Exploring Age and Gender Differences in ICT Cybersecurity Behaviour

Dawn Branley-Bell*[1], Lynne Coventry[1], Matt Dixon[1], Adam Joinson[2], and Pam Briggs[1]

[1]Department of Psychology, Northumbria University, Newcastle upon Tyne, NE1 8ST
[2]School of Management, University of Bath, BA2 7AY

[*]Corresponding author: Dawn Branley-Bell, Department of Psychology, Northumbria University, Newcastle upon Tyne, NE1 8ST, UK. dawn.branley-bell@northumbria.ac.uk

Exploring Age and Gender Differences in ICT Cybersecurity Behaviour

Known age differences exist in relation to Information and Communication Technology (ICT) use, attitudes, access and literacy. Less is known about age differences in relation to cybersecurity risks and associated cybersecurity behaviours. Using an online survey, this study analyses data from 576 participants to investigate age differences across four key cybersecurity behaviours: Device securement, password generation, proactive checking, and software updating. Significant age differences were found; however, this is not a straightforward relationship. Older users appear less likely to secure their devices compared to younger users, however the reverse was found for the other behaviours, with older users appearing more likely to generate secure passwords, show proactive risk awareness and regularly install updates. Gender was not a significant predictor of security behaviour (although males scored higher for self-reported computer self-efficacy and general resilience). Self-efficacy was identified as a mediator between age and three of the cybersecurity behaviours (password generation, proactive checking and updating). General resilience was also a significant mediator for device securement, password generation and updating, however resilience acted as a moderator for pro-active checking. These findings have implications for the design of targeted training and development of interventions for different cybersecurity behaviours.

1. Introduction

More people are using digital technology than ever before, however ‘digital divides’ remain prevalent across user groups [1–3]. Demographic factors such as age and gender have often been cited as moderators of these digital divides. Younger age ranges have traditionally been the earliest adopters of ICT, however these age groups are reaching saturation (99% of young adults now use the internet in the UK [4]). Consequently, older adults are now the fastest growing group of adopters [4–6]. Despite many older adults being keen to adopt technology [7], a negative narrative prevails [8]. For example research suggests that this user-group may still lack confidence in their ability (or self-efficacy) to use their devices [9–11] and may show deficits in ICT skills and literacy [2,12,13], something often referred to as the ‘second level’ of the digital divide (where *access* to ICT forms the first level [1]). However, some researchers have argued that, rather than there being an age-related skills gap, older adults may simply underestimate their actual capabilities and knowledge [14]. In their review of this issue, Hunsaker and Hargittai [2] note a methodological issue with researching older adults, pointing out that studies differ in how they group age categories, the categories included and the age that is used to signal the start of older adulthood. They called for further work to identify whether age disparities are continuing.

For all users, the cost of embracing digital connectivity is a growing cybersecurity risk. As older adults now spend longer online, they in turn have become the latest target population for cyber-attacks, with £4m lost by older adults in the UK between 2018-19 [15]. However, research into age related differences in cybersecurity posture and attitude is scarce [11,16], which means it is difficult to identify and mitigate age-specific issues.

The risks that individual users are susceptible to may vary with age, but this is by no means conclusive. For example, while [17] suggests that younger users are more vulnerable to phishing attacks, Grilli et al. [18] found that older adults were worse at discriminating between genuine and phishing emails based on perceived suspiciousness. Sarno et al. [19] found no age differences in the ability to classify emails as phishing or not. Oliveri et al. [20] discovered that older and younger adults fall for different persuasion triggers, with older women being the most vulnerable group. Other research suggests that younger adults display fewer privacy and security concerns compared to older users (the latter potentially due to high levels of social media use and the associated sharing of personal data [21,22]). Note, however, that this may not be a simple linear relationship, given a study by Little and colleagues, who found a more complex U-shaped trend with younger and older internet users appearing less protective of their privacy than their middle-aged counterparts [23]. Older adults show a reluctance to fully engage with cybersecurity behaviours, citing reasons including low self-efficacy and a lack of awareness [11]. They are also less likely to adopt security measures to protect against unauthorised access to their devices, e.g., PIN or biometric protections [24]. Taken as a whole, the current research suggests that cybersecurity concerns may be more complicated than simply identifying a single age range as vulnerable or 'at risk'. It is important that we understand how adults of different ages engage with different security behaviours to protect themselves online. This study addresses this gap in the literature and concentrates on four key cybersecurity related behaviours: Device securement (e.g., locking their device screen when not in use), secure password generation, proactive checking (checking legitimacy and security indicators such as URLs and senders before clicking), and regular software updating.

Using data from across the adult lifespan (18-82yrs), the current study addresses some of the limitations of previous research, where quite limited age ranges have been investigated (often due to practical difficulties in data collection [25]). For example, Ayyagari and Crowell [26] recently investigated differences between three age groups in relation to cybersecurity behaviours however they were restricted to a university sample and their eldest group constituted anyone over 35 years. In addition to assessing reported behaviours, we also expand the current literature by exploring the role of computer self-efficacy, as this has been shown to influence ICT behaviour [27,28]. Psychological resilience has also been linked to risky behaviour. Specifically, resilience has been linked to both risk seeking and risk adverse behaviours, depending upon the study and/or context [29,30]. We therefore include a general resilience measure as a variable within our study.

