should work together to promote simplicity in their designs, something which is likely to promote efficacy, feelings of control, and engagement in updating and other protective behaviors. It appears that currently Apple devices are the easiest for older adults in terms of engaging in security processes.

4.1.3 | Policy makers

The third set of implications generated from this study is addressed to policy makers charged with promoting online public safety and awareness. We found that conflicting advice, such as https encryption no longer being a reliable indicator of security (after years of this being key advice) (Herzberg, 2009), may cause ongoing distrust. The message that is delivered regarding such new advice should come with a note of caution that the Internet offers a rapidly changing environment and can often be out of date by the time it is published.

Second, advice should be readily accessible to older adults, some of which are the most in need, and the most desiring, of such advice. Too often sites which offer advice incorporate cyber-security jargon. This is likely to undermine older adults, or those with low digital literacy, reinforcing feelings of low self-efficacy and contributing to digital exclusion (Briggs & Thomas, 2015). Either advice needs to be simplified or separate advice should be prepared for those unable to understand such terminology. Something as simple as hover-over definitions would give older adults a much greater chance of breaking through jargon. Policy makers should attempt to work with both older adult researchers and older adults themselves to provide appropriate, digestible, tailored advice.

This study also supports earlier findings that mental models may be important to understanding older adult's engagement with cyber-security (Frik et al., 2019; Ray et al., 2019). Campaigns should seek to improve and develop basic mental models, designed at promoting mechanistic understanding, something which may also inspire confidence through increasing tangibility of threats and behaviors. Furthermore, such campaigns should seek to promote feelings of control, something which is likely to promote acceptance of such behaviors (Bada et al., 2019). Finally, the findings of this study suggest that campaigns which promote positive support styles ("show them, don't do it for them") may be useful in changing how support is delivered. It is easy to imagine an advert where a grandparent takes a child's homework from them and fills in the answer, metaphorically demonstrating what negative support is effectively doing to older adults, that is promoting a sense of dependence on others and disempowering those involved.

4.2 | Conclusion

We set out to investigate what factors influence older adults' engagement with and confidence in cyber-security protection. Older adults are keen to continue to use technology and most are keen to protect

themselves online and generally understand the repercussions of not doing so. Where possible, older adults will engage in protective behaviors, but too often this is seen as an unforgiving process which generates anxiety and ultimately avoidance and denial. Poor sources of support in terms of available information and accessible expertise may contribute to declining digital literacy in older adults, and act to lower the salience of cyber protection, something which researchers and policy makers should attempt to counteract. Older adults have a desire to protect themselves and researchers, developers, and policy makers should work together to empower them to do so.

ACKNOWLEDGMENTS

This work was supported by the Engineering and Physical Sciences Research Council (grant no. EP/P011454/1).

CONFLICT OF INTERESTS

The authors declare that there are no conflict of interests.

PEER REVIEW

The peer review history for this article is available at https://publons.com/publon/10.1002/hbe2.291.

DATA AVAILABILITY STATEMENT

Full interview transcripts are not publicly available due to privacy concerns.

ETHICS STATEMENT

Ethical approval for this study was granted by the Faculty of Health and Life Sciences ethical review process at the University of Northumbria at Newcastle. Written informed consent was obtained by all participants within this study.

REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/10.1145/322796.322806

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology and Health*, *26*(9), 1113–1127. https://doi.org/10.1080/08870446.2011.613995

Bada, M., Sasse, A., & Nurse, J. (2019). Cyber security awareness campaigns why they fail to change behavior. Global Cyber Security Capacity Centre.

Berkowsky, R. W., Sharit, J., & Czaja, S. J. (2017). Factors predicting decisions about technology adoption among older adults. *Innovation in Aging*, *1*(3), 1–12. https://doi.org/10.1093/geroni/igy002

Betts, L. R., Hill, R., & Gardner, S. E. (2019). "There's not enough knowledge out there": Examining older Adults' perceptions of digital technology use and digital inclusion classes. *Journal of Applied Gerontology*, *38*(8), 1147–1166. https://doi.org/10.1177/0733464817737621

Boothroyd, V., & Chiasson, S. (2013). Writing down your password: Does it help? 2013 11th Annual Conference on Privacy, Security and Trust, 267–274. https://doi.org/10.1109/PST.2013.6596062

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Briggs, P., & Thomas, L. (2015). An inclusive, value sensitive design perspective on future identity technologies. *ACM Transactions on Computer-Human Interaction*, *22*(5), 1–28. https://doi.org/10.1145/2778972

