

Dissecting Generation Gaps in Cybersecurity Practices

Muhammad Sohail Munir ¹  and Muhammad Hamid ^{2,*} 

¹ Punjab Institute of Management and Professional Development, Government of the Punjab, Lahore, Pakistan;
r.m.sohail.munir@gmail.com.

² Department of Computer Science, Government College Women University, Sialkot, Pakistan; mhamid@gcwus.edu.pk.

* Correspondence: mhamid@gcwus.edu.pk;

Abstract: As the global population ages, Internet use among older adults is increasing, making it important to understand their usage patterns and changes over time. This knowledge can inform strategies to support digital engagement in later life. This article reviews quantitative studies on older adults' Internet use, focusing on access, skills, and usage types, as well as social inequalities. It also examines links between health and digital behaviors. Using an online survey of 740 participants, the study analyzed age differences in security practices such as software updates, password creation, device protection, and monitoring. Results show older adults update less but create stronger passwords and display proactive awareness. Gender had no effect, while resilience shaped multiple behaviors. Findings support targeted training and policies.

Keywords: Digital Inequality; Internet Usage; Internet Skills; Older Folks; Surveys.

1. Introduction

With the world population experiencing an aging trend and longer life expectancies [1], the demographic of older individuals is becoming increasingly significant in terms of the present. The prolongation of life spans has resulted in a considerable fraction of individuals experiencing a substantial period of their lives as older adults. However, current research suggests that antiquated societal perceptions of aging hinder technology marketplaces from recognizing older adults' valuable and enormous consumer potential [2]. Moreover, it is worth noting that a significant proportion of the elderly population holds a favorable perception of the societal benefits of technology. However, a substantial majority, over 75%, of older persons express a lack of self-assurance when utilizing electronic gadgets for online activities [3]. The contrasts above manifest in the persistent global inequality in internet usage between older individuals, the general adult population and younger age cohorts [4]. Gaining insight into the internet usage and skills of older adults and examining the evolution of their measurement methods holds considerable importance. This endeavor contributes to a more holistic understanding of internet usage within society. It provides valuable insights into the extent to which digital media can effectively cater to the needs of this demographic [5].

More people are utilizing digital technology than ever; nonetheless, "digital divides" remain problematic among user groups [6, 7 & 8]. These digital inequalities are frequently discussed about demographic parameters such as age and gender as potential modifiers. Even though younger age groups have traditionally been the first to embrace ICT, this demographic is already nearing saturation (99% of UK youth currently use the Internet [9]). As a direct result, those over the age of 65 have become the demographic with the highest rate of adoption [9, 10 & 11]. Even though many people over 60 are eager to adopt new technologies [12], a negative narrative is still prevalent [13].

For instance, studies reveal that this user group still shows impairments in ICT skills and literacy [7, 17 & 18] and that they may still lack confidence in their abilities (or self-efficacy) to utilize their devices [14, 15 & 16]. This is what many people mean when they talk about the "second level" of the digital divide (the first level being access to ICT) [6]. However, other research suggests that older people may underestimate their talents and knowledge rather than suffer from a genuine skill gap [19]. Hunsaker and Hargittai [7] examine this issue and note a methodological difficulty when

studying older people. They note that the order of ages, the types of ages considered and the threshold for maturity all vary among researchers. The age at which older adulthood should begin varies from study to study. They advocated for additional research to determine whether or not age differences are still present.

There may be an age-related difference in the vulnerabilities of different users; however, this has not been proven. However, [20] suggests consumers under 30 are more vulnerable to phishing attacks. Despite their natural skepticism, older adults have problems distinguishing between real and phishing emails [21]. The capacity to recognize phishing emails was not affected by age, as reported by Sarno et al. [22], with older women being straightforward prey. According to other studies, the older generation may be less concerned about privacy and security because they are more likely to utilize social media and share personal information [23, 24 & 25]. An increasing cybersecurity risk is associated with the widespread adoption of digital connectivity. The elderly are the newest demographic to be targeted by cybercriminals as they spend more time online; in the UK alone, the elderly lost 4 million pounds in 2018 and 2019 [26 & 27]. Detecting and addressing age-specific vulnerabilities is challenging due to the lack of studies and investigations of changes in posture and attitude toward cybersecurity associated with age [16 & 28].