This study also investigates gender differences as existing research in this area is inconclusive. Traditionally research has suggested that females score lower for computer self-efficacy than males [20,21] although more recently [22] suggest that this gender difference may be diminishing. It is important to note that self-efficacy relates to the individuals own beliefs about how they can perform [23]. As such, it is not possible to determine whether any gender differences reflect differences in actual ability and/or differences in self-perception [24]. Computer self-efficacy can also be context dependent, with several studies showing that gender differences may differ depending on the context (e.g., ICT for educational versus general use; [25] or the specific task (e.g., internet tasks versus high level software-related tasks, [31]). Interestingly, some studies looking specifically at cybersecurity behaviours report that females tend to show greater online privacy concerns [27] and greater security policy compliance [28]. Whilst other studies show no gender differences, for example Vance and colleagues [32] found no gender differences for intention to comply with security policies, and others suggest that females are likely to act less securely [33]. In their review of older adult research, Hunsaker and Hargittai also described the existing literature as inconclusive. We address this need for increased understanding by including gender analyses in the current study.

In summary, our study tests for age and gender differences in cybersecurity behaviour across the adult lifespan, after controlling for computer self-efficacy and general resilience. The results have implications for identifying priority areas for future targeted training and development interventions.

2. Materials and Methods

Full ethical approval was granted from the School of Health and Life Sciences ethics committee at Northumbria University. An online survey was distributed by online recruitment platform 'Prolific.ac'. Prolific is a paid service that distributes online questionnaires to their userbase of participants. The initial sample of 607 responses was cleaned and 31 responses removed due to failing the 'attention check' question. The final sample consists of data from 579 participants, aged 18-82 years (*M* = 33.86yrs, *SD* = 11.80yrs). Further demographics are shown in Table 1.

Table 1. Sample demographics (N = 579)

		N	***%***
Age	18-24	131	22.6
	25-34	219	37.8
	35-44	143	24.7
	45-54	46	7.9
	55-64	26	4.5
	65-74	12	2.1
	75-82	2	0.3
Gender	Male	236	40.8
	Female	340	58.7
	Other	3	0.5
Education	Primary/Elementary School	4	.07
	Secondary/High School	67	11.6
	College/A-Level	146	25.2
	Bachelors	239	41.3
	Masters	98	16.9
	Doctorate	25	4.3
Country	UK	275	47.5
	USA	152	26.2
	Canada	152	26.3

In addition to the demographic questions, participants were asked to complete a series of scale items to measure their cybersecurity behaviour, their computer self-efficacy and their general resilience. Cybersecurity related behaviour was measured using the Security Behaviour Intentions Scale (SeBIS) [34]. SeBIS is a 16-item scale consisting of four subscales that measure attitudes towards device securement, password generation, proactive checking and software updating. The scale showed acceptable reliability in our study with Cronbach's alpha (α) ranging from .64-.75 for the four subscales (see Table 3). The Computer Self-Efficacy scale [35] was used to measure users' beliefs about their ICT capabilities. The scale showed excellent reliability (α = .93). General resilience was measured using the Brief Resilience Scale [36] (α = .89).

3. Results

Missing data accounted for less than 0.3% of the items. Little's MCAR test was non-significant (X^2 (117) = 118.88, p = .43) indicating that the data was missing completely at random, therefore Estimated Maximum Likelihood was used to compute the missing data. Due to insufficient sample size (n=3) the other gender category was excluded from the analyses.

Data was checked to ensure it met the assumptions of normality, independence and homoscedasticity. All values were checked to ensure that they were within the excepted ranges given the measurement scales used. There was no sign of multicollinearity between the predictor variables (all correlations <.7, see Table 2; VIF scores <2), scatterplots indicated a linear relationship between the IVs and DVs and plotting the standardised residuals and predicted values indicated adequate homoscedasticity. All dependent variables appeared normally distributed on the Q-Q plots (and skew and kurtosis values <2), except for device securement. The latter indicated negative skew (more scores towards the top of the scale) although this was still within the acceptable threshold of +/-2 [37]. Device securement also showed a kurtosis value of 2.28. Therefore, as the normality assumption was violated for device securement, all analyses using this variable were conducted using the bootstrapping method (with bias-corrected and accelerated confidence intervals, samples = 2000) to ensure robustness.

Bivariate correlations are shown for each of the variables (Table 2). There is no significant correlation between age and gender. None of the correlations raise concerns around multicollinearity.