Camp, L. J., Asgharpour, F., & Liu, D. (2007). Experimental evaluations of expert and non-expert computer Users' mental models of security risks, *Proceedings of WEIS 2007*, 1–24. http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Experimental+Evaluations+of+Expert+and+Non-expert+Computer+Users'+Mental+Models+of+Security+Risks#0

Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in Human Behavior*, *23*(3), 1273–1284. https://doi.org/10.1016/j.chb.2004.12.005

Chiu, C. J., & Liu, C. W. (2017). Understanding older adult's technology adoption and withdrawal for elderly care and education: Mixed method analysis from National Survey. *Journal of Medical Internet Research*, *19*(11), e374. https://doi.org/10.2196/jmir.7401

Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987–995. https://doi.org/10.1016/j.chb.2010.02.012

Chung, J., & Monroe, G. S. (2000). The effects of experience and task difficulty on accuracy and confidence assessments of auditors. *Accounting and Finance*, *40*(2), 135–151. https://doi.org/10.1111/1467-629X.00040

Cook, D. M., Szewczyk, P., & Sansurooah, K. (2011). Seniors language paradigms: 21 st century jargon and the impact on computer security and financial transactions for senior citizens. *Proceedings of the 9th Australian Information Security Management Conference*, 63–68.

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices improve the public's use of cyber. Government Office for Science, 19. https://doi.org/10.13140/RG.2.1.2387.3761

Czaja, S. J., Charness, N., Fisk, A. D., Hertzog, C., Nair, S. N., Rogers, W. A., & Sharit, J. (2006). Factors predicting the use of technology: Findings from the Center for Research and Education on aging and technology enhancement (CREATE). *Psychology and Aging*, *21*(2), 333–352. https://doi.org/10.1037/0882-7974.21.2.333

Damodaran, L., & Sandhu, J. (2016). The role of a social context for ICT learning and support in reducing digital inequalities for older ICT users. *International Journal of Learning Technology*, *11*(2), 1–20. https://doi.org/10.1504/IJLT.2016.077520

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/MIS0742-1222310210

Duggan, G. B., Johnson, H., & Grawemeyer, B. (2012). Rational security: Modelling everyday password use. *International Journal of Human Computer Studies*, *70*(6), 415–431. https://doi.org/10.1016/j.ijhcs.2012.02.008

Dupree, J. L., Devries, R., Berry, D. M., & Lank, E. (2016). Privacy personas: Clustering users via attitudes and behaviors toward security practices. *Conference on Human Factors in Computing Systems*, 5228–5239. https://doi.org/10.1145/2858036.2858214

Durrant, A., Kirk, D., Trujillo Pisanty, D., Moncur, W., Orzech, K., Schofield, T., Elsden, C., Chatting, D., & Monk, A. (2017). Transitions in digital personhood. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 6398–6411. https://doi.org/10.1145/3025453.3025913

Fagan, M., Albayram, Y., Khan, M. M. H., & Buck, R. (2017). An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences*, *7*(1), 12. https://doi.org/10.1186/s13673-017-0093-6

Fagan, M., & Khan, M. M. H. (2019). Why do they do what they do? A study of what motivates users to (not) follow computer security advice. *12th Symposium on Usable Privacy and Security*, 59–75.

Faily, S., & Flechais, I. (2011). Persona cases: A technique for grounding personas. *Conference on Human Factors in Computing Systems*, 2267–2270. https://doi.org/10.1145/1978942.1979274

Fletcher-Watson, B., Crompton, C., Hutchison, M., & Hongjin, L. (2016). Strategies for enhancing success in digital tablet use by older adults: A pilot study. *Geron*, *3*(3), 162–170.

Friemel, T. N. (2016). The digital divide has grown old: Determinants of a digital divide among seniors. *New Media & Society*, *18*(2), 313–331. https://doi.org/10.1177/1461444814538648

Frik, A., Nurgalieva, L., Bernd, J., Lee, J. S., Schaub, F., & Egelman, S. (2019). Privacy and security threat models and mitigation strategies of older adults. *Proceedings of the 15th Symposium on Usable Privacy and Security*, 21–40.