The present study aims to overcome the limitations observed in earlier research by utilizing data collected from individuals across the whole adult lifespan, ranging from 19 to 83 years. Earlier studies have frequently focused on narrow age ranges, primarily due to practical challenges associated with data collecting [29]. A recent survey by Ayyagari and Crowell [30] examined variations in cybersecurity behaviors among three distinct age groups. However, it is essential to note that their investigation was partial to a sample populace from an academic setting and the oldest age group included individuals aged 36 years and above. Furthermore, our paper gives to the existing body of writings by examining the impact of computer self-efficacy on ICT behavior and evaluating reported behaviors [31 & 32]. There is a documented association between psychological resilience and engagement in risky behavior. Resilience is associated with risk-averse behaviors, contingent on particular studies on contextual factors [33 & 34]. Consequently, we incorporate a comprehensive measure of resilience as an independent variable in our research. Low confidence and lack of knowledge are cited as factors that cause the difficulty of older people in participating fully in cybersecurity actions [16]. Older adults are less likely to understand the dangers of doing nothing. They also can't use security features like a PIN or biometric check to prevent illegal device access [35]. For instance, they are less likely to implement safeguards to prevent malicious software from accessing their machines. Considered as a whole, the present study's findings suggest that concerns about cyber security may include more factors that can be reduced to categorizing individuals based on their age. Understanding how adults of varying ages participate in various security behaviors to protect themselves online is critical. This study fills a void in the existing research by focusing on four essential behaviors that are related to cybersecurity. These behaviors are secure password generation, device securement (for example, Users should engage in the practice of securing their device screen by locking it while it is not actively being utilized.), regular software updating and proactive checking (It is advisable to verify the authenticity and security indicators of hyperlinks before to engaging with them, including scrutinizing unified resource locators and the senders associated with them).

This study additionally examines gender disparities, given the uncertain nature of prior research in this domain. Historically, scholarly investigations have indicated that females are traditionally less confident using computers than men. [23 & 24]. However, more recent studies [25] propose that this masculinity disparity may be lessening. It is imperative to acknowledge that self-efficacy pertains to an individual's convictions regarding their ability to perform [26]. Therefore, it is challenging to ascertain if gender disparities indicate disparities in genuine aptitude and/or self-perception [35]. The concept of computer self-efficacy can exhibit contextual variations, as evidenced by multiple studies indicating that gender disparities may vary depending on the specific context, for example, the use of information and communication technology (ICT) for educational objectives in contrast to its

application in the public domain [29], or the nature of the task itself, such as internet-related tasks versus more advanced software-related tasks [36]. Several studies on cybersecurity behaviors have found that females exhibit higher online privacy concerns [31] and stronger adherence to security policies [37]. While some studies indicate the absence of gender disparities, such as the research conducted by Vance et al. [37], which identified no gender differences in intention to adhere to security standards, other studies propose females may exhibit less secure behavior [38]. In their review, Hunsaker and Hargittai [7] characterized the extant literature on older adult studies as inconclusive. To cater to the imperative of enhanced comprehension, we have incorporated gender analyses into the present investigation.

After adjusting for factors such as computer self-efficacy and general resilience, the paper aims to examine whether there are variances in cybersecurity behavior across the mature/adult lifetime depending on aspects such as time of life and gender. The findings determine which regions should receive priority in future-focused training and development efforts.

In this article, Section 2 explains the methodology and experiments needed to carry out this research, Section 3b discusses the results, Section 4 discusses the key findings and Section 5 concludes the overall research with future work.

2. Methodology/ Experimentation

This section discusses the methodology and experiments used to find cybersecurity behaviors.

An online survey was disseminated through the online platforms Google Forms and SurveyMonkey. The initial sample of 915 replies underwent a cleaning process, during which 175 responses were excluded from the analysis due to not meeting the quality control criteria. The sample for this study comprises data collected from 740 participants, whose ages ranged from 19 to 90 ($M=35.49$ years, $SD=12.10$ years). Table 1 displays more detailed information.

Table 1. Dissecting Gender and Age Gaps in Cybersecurity.