Table 2. Bivariate correlations for each of the variables

	M	SD	1.	2.	3.	4.	5.	6.	7.	8.
1. Age	33.85	11.82	-							
2. Gender	-	-	.03	-						
3. S.Efficacy	3.64	.82	-.11**	.39***	-					
4. Resilience	3.24	.85	.11**	-.12**	.23***	-				
5. Device Securement	4.06	.83	-.18***	-.01	.10*	.11**	-			
6. Password Generation	3.29	.82	.15***	-.17***	.27***	.21***	.20***	-		
7. Proactive Checking	3.71	.69	.12**	-.16***	.31***	.17***	.19***	.46***	-	
8. Updating	3.42	.87	.14***	-.17***	.33***	.20***	.18***	.32***	.29***	-

Note: ***p<.001 **p<.01 *p<.05

3.1. Age and Gender differences in perceived Computer Self-Efficacy and General Resilience

Independent samples t-tests showed a significant difference between the genders, with males (M = 4.02, SD = .74) scoring significantly higher than females for perceived computer self-efficacy (M = 3.38, SD = .78), t(574) = 9.99, p <.001. T-tests also show a significant difference between the genders for general resilience, with males (M = 3.21, SD = .81) scoring significantly higher than females (M = 3.16, SD = .88), t(574) = 2.87, p = .004. There were no significant age differences for self-efficacy or resilience scores.

3.2. Predictors of Cybersecurity Behaviours

The data were analysed using a series of hierarchical regressions to test the predictors (age, gender, computer self-efficacy and general resilience) of cybersecurity behaviour. As aforementioned, the device securement regression was conducted using the bootstrapping method due to violating the assumptions of homoscedasticity, therefore confidence intervals are reported for this regression. All four models were significant (Table 3): Device securement (Bootstrap Samples = 2000, R^2 = .05, BCa CI [.03 - .08]), Password generation ($F(4,571)$ = 12.06, p<.001, R^2 = .13), Proactive checking ($F(4,571)$ = 20.19, p<.001, R^2 = .12), and Updating ($F(4,571)$ = 25.13, p<.001, R^2 = .15).

Investigating the individual predictors revealed that age was a significant predictor for all four cybersecurity behaviours (Table 3). Age was a negative predictor of device securement, but a positive predictor for the other behaviours (password generation, proactive checking and updating). Gender was not a significant predictor for any of the behaviours.

The standardised coefficients show the strongest predictors. For three of the four behaviours (password generation, proactive checking and updating), computer self-efficacy was the strongest predictor, followed by age and then general resilience. All of which were positive predictors.

Device securement differed from the other behaviours. The strongest predictor variable, age, acted as a negative predictor of this behaviour. General resilience was the only other significant predictor, acting as a positive predictor of secure behaviour.

Table 3. Regression results

	Device Securement[±] (α=.64)					Password Generation (α=.71)					Proactive Checking (α=.66)					Updating (α=.75)				
	B	Beta	SE	BCa CI	R^2 [CI]	B	Beta	SE	*t*	R^2	B	Beta	SE	*t*	R^2	B	Beta	SE	*t*	R^2
Age	-.01	-.18	.00	-.02, -.01***		.01	.16	.00	4.09***		.01	.14	.00	3.51***		.01	.16	.00	4.16***	
Gender	.07	.04	.08	-.09, .22		-.11	-.07	.07	-1.61		-.06	-.04	.06	-.92		-.08	-.05	.07	-1.12	
S.Efficacy	.07	.07	.05	-.02, .16		.23	.23	.04	5.38***		.24	.29	.04	6.58***		.32	.30	.05	7.01***	
Resilience	.12	.12	.05	.03, .21*	.05 [.03, .08]	.13	.13	.04	3.31**	.13*	.07	.08	.03	2.02*	.124**	.11	.11	.04	2.61**	.15*

Note: [±]2000 bootstrap samples. ****p*<.001 ***p*<.01 **p*<.05

3.3. Mediation Analysis

The relationship between age and perceived computer self-efficacy and resilience was investigated further with parallel mediation analysis using the PROCESS macro for SPSS, model 4 (Hayes, 2013, Figure 1).

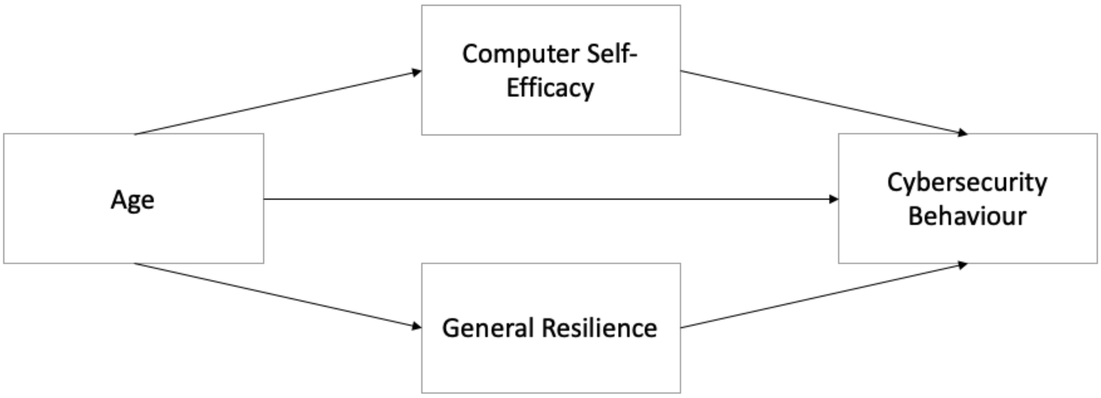

Figure 1. Parallel mediation model (PROCESS model 4)

To aid interpretation of the results, all variables that defined products were mean centered during the PROCESS mediation analysis. The results are shown in Table 4.