Fujs, D., Mihelič, A., & Vrhovec, S. L. R. (2019). The power of interpretation: Qualitative methods in cybersecurity research. ACM International Conference Proceeding Series. https://doi.org/10.1145/3339252.3341479

Grilli, M. D., McVeigh, K. S., Hakim, Z. M., Wank, A. A., Getz, S. J., Levin, B. E., Ebner, N. C., & Wilson, R. C. (2020). Is this phishing? Older age is associated with greater difficulty discriminating between safe and malicious emails. *The Journals of Gerontology: Series B*, https://doi.org/10.1093/geronb/gbaa228

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of internet hazards. *Educational Gerontology*, *36*(3), 173–192. https://doi.org/10.1080/03601270903183065

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough?: An experiment with data saturation and variability. *Field Methods*, *18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Hall, J., & Watson, W. H. (1970). The effects of a normative intervention on group decision-making performance. *Human Relations*, *23*(4), 299–317. https://doi.org/10.1177/001872677002300404

Herzberg, A. (2009). Why Johnny can't surf (safely)? Attacks and defenses for web users. *Computers and Security*, *28*(1–2), 63–71. https://doi.org/10.1016/j.cose.2008.09.007

Hicks, C. M., Gonzales, R., Morton, M. T., Gibbons, R. V., Wigton, R. S., & Anderson, R. J. (2000). Procedural experience and comfort level in internal medicine trainees. *Journal of General Internal Medicine*, *15*(10), 716–722. https://doi.org/10.1046/j.1525-1497.2000.91104.x

Holmes, M., & Ophoff, J. (2019). Online security behaviour: factors influencing intention to adopt two- factor authentication. *Proceedings of the 14th International conference on cyber warfare and security, ICCWS 2019*, 123–132.

Hunsaker, A., & Hargittai, E. (2018). A review of internet use among older adults. *New Media and Society*, *20*(10), 3937–3954. https://doi.org/10.1177/1461444818787348

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and Management*, *51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

Ion, I., Reeder, R., & Consolvo, S. (2015). "...No one can hack my mind": Comparing expert and non-expert security practices. *Proceedings of the 11th Symposium on Usable Privacy and Security*, 327–346.

Jiang, M., Tsai, H.-y. S., Cotten, S. R., Rifon, N. J., LaRose, R., & Alhabash, S. (2016). Generational differences in online safety perceptions, knowledge, and practices. *Educational Gerontology*, *42*(9), 621–634. https://doi.org/10.1080/03601277.2016.1205408

Juárez, M. A. R., González, V. M., & Favela, J. (2018). Effect of technology on aging perception. *Health Informatics Journal*, *24*(2), 171–181. https://doi.org/10.1177/1460458216661863

Lafferty, J. C., Eady, P. M., & Elmers, J. (1974). The desert survival problem. In *Experimental learning methods*. Human Synergistics.

Lawson, S. T., Yeo, S. K., Yu, H., & Greene, E. (2016). The cyber-doom effect: The impact of fear appeals in the US cyber security debate. International Conference on Cyber Conflict, 65–80. https://doi.org/10.1109/CYCON.2016.7529427

Lazarus, R. S., & Folkman, S. (1987). Transactional theory and research on emotions and coping. *European Journal of Personality*, *1*(3), 141–169. https://doi.org/10.1002/per.2410010304

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Lee, A. R., Son, S. M., & Kim, K. K. (2016). Information and communication technology overload and social networking service fatigue: A stress perspective. *Computers in Human Behavior*, *55*, 51–61. https://doi.org/10.1016/j.chb.2015.08.011

Levitt, H. M., Bamberg, M., Creswell, J. W., Frost, D. M., Josselson, R., & Suárez-Orozco, C. (2018). Journal article reporting standards for qualitative primary, qualitative meta-analytic, and mixed methods research in psychology: The APA publications and communications board task force report. *American Psychologist*, *73*(1), 26–46. https://doi.org/10.1037/amp0000151

Li, Z., He, W., Akhawe, D., & Song, D. (2014). The Emperor's new password manager: Security analysis of web-based password managers. *23rd USENIX Security Symposium (USENIX Security 14)*, 465–479.

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to spear-phishing emails. *ACM Transactions on Computer-Human Interaction*, *26*(5), 1–28. https://doi.org/10.1145/3336141

Marquié, J. C., Jourdan-Boddaert, L., & Huet, N. (2002). Do older adults underestimate their actual computer knowledge? *Behaviour and Information Technology*, *21*(4), 273–280. https://doi.org/10.1080/0144929021000020998

Martínez-Alcalá, C. I., Rosales-Lagarde, A., de los ángeles Alonso-Lavernia, M., Ramírez-Salvador, J. A. Á., Jiménez-Rodríguez, B., Cepeda-Rebollar, R. M., López-Noguerola, J. S., Bautista-Díaz, M. L., & Agis-Juárez, R. A. (2018). Digital inclusion in older adults: A comparison between face-to-face and blended digital literacy workshops. *Frontiers in ICT*, *5*, 1–17. https://doi.org/10.3389/fict.2018.00021