		Sample Number	Percentage
Age	19-25	131	22.6
	26-35	219	37.8
	36-45	143	24.7
	46-55	46	7.9
	56-65	26	4.5
	66-75	12	2.1
	76-90	2	0.3
Gender	Male	385	52.02
	Female	348	47.02
	Other	7	.96
Education	Primary/elementary school	5	0.66
	Secondary/high school	70	9.46
	College/A-level	200	27.03
	Bachelors	300	40.56
	Masters	135	18.24
	Doctorate	30	4.05
Country	Canada	90	12.16
	Germany	55	7.43

	France	30	4.05
	New Zealand	40	5.41
	Norway	45	6.08
	Russia	140	18.92
	South Africa	100	13.51
	United Kingdom	110	14.86
	USA	130	17.57

In conjunction with the demographic inquiries, contributors were requested to respond to questions assessing cybersecurity behavior, computer proficiency and overall pliability. Cybersecurity-related behavior was measured via the Security Behavior Intentions Scale [39]. The Security Behavior Intentions Scale comprises sixteen items organized into four distinct subscales. These subscales assess individuals' attitudes toward device securement, software updating, proactive checking and password generating. Cronbach's alpha (α) values for the scale's four subscales ranged from .65 to .76, indicating that the scale's reliability produced promising findings in our study. These values may be found in Tables 2, 3, 4 and 5. The researchers employed the computer proficiency gauge [40] to assess participants' perceptions of their competence in information and communication technologies. The dependability of the scale was found to be excellent, with a coefficient alpha value of 0.95. Overall pliability was measured using the Brief Resilience Scale [41], with a reliability coefficient (α) of .91.

Table 2. Regression Results of Device Securement.

Device securement $\pm$ ($\alpha=.65$)				
B	Age	Gender	Self- efficiency	Resilience
Beta	-.02	.08	.08	.13
SE	-.19	.05	.08	.13
BCa CI	.00	.09	.06	.06
R2 (CI)	-.03, -.02 ***	-.10, .23	-.03, .17	.04, .22*
B				.06(.03, .09)
Note: ± 3000 bootstrap samples. *** $p < .001$, ** $p < .01$ and * $p < .05$				

Table 3. Regression Results of Password Generation.

Password Generation ($\alpha=.72$)				
	Age	Gender	Self- efficiency	Resilience
B	.02	-.12	.24	.14
Beta	-.17	-.07	.24	.14
SE	.00	.08	.05	.05
t	4.10 ***	-1.62	5.40***	3.32**
R2				.14*
Note: ± 3000 bootstrap samples. *** $p < .001$, ** $p < .01$ and * $p < .05$				

Table 4. Regression Results of Proactive Checking.

Proactive Checking ($\alpha=.67$)				
	Age	Gender	Self- efficiency	Resilience
B	.02	-.07	.25	.08
Beta	.15	-.05	.30	.09
SE	.00	.07	.05	.04
t	3.52 ***	-0.93	6.59***	2.03*
R2				.126**
Note: ± 3000 bootstrap samples. *** $p < .001$, ** $p < .01$ and * $p < .05$				

Table 5. Regression Results of Updating.

Updating ($\alpha=.76$)				
	Age	Gender	Self- efficiency	Resilience
B	.02	-.09	.32	.11
Beta	.17	-.06	.31	.12
SE	.00	.08	.06	.05
t	4.16 ***	-1.13	7.02***	2.61**
R2				.16*
Note: ± 3000 bootstrap samples. *** $p < .001$, ** $p < .01$ and * $p < .05$				

The study assessed hypothesis and discriminant cogency to verify that the scale accurately measured its intended construct & the scales were effectively loading onto distinct apparatuses/components. The convergent soundness of both measures demonstrates a high level of

excellence. Specifically, the computer self-efficacy scale exhibits a construct validity coefficient of .97 and an average variance extracted of .65. Similarly, the general reliance scale demonstrates a construct validity coefficient of .94 and an average variance extracted of .67. The researchers used the heterotrait-monotrait ratio of correlations as a method to evaluate the discriminant validity. The discriminant validity was assessed as excellent, as shown by a Heterotrait-Monotrait ratio of 0.30 (42).