The indirect effect of age on cybersecurity behaviour, via self-efficacy (mediator 1), was significant for three of the four behaviours: Password generation, proactive checking and updating. Self-efficacy was not a significant mediator for device securement.

The indirect effect of age on cybersecurity behaviour, via resilience (mediator 2), was significant for three of the four behaviours: Device securement, password generation and updating. The effect of resilience on the remaining cybersecurity behaviour, proactive checking, was investigated using PROCESS model 5. The results indicate that for this behaviour, resilience acts as a moderator rather than a mediator. The tested model is shown in Figure 2.

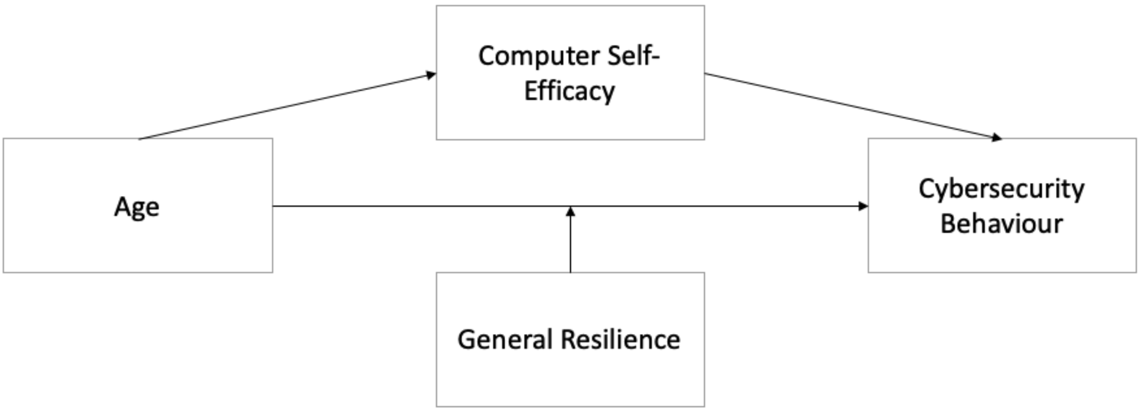

Figure 2. Model testing mediation via computer self-efficacy and moderation via general resilience (PROCESS model 5)

Plotting the estimates shows that the moderation effect of resilience on proactive checking for low (-1SD), mean, and high (+1SD) age (Figure 3). The effect of age on proactive checking is strongest for the high resilience users.

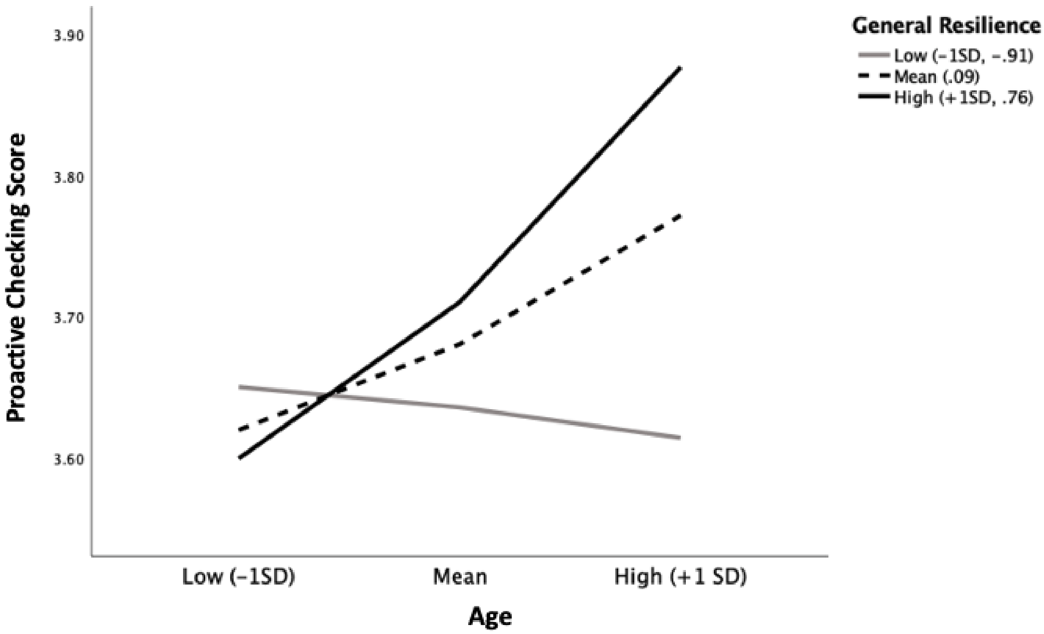

Figure 3. Moderation of the effect of general resilience on proactive checking across low, mean and high age groups.