McDermott, R. (2012). Privacy and security emotion and security. *Communications of the ACM*, *55*(2), 35–37. https://doi.org/10.1145/2076450.2076462

Merdenyan, B., & Petrie, H. (2018). Generational differences in password management behaviour. *Proceedings of the 32nd International BCS Human Computer Interaction Conference*, 1–10. https://doi.org/10.14236/ewic/HCI2018.60

Mitzner, T. L., Boron, J. B., Fausset, C. B., Adams, A. E., Charness, N., Czaja, S. J., Dijkstra, K., Fisk, A. D., Rogers, W. A., & Sharit, J. (2010). Older adults talk technology: Technology usage and attitudes. *Computers in Human Behavior*, *26*(6), 1710–1721. https://doi.org/10.1016/j.chb.2010.06.020

Mitzner, T. L., Savla, J., Boot, W. R., Sharit, J., Charness, N., Czaja, S. J., & Rogers, W. A. (2019). Technology adoption by older adults: Findings from the PRISM trial. *Gerontologist*, *59*(1), 34–44. https://doi.org/10.1093/geront/gny113

Morrison, B. A., Coventry, L., & Briggs, P. (2020). Technological change in the retirement transition and the implications for cybersecurity vulnerability in older adults. *Frontiers in Psychology*, *11*, 1–13. https://doi.org/10.3389/fpsyg.2020.00623

Munanga, A. (2019). Cybercrime: *A new and growing problem for older adults*. *Journal of Gerontological Nursing*, *45*, 3–5.

Nägle, S., & Schmidt, L. (2012). Computer acceptance of older adults. *Work*, *41*(Suppl 1), 3541–3548. https://doi.org/10.3233/WOR-2012-0633-3541

Nicholson, J., Coventry, L., & Briggs, P. (2013). Age-related performance issues for PIN and face-based authentication systems. *Conference on Human Factors in Computing Systems - Proceedings*, 323–332. https://doi.org/10.1145/2470654.2470701

Nicholson, J., Coventry, L., & Briggs, P. (2019a). If It's important it will be a headline: Cybersecurity information seeking in older adults. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3290605.3300579

Nicholson, J., Coventry, L., & Briggs, P. (2019b). Introducing the cybersurvival task: Assessing and addressing staff beliefs about

effective cyber protection. *Proceedings of the 14th Symposium on Usable Privacy and Security*, 443–457.

Nicholson, J., Morrison, B., Dixon, M., Holt, J., Coventry, L., & McGlasson, J. (2021). Training and embedding cybersecurity guardians in older communities. *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–15. https://doi.org/10.1145/3411764.3445078

Nthala, N., & Flechais, I. (2018). Informal support networks: An investigation into Home Data Security Practices. This paper is included in the Proceedings of the Informal Support Networks.

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Guidelines for usable cybersecurity: Past and present. *Proceedings—3rd International Workshop on Cyberspace Safety and Security*, 21–26. https://doi.org/10.1109/CSS.2011.6058566

Olivier, S., Burls, T., Fenge, L. A., & Brown, K. (2015). "Winning and losing": Vulnerability to mass marketing fraud. *Journal of Adult Protection*, *17*(6), 360–370. https://doi.org/10.1108/JAP-02-2015-0002

Pauwels, L., & Mannay, D. (2019). *The SAGE handbook of visual research methods*. SAGE.

Portz, J. D. (2017). A review of web-based chronic disease self-management for older adults. *Geron*, *16*(1), 12–20. https://doi.org/10.4017/gt.2017.16.1.002.00

Ray, H., Wolf, F., Kuber, R., & Aviv, A. J. (2019). "Woe is me:" examining older adults' perceptions of privacy. *Conference on Human Factors in Computing Systems - Proceedings*, 1–6. https://doi.org/10.1145/3290607.3312770

Ray, H., Wolf, F., Kuber, R., & Aviv, A. J. (2021). Why older adults (Don't) use password managers. *ArXiv*.