3. Results

The statistical software, the Statistical Package for the Social Sciences, was used to analyze the data. The proportion of missing data was less than 0.4% of the total elements. The results of Little's MCAR test were not statistically significant ($\chi^2(120) = 123.67, p = .47$), suggesting that the missing data in the study were entirely random. Consequently, the researchers employed the estimated maximum likelihood method to calculate the missing data. The exclusion of the other gender category from the analysis resulted from the limited sample size ($n = 4$).

The data was subjected to a comprehensive analysis to ascertain whether or not they complied with the presumptions of normalcy, independence and homoscedasticity. After taking the readings, they were checked to ensure they were within the expected limits according to the measurement scales used. There was no indication that the predictor factors were correlated with one another in any way, as evidenced by the correlations between them being less than 0.8 (refer to Table 6). Additionally, the variance inflation factor (VIF) scores were below 3. Furthermore, while examining the standardized residuals and predicted values showed that homoscedasticity was reasonably satisfied. All dependent variables exhibited a typical distribution pattern on the Q-Q plots, with skewness and kurtosis values below 3, except for the variable related to device securement. The latter observation demonstrated a negative skew, indicating a greater concentration of scores towards the upper end of the scale. However, it is essential to note that this skew is within the permitted range of ± 3 [43]. The securement of the device likewise exhibited a kurtosis value of 2.30. As a result of the breach of the normality assumption in device securement, all analyses about this variable were conducted via the bootstrapping approach. This approach, which employed bias-corrected and accelerated confidence intervals with a sample size of 3000, was used to ensure the reliability and stability of the results.

Table 6 illustrates the bivariate correlations for each component, which may be found here. There is no significant correlation between age and gender, and none of the connections raises any red flags regarding the possibility of multiple correlations.

Table 6. Bivariate Correlations for Each of the Variables.

			SD	1	2	3	4	5	6	7	8
1.	Age	35.49	12.10	—							
2.	Gender	—	—	.04	—						
3.	Self-efficacy	3.65	.85	-.12**	.40***	—					
4.	Resilience	3.25	.88	.12**	-.13**	.24** *	—				
5.	Device seurement	4.07	.86	-.19***	-.02	.11*	.12**	—			
6.	Password generation	3.30	.85	.16***	-.18***	.28** *	.22** *	.20***	—		
7.	Proactive checking	3.72	.70	.13**	-.17***	.32** *	.18** *	.19***	.46***	—	
8.	Updating	3.43	.90	.15***	-.18***	.35** *	.21** *	.18***	.32***	.29***	—

We used a parallel mediation analysis with the PROCESS macro for SPSS (Hayes Process Macro – Model 4 – Mediation Analysis with Multiple Mediators, Figure 1.) to delve deeper into the correlation between chronological age and a person's sense of computer self-efficacy and resilience.

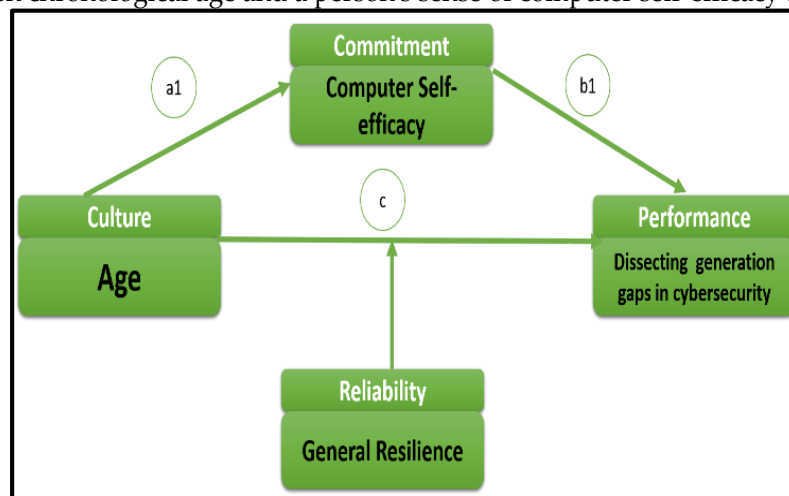


Figure 1. Mediation Analysis with Multiple Mediators.