Table 4. Parallel mediation analysis for each of the cybersecurity behaviours. Significant paths are indicated with an asterix(*).

	Device Securement			Password Generation			Proactive Checking			Updating		
	B	*SE*	CI	*B*	*SE*	CI	*B*	*SE*	CI	*B*	*SE*	CI
Total Effect of Age	-.01	.00	[-.02, -.01]*	.01	.00	[.00, .02]*	.01	.00	[.00, .01]*	.01	.00	[.00, .02]*
Direct Effect of Age	-.01	.00	[-.02, -.01]*	.01	.00	[.01, .02]*	.01	.00	[.00, .01]*	.01	.00	[.01, .02]*
Indirect Effect via Self-Efficacy	-.00	.00	[-.00, .00]	-.00	.00	[-.00, -.00]*	-.00	.00	[-.00, -.00]*	-.00	.00	[-00, -.00]*
Indirect Effect via Resilience	.00	.00	[.00, .00]*	.00	.00	[.00, .00]*	.00	.00	[.00, .00]	.00	.00	[.00, .00]*

4. Discussion

This study expands upon the current literature by investigating age and gender differences in relation to different cybersecurity behaviours. Our results show that rather than older adults being universally more at risk than others, age differences vary according to the specific security behaviour in question. Therefore, rather than focusing on first level digital divides (i.e., ICT access and adoption) our findings highlight the importance of investigating ICT behaviour on a more granular level, i.e., investigating specific types of behaviour and/or activities (something also identified by [19]). Whilst younger users appear more likely to secure access to their devices than the older age groups, they also appear *less* likely to generate secure passwords and/or update their device, and show less proactive URL/email checking behaviours. Our result regarding proactive checking provides a reason younger users may be more susceptible to phishing [17], and older adults to be less likely to adopt security measures to secure physical use of their devices [24]. Similarly, a recent study [38] found that – in direct contrast to their original hypothesis - older users are less likely to share their passwords. Our study helps to strengthen the emerging positive discourse that older users are security conscious, challenging dated stereotypes that this age group are not tech savvy [14]. Many older adults actually display high levels of awareness and ability in regards to cybersecurity [38–40].

It can appear contradictory that older users on the one hand are security conscious and generate more secure passwords but are also *less* likely to secure access to their devices, e.g., failing to lock their screen when the device is not in use. On further consideration, this may be due to differences in perceived risks. Existing literature suggests that this age group focuses heavily upon the privacy and security of the data they enter online [41] – which is in keeping with our results which show they are more likely to generate strong passwords, update devices and show proactive checking for risk. In comparison, it is possible that they are not as aware or not as cautious of 'offline risks' around the security of their physical device, such as it being stolen or used maliciously. For instance, if their main point of access is a home computer, they may feel they the device is already secure within the home and that there is little risk of other people accessing it [11]. Interventions to increase the salience and importance of physical device securement may be beneficial for this age group. Based on the existing literature, the most favoured and/or effective intervention approaches for older adults may be those involving in-person support and/or promoting these security behaviours through social connections, peer support and family members [3,40,41,43]. However, it is also important to note that a lack of device securement may be an active choice on behalf of some users and may not represent a lack of awareness. For example, it is possible that older adults knowingly allow others to access their devices, for example research suggests older adults may be more likely to ask trusted others to complete ICT tasks on their behalf [11,44]. There may also be barriers due to problems with biometric security, for example Morrison and colleagues identified that fingerprint readers can be problematic for older users [11].

Similarly, if younger users are the earliest and most intensive users of ICT, and they are *more* likely to secure access to their devices, why is it that they appear to be *less* likely to generate secure passwords, demonstrate pro-active checking for risk or update their devices? Some of these findings could potentially be explained through differences in usage and/or device type. For example, in relation to secure passwords – it could be that younger users are relying more heavily upon automatic password generators [11,45] and/or biometrics (e.g., face ID, fingerprints), therefore removing much of the emphasis on personally generating a secure password. In relation to proactive checking for risk, frequent ICT usage and over familiarisation with the sharing of personal data can lead to overconfidence, complacency and/or security fatigue [46–49] – factors which have been linked to cybersecurity vulnerability [50]. It also possible that the salience of a possible attack may be reduced in the younger age groups due to a lack of learned experience (i.e., not having personally suffered an attack, or heard of friends or family being affected). Regarding younger users reporting being less likely to update their devices, many devices now automatically install software updates as they become available. Trust in automation could lead to users feeling less responsibility and reduce the requirement to check whether their devices are up to date. Our mediation results also suggest that self-efficacy is a significant mediator of age and security behaviour, therefore suggesting that, at least to some extent (and again potentially related to a reliance upon automation), younger users may demonstrate reduced self-efficacy compared to older users. Further qualitative and quantitative research is necessary to identify the factors underlying the age differences and the role of efficacy identified in this study. These insights can help to guide the design of future interventions to promote more secure behaviour.