Redmiles, E. M., Malone, A. R., & Mazurek, M. L. (2016). I think They're trying to tell me something: Advice sources and selection for digital security. *Proceedings—2016 IEEE Symposium on Security and Privacy*, 272–288. https://doi.org/10.1109/SP.2016.24

Renaud, K., Zimmermann, V., Schürmann, T., & Böhm, C. (2021). Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications*, *8*(1), 75. https://doi.org/10.1057/s41599-021-00746-5

Sandhu, J., Damodaran, L., & Ramondt, L. (2013). ICT skills acquisition by older people: Motivations for learning and barriers to progression. *International Journal of Education and Ageing*, *3*(2), 95–114.

Schreurs, K., Quan-Haase, A., & Martin, K. (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), 359–377. https://doi.org/10.22230/cjc.2017v42n2a3130

Seifert, A., & Schelling, H. R. (2018). Seniors online: Attitudes toward the internet and coping with everyday life. *Journal of Applied Gerontology*, *37*(1), 99–109. https://doi.org/10.1177/0733464816669805

Shao, J., Zhang, Q., Ren, Y., Li, X., & Lin, T. (2019). Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud. *Journal of Elder Abuse and Neglect*, *31*(3), 225–243. https://doi.org/10.1080/08946566.2019.1625842

Stacey, P., Taylor, R., Olowosule, O., & Spanaki, K. (2021). Emotional reactions and coping responses of employees to a cyber-attack: A case study. *International Journal of Information Management*, *58*, 102298. https://doi.org/10.1016/j.ijinfomgt.2020.102298

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *IT Professional*, *18*(5), 26–32. https://doi.org/10.1109/MITP.2016.84

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human Computer Studies*, *123*, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Van Boekel, L. C., Peek, S. T., & Luijkx, K. G. (2017). Diversity in older adults' use of the internet: Identifying subgroups through latent class analysis. *Journal of Medical Internet Research*, *19*(5), e180. https://doi.org/10.2196/jmir.6853

van Schaik, P., Renaud, K., Wilson, C., Jansen, J., & Onibokun, J. (2020). Risk as affect: The affect heuristic in cybersecurity. *Computers and Security*, *90*, 101651. https://doi.org/10.1016/j.cose.2019.101651

Vaniea, K. E., Rader, E., & Wash, R. (2014). *Betrayed by updates: How negative experiences affect future security*. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2671–2674. https://doi.org/10.1145/2556288.2557275

Vaportzis, E., Clausen, M. G., & Gow, A. J. (2017). Older adults perceptions of technology and barriers to interacting with tablet computers: A focus group study. *Frontiers in Psychology*, *8*, 1–11. https://doi.org/10.3389/fpsyg.2017.01687

Venkatesh, V., & Bala, H. (2008). TAM3 technology acceptance model 3 and a research agenda on interventions. *Decision Sciences*, *39*(2), 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425. https://doi.org/10.2307/30036540

Vroman, K. G., Arthanat, S., & Lysack, C. (2015). "Who over 65 is online?" older adults' dispositions toward information communication technology. *Computers in Human Behavior*, *43*, 156–166. https://doi.org/10.1016/j.chb.2014.10.018

Vu, K. P. L., & Hills, M. M. (2013). The influence of password restrictions and mnemonics on the memory for passwords of older adults. In *Human interface and the management of information. Information and interaction design* (Vol. 8016, pp. 660–668). Springer. https://doi.org/10.1007/978-3-642-39209-2-74

Wash, R. (2010). Folk models of home computer security. ACM International Conference Proceeding Series. https://doi.org/10.1145/1837110.1837125

Wash, R., & Rader, E. (2011). Influencing mental models of security: A research agenda. *Proceedings New Security Paradigms Workshop*, 57–66. https://doi.org/10.1145/2073276.2073283

Whitty, M. T. (2017). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 105–109. https://doi.org/10.1089/cyber.2016.0729

Whitty, M. T., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior and Social Networking*, *18*(1), 3–7. https://doi.org/10.1089/cyber.2014.0179

Woods, N., & Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human Computer Studies*, *111*, 36–48. https://doi.org/10.1016/j.ijhcs.2017.11.002

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Xie, B. (2007). Information technology education for older adults as a continuing peer-learning process: A Chinese case study. *Educational Gerontology*, *33*(5), 429–450. https://doi.org/10.1080/03601270701252872

Yagil, D., Cohen, M., & Beer, J. D. (2016). Older Adults' coping with the stress involved in the use of everyday technologies. *Journal of Applied Gerontology*, *35*(2), 131–149. https://doi.org/10.1177/0733464813515089

AUTHOR BIOGRAPHIES

Benjamin Morrison is an Innovation Fellow within the Centre of Digital Citizens at Northumbria University. He is based within the

Psychology and Communication Technology (PaCT Lab), within the psychology department. His work focuses on human-factors cyber-security vulnerability in the older adult population, as well as digital exclusion and the digital inequalities experienced by older adults.