All product-defining variables were mean-centered in the PROCESS mediation analysis to facilitate data interpretation. Table 7 displays the findings. The study found that age indirectly influenced cybersecurity behavior through the mediator of self-efficacy. Specifically, this indirect effect was significant for 3/4 of the behaviors examined, namely “password generation,” “proactive checking,” and “updating.” The outcomes of this study indicate that self-efficacy did not have a significant mediating role in “device securement.”

Table 7. Dissecting Generation Gaps in Cybersecurity Practices through Parallel Mediation Analysis.

		The cumulative impact of age	A direct result of aging	Self-confidence's indirect influence	Indirect impact via adaptability
Device securement	B	-.01	-.01	-.00	.00
	SE	.00	.00	.00	.00
	CI	(-.02, -.01) *	(-.02, -.01) *	(-.00, .00)	(.00, .00) *
Password generation	B	.01	.01	-.00	.00
	SE	.00	.00	.00	.00
	CI	(.00, .02) *	(.01, .02) *	(-.00, -.00) *	(.00, .00) *
Proactive checking	B	.01	.01	-.00	.00
	SE	.00	.00	.00	.00
	CI	(.00, .01) *	(.00, .01) *	(-.00, -.00) *	(.00, .00)
Updating	B	.01	.01	-.00	.00
	SE	.00	.00	.00	.00
	CI	(.00, .02) *	(.01, .02) *	(-.00, -.00) *	(.00, .00) *
Note: * shows significant path					

The study found that age had a substantial indirect impact on cybersecurity behavior via the mediator of resilience. Specifically, this effect was shown in three behaviors: password generation, updating and device securement. The research used the PROCESS-model-5 framework to investigate

the influence of resilience on proactive checking, the final cybersecurity activity. According to the findings, resilience does not play the role of a mediator regarding this particular behavior. Instead, it plays the role of a moderator. Figure 2 shows the model that was put through its paces.

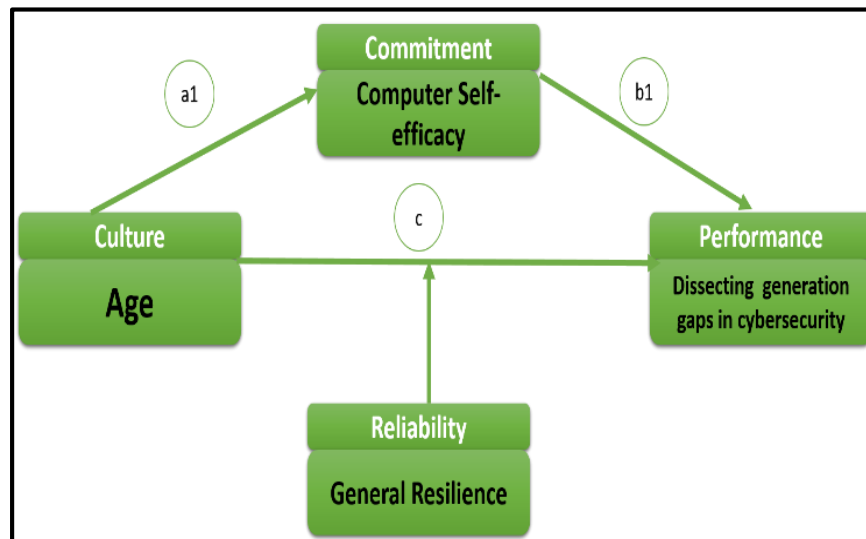


Figure 2. PROCESS-model-5 framework.

4. Findings

Our study's findings indicate that older persons' vulnerability to security risks is not uniform but contingent upon the particular security behavior under consideration. Hence, instead of prioritizing primary-level disparities in digital access and adoption, our research underscores the need to examine the behavior of information communication technologies at a more detailed level. This entails researching certain kinds of behavior and/or activities, as well acknowledged by previous studies [22]. While it is observed that younger folks generally possess more accessibility to their electronic devices in comparison to older age cohorts, they also exhibit a diminished inclination towards establishing robust passwords, updating their technological equipment and actively verifying site addresses, web forms and emails. The findings of our study suggest that younger individuals may be more vulnerable to phishing attacks [20]. At the same time, older persons may exhibit a lower willingness to implement security measures for protecting the physical usage of their devices [35].