It is not unexpected that computer self-efficacy would positively predict some cybersecurity behaviour given that it relates to the individual's confidence in their IT capabilities (a similar result was found by Mitzer et al. [51]) and therefore their ability to act securely. It is perhaps more surprising that general resilience was a significant positive predictor across all four behaviours. It could have been expected that resilience would act as a negative predictor due to being associated with self-confidence in 'bouncing back' if anything bad happens, and therefore perhaps less incentive to avoid risks. However, the literature shows that the relationship between resilience and risk is not this simple. It has been suggested that resilience negatively predicts negative health behaviours (e.g., smoking, heavy drinking, drug use) and positively predicts protective health and safety promotion behaviours (e.g., wearing a seatbelt, eating a healthy diet, exercising, crossing the street safely) [29]. This resonates with our results as the behaviours we were predicting were safety promoting. Our findings indicate the general resilience acts as a mediator for three of the four behaviours (device securement, password generation and updating) and as a moderator for the remaining behaviour, pro-active checking for risk. The greatest effect of age on pro-active checking was found for those users who scored high for general resilience. One potential explanation is that younger users' perceptions of resilience may be based more on optimism bias (i.e., feeling resilient but not being proactive to protect against risk), whereas older users' resilience may be based more upon learned experience (and therefore their learned abilities to act proactively to protect against risk in the future). Future research may wish to further investigate the role of resilience in relation to online behaviour.

Interestingly, we found no evidence of gender differences in relation to any of the cybersecurity behaviours. There was a gender difference for computer self-efficacy scores; with males scoring significantly higher than females. This is not unexpected as this trend has traditionally been reported in the previous literature [52]. As self-efficacy can be context specific [31], it is also possible that the Computer Self-Efficacy Scale [35] measures self-efficacy in relation to tasks that males generally feel more confident with. Furthermore - and as noted earlier - self-efficacy relates to an individual's own beliefs about their ability; and does not necessarily reflect actual differences in ability or performance [53]. Even so, it is worth noting, that our findings are contrary to research suggesting that gender differences in perceptions of computer self-efficacy may have abated in recent years [54]. We also found that males scored significantly higher on general resilience, this is a trend that has been observed in the existing literature [55]. Previous research [56] has attributed higher male resilience scores to differences in self-perception and cultural constructions of 'masculinity'.

We recognise the limitations within the current study and make recommendations for future research. Firstly, whilst we included a broad range of ages, most of our participants were below 45 years of age. Future research should seek to follow the recommendations of Hunsaker and Hargittai [2], who call for research to include more subcategories of older adults (see for example [57] who use the categories 55-64yrs, 65-79yrs and 80-97yrs). With more granular analysis of older age groups, it is possible that further group disparities and more complex relationships could emerge (such as U-shaped trends similar to those found by [23].) Secondly, we recognise that this study relies upon self-reported data, and we suggest that future research utilises experimental and/or observational methods. Thirdly, our participants were recruited via an online recruitment platform, therefore they may be more tech-savvy than the general population (similar to that found for mTurk users, e.g., [17]). It should be recognised that they may not be representative of the larger population of ICT users.

5. Conclusions

In this paper we identify behaviour-specific age differences in cybersecurity, highlighting the need for a granular, context-specific approach to identify age-related differences in cybersecurity behaviours; and advise against labelling a particular age group as universally more at risk. While within our sample, older users were more likely to report generating secure passwords, updating their devices and demonstrating pro-active checking for risk. In comparison, they were less likely to secure their device to prevent unauthorised access (e.g., by locking the screen), the relationship between age and security behaviour was mediated by computer efficacy for three of the four behaviours, with the exception being device securement. This indicates that a lack of device securement by older users is due to other reasons, this could include low perceived risk of physical access to devices by malicious parties, and/or an active choice to allow access by others such as family members. General resilience was also a mediator for three of the four behaviours, and a moderator for the remaining behaviour (proactive checking for risk). The relationship between age and pro-active checking was strongest for those users scoring high for resilience. We suggest that this may represent a move from optimism bias in younger users to learned experience (and therefore learned protective mechanisms) in older users. We present multiple recommendations for future research to further explore the impact of age, self-efficacy and resilience on cybersecurity behaviour. Despite gender differences in self-perceived computer self-efficacy and general resilience, no gender differences were found for the cybersecurity behaviours; suggesting that gender does not play a role in cybersecurity behaviour intentions. These findings have implications for future design and development of targeted cybersecurity interventions.

Data Availability

The survey data used to support the findings of this study have been deposited in the University of Bath data archive (DOI will be provided upon publication).