Lynne Coventry is a Professor in the Psychology department. She leads the Human and Digital Design multidisciplinary research theme across Northumbria University. She has an interdisciplinary human–computer interaction background. Her research focuses on inclusive interaction with technology ensuring the diversity of needs and abilities are accommodated through the design.

Pam Briggs holds a Research Chair in Applied Psychology at Northumbria University and is a Visiting Professor at Newcastle University. She is a Co-Director of the UK *Centre for Digital Citizens* and is one of the founder members of the UK's Research Institute in Sociotechnical Cybersecurity. Her research addresses issues of trust, privacy, identity, and security in the digital world, and her most recent publications highlight issues of inclusivity and diversity in digital engagement. She has contributed to three UK Government Office for Science reports (*The Future of Identity*; *Using Behavioral Insights to Improve the Public's Use of Cyber Security Best Practice* and *Responsible Use of Data*) and to the European Commission's (2017) report *Cybersecurity in the European Digital Single Market*.

How to cite this article: Morrison, B., Coventry, L., & Briggs, P. (2021). How do Older Adults feel about engaging with Cyber-Security? *Human Behavior and Emerging Technologies*, *3*(5), 1033–1049. https://doi.org/10.1002/hbe2.291

APPENDIX A.—EXAMPLES OF CARD SORTING OUTCOMES

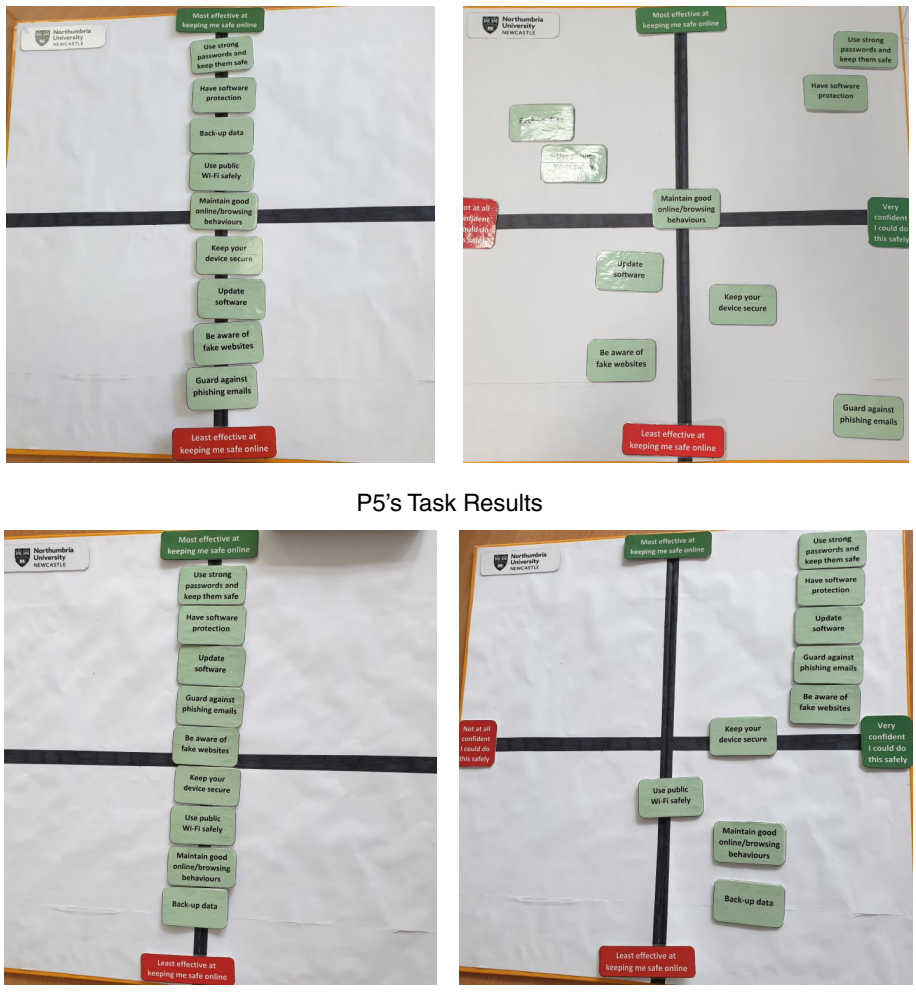

FIGURE A1 P5's task results