In line with the researchers' initial idea, a recent study [44] discovered that elderly individuals have a decreased tendency to reveal passwords. Our research contributes to the growing body of evidence showing older individuals exhibit a heightened awareness of security measures, contradicting outdated assumptions that this demographic lacks technological proficiency [19]. Many elderly individuals exhibit notable knowledge and proficiency in cybersecurity [44, 45 & 46]. The observation may be that older individuals exhibit paradoxical behavior regarding their security practices. On one side, they demonstrate a heightened security awareness by creating more robust and secure passwords. On the other hand, they tend to neglect securing access to their devices, such as activating screen locks while the devices are not in use. Upon further examination, the observed variations might be attributed to disparities in the contextual application and the corresponding perceived levels of risk.

The available scholarly sources indicate that individuals in this particular age bracket exhibit a significant concern for the privacy and security of the information they provide on the Internet [47]. This finding aligns with our research findings, demonstrating that this age group is more inclined to create robust passwords, regularly upgrade their devices and actively engage in risk assessment. In

contrast, it is conceivable that individuals may exhibit a lesser degree of awareness or caution about "The potential hazards associated with offline activities" regarding the security of their physical devices, such as the potential for theft or malevolent use. For example, individuals who primarily use a personal computer for their online activities may perceive that the equipment is adequately protected inside the confines of their residence, hence perceiving less vulnerability to unauthorized access by others [16].

Implementing interventions to enhance the visibility and significance of securely fastening physical devices might benefit individuals within this particular age cohort. According to the extant research, intervention techniques that are highly regarded and potentially efficacious for older persons include face-to-face assistance and encourage the adoption of secure behaviors via social networks, peer support and familial relationships [8, 46, 47 & 48]. Nevertheless, it is crucial to acknowledge that the absence of device securement might potentially be a deliberate decision made by some users rather than indicating deficient understanding. It's conceivable, for instance, that seniors would knowingly hand over control of their smartphones to their children or grandchildren. Some evidence suggests that older people are more likely to enlist the help of reliable third parties when completing ICT tasks [16, 49]. Barriers may also arise as a result of challenges associated with biometric security. For instance, Morrison et al. [16] have highlighted the potential issues elderly users may have with fingerprint scanners.

The optimistic prediction of specific cybersecurity behavior by computer self-efficacy may be anticipated since it is associated with an individual's confidence in their Information Technology skills. This finding aligns with the results reported by Mitzer et al. [50], suggesting that higher levels of computer self-efficacy are linked to a greater capacity to engage in secure actions. It is noteworthy that overall resilience had a significant positive predictive relationship with all four behaviors. The negative predictive nature of resilience may be anticipated since it is linked to self-confidence in effectively recovering from adverse events, perhaps resulting in less motivation to evade hazards. Nevertheless, existing data indicates the association between pliability and risk is not as straightforward as previously assumed.

Previous research has proposed a correlation between resilience and health-related behaviors. Specifically, it has been suggested that resilience is inversely associated with harmful health behaviors such as smoking, heavy drinking and drug use. Conversely, resilience is positively associated with engaging in health-promoting behaviors that provide protection and safety, such as wearing a seatbelt, maintaining a healthy diet, engaging in regular exercise and practicing safe pedestrian behavior [35]. Our findings align with the outcomes obtained since the behaviors we hypothesized were shown to be conducive to fostering safety. Our findings show that general resilience mediates the relationships between three of the four behaviors we looked at (device security, password generation and updating and proactive screening for risk) and moderates the relationship between the other two behaviors. The individuals who exhibited high levels of overall resilience were shown to be more significantly impacted by age regarding proactive checking. One plausible explanation is that the perception of resilience among younger users could be influenced by optimism bias, wherein they feel resilient without actively taking measures to mitigate risks. In contrast, older users' resilience may be rooted in their accumulated experiences, enabling them to safeguard against future risks proactively. Subsequent studies may consider doing deeper investigations into the significance of resilience in the context of online behavior.

In a similar vein, it is worth considering why younger users, who tend to be the first and most avid adopters of information and communication technology, exhibit a lower propensity to create safe passwords, engage in proactive risk assessment, or regularly upgrade their devices, despite their greater likelihood of possessing exclusive access to those gadgets. Specific results may be attributed to