Conflicts of Interest

The authors declare no conflicts of interest.

Funding Statement

This work was supported by the Engineering and Physical Sciences Research Council (EPSRC) as part of the Cybersecurity across the Lifespan (cSALSA) project [EP/P011454/1] and the Centre for Digital Citizens [EP/T022582/1].

6. References

1. Hargittai E. Second-Level Digital Divide: Differences in People's Online Skills. *First Monday* 2002;**7**, DOI: 10.5210/fm.v7i4.942.

2. Hunsaker A, Hargittai E. A review of Internet use among older adults. *New Media Soc* 2018;**20**:3937–54.

3. Mendel T, Toch E. My Mom was Getting this Popup: Understanding Motivations and Processes in Helping Older Relatives with Mobile Security and Privacy. *Proc ACM Interact Mob Wearable Ubiquitous Technol* 2019;**3**:147:1-147:20.

4. *Internet Users, UK*. Office for National Statistics, 2021.

5. *Demographics of Internet and Home Broadband Usage in the United States*. Pew Research Center, 2021.

6. Frik A, Nurgalieva L, Bernd J *et al.* Privacy and Security Threat Models and Mitigation Strategies of Older Adults. 2019, 21–40.

7. Tyler M, Simic V, De George-Walker L. Older adult Internet super-users: counsel from experience. *Act Adapt Aging* 2018;**42**:328–39.

8. Kropczynski J, Aljallad Z, Elrod NJ *et al.* Towards Building Community Collective Efficacy for Managing Digital Privacy and Security within Older Adult Communities. *Proc ACM Hum-Comput Interact* 2021;**4**:255:1-255:27.

9. Anderson M, Perrin A. *Tech Adoption Climbs Amongst Older Adults*. Pew Research Center, 2017.

10. Tyler M, De George-Walker L, Simic V. Motivation matters: Older adults and information communication technologies. *Stud Educ Adults* 2020;**52**:175–94.

11. Morrison B, Coventry L, Briggs P. How do Older Adults feel about engaging with Cyber-Security? *Hum Behav Emerg Technol* 2021;**3**:1033–49.

12. Berkowsky RW, Sharit J, Czaja SJ. Factors Predicting Decisions About Technology Adoption Among Older Adults. *Innov Aging* 2018;**2**:igy002.

13. Page T. Touchscreen mobile devices and older adults: a usability study. *Int J Hum Factors Ergon* 2014;**3**:65.

14. Marquié JC, Jourdan-Boddaert L, Huet N. Do older adults underestimate their actual computer knowledge? *Behav Inf Technol* 2002;**21**:273–80.

15. Coker J. Elderly People in the UK Lost Over £4m to Cybercrime Last Year. *Infosecurity Mag* 2020.

16. Lebek B, Uffen J, Neumann M *et al.* Information security awareness and behavior: A theory-based literature review. *Manag Res Rev* 2014;**22**:42–75.

17. Sheng S, Holbrook M, Kumaraguru P *et al.* Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, 2010, 373–82.

18. Grilli MD, McVeigh KS, Hakim ZM *et al.* Is This Phishing? Older Age Is Associated With Greater Difficulty Discriminating Between Safe and Malicious Emails. *J Gerontol Ser B* 2021;**76**:1711–5.

19. Sarno DM, Lewis JE, Bohil CJ *et al.* Which Phish Is on the Hook? Phishing Vulnerability for Older Versus Younger Adults. *Hum Factors* 2020;**62**:704–17.

20. Oliveira D, Rocha H, Yang H *et al.* Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, 2017, 6412–24.

21. Jones SL, Collins EIM, Levordashka A *et al.* What is “Cyber Security”? Differential Language of Cyber Security Across the Lifespan. *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, 2019, 1–6.

22. Kezer M, Sevi B, Cemalcilar Z *et al.* Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology J Psychosoc Res Cyberspace* 2016;**10**, DOI: 10.5817/CP2016-1-2.

23. Little L, Briggs P, Coventry LM. Who knows about me? An analysis of age-related disclosure preferences. 2011, DOI: 10.14236/ewic/HCI2011.31.

24. Harbach M, De Luca A, Malkin N *et al.* Keep on Lockin’ in the Free World: A Multi-National Comparison of Smartphone Locking. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery, 2016, 4823–7.

25. Friemel TN. The digital divide has grown old: Determinants of a digital divide among seniors. *New Media Soc* 2016;**18**:313–31.

26. Ayyagari R, Crowell A. Risk and Demographics’ Influence on Security Behavior Intentions. *J South Assoc Inf Syst* 2020;**7**.

27. Pearce KE, Rice RE. Digital Divides From Access to Activities: Comparing Mobile and Personal Computer Internet Users. *J Commun* 2013;**63**:721–44.

28. Rhee H-S, Kim C, Ryu YU. Self-efficacy in information security: Its influence on end users’ information security practice behavior. *Comput Secur* 2009;**28**:816–26.

29. Nintachan P. Resilience and Risk-Taking Behavior Among Thai Adolescents Living in Bangkok, Thailand. *Theses Diss* 2007, DOI: https://doi.org/10.25772/HZK1-1S44.

30. Rutter M. Implications of Resilience Concepts for Scientific Understanding. *Ann N Y Acad Sci* 2006;**1094**:1–12.

31. Tømte C, Hatlevik OE. Gender-differences in Self-efficacy ICT related to various ICT-user profiles in Finland and Norway. How do self-efficacy, gender and ICT-user profiles relate to findings from PISA 2006. *Comput Educ* 2011;**57**:1416–24.

32. Vance A, Lowry PB, Eggett D. Using Accountability to Reduce Access Policy Violations in Information Systems. *J Manag Inf Syst* 2013;**29**:263–90.

33. Alotaibi F, Alshehri A. Gender Differences in Information Security Management. *J Comput Commun* 2020;**8**:53–60.

34. Egelman S, Peer E. Scaling the Security Wall Developing a Security Behavior Intentions Scale (SeBIS). 2015.

35. Howard MC. Creation of a Computer Self-Efficacy Measure: Analysis of Internal Consistency, Psychometric Properties, and Validity. *Cyberpsychology Behav Soc Netw* 2014;**17**:677–81.

36. Smith BW, Dalen J, Wiggins K *et al.* The brief resilience scale: Assessing the ability to bounce back. *Int J Behav Med* 2008;**15**:194–200.

37. George D, Mallery P. *SPSS for Windows Step by Step: A Simple Guide and Reference, 17.0 Update - Darren George, Paul Mallery - Google Books*. Allyn & Bacon, 2010.

38. Whitty M, Doodson J, Creese S *et al.* Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology Behav Soc Netw* 2015;**18**:3–7.

39. Hoofnagle CJ, King J, Li S *et al.* How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? *Soc Sci Res Netw* 2010;**4**:10–10.

40. Hunsaker A, Nguyen MH, Fuchs J *et al.* Unsung helpers: older adults as a source of digital media support for their peers. *Commun Rev* 2020.

41. Jiang M, Tsai HS, Cotten SR *et al.* Generational differences in online safety perceptions, knowledge, and practices. *Educ Gerontol* 2016;**42**:621–34.

42. Generational differences in online safety perceptions, knowledge, and practices: Educational Gerontology: Vol 42, No 9.

43. Prange S, Mecke L, Buschek D *et al.* ``Outsourcing'' Security: Supporting People to Support Older Adults. *Proceedings of the Mobile HCI '18 Workshop on Mobile Privacy and Security for an Aging Population*. Barcelona, Spain, 2018, 4.

44. Nthala N, Flechais I. Informal Support Networks: an investigation into Home Data Security Practices. 2018.

45. Ray H, Wolf F, Kuber R *et al.* Why Older Adults (Don't) Use Password Managers. *Proceedings of the 30th USENIX Security Symposium*. 2021, 73–90.

46. Furnell S, Thomson K-L. Recognising and addressing 'security fatigue.' *Comput Fraud Secur* 2009;**2009**:7–11.

47. Livingstone S, Helsper E. Balancing opportunities and risks in teenagers' use of the internet: the role of online skills and internet self-efficacy. *New Media Soc* 2010;**12**:309–29.

48. Stanton B, Theofanos MF, Prettyman SS *et al.* Security Fatigue. *IT Prof* 2016;**18**:26–32.

49. Brodsky JE, Lodhi AK, Powers KL *et al.* "It's just everywhere now": Middle-school and college students' mental models of the Internet. *Hum Behav Emerg Technol* 2021;**3**:495–511.

50. Nicholson J, Coventry L, Briggs P. Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection. 2017.

51. Mitzner TL, Boron JB, Fausset CB *et al.* Older adults talk technology: Technology usage and attitudes. *Comput Hum Behav* 2010;**26**:1710–21.

52. Hargittai E, Shafer S. Differences in Actual and Perceived Online Skills: The Role of Gender*. *Soc Sci Q* 2006;**87**:432–48.

53. Fatokun FB, Hamid S, Norman A *et al.* The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *J Phys Conf Ser* 2019;**1339**:012098.

54. Hatlevik OE, Throndsen I, Loi M *et al.* Students' ICT self-efficacy and computer and information literacy: Determinants and relationships. *Comput Educ* 2018;**118**:107–19.

55. Rahimi B, Baetz M, Bowen R *et al.* Resilience, stress, and coping among Canadian medical students. *Can Med Educ J* 2014;**5**:e5–12.

56. Overholt JR, Ewert A. Gender Matters: Exploring the Process of Developing Resilience Through Outdoor Adventure. *J Exp Educ* 2015;**38**:41–55.

57. Hargittai E, Dobransky K. Old Dogs, New Clicks: Digital Inequality in Skills and Uses among Older Adults. *Can J Commun* 2017;**42**, DOI: 10.22230/cjc.2017v42n2a3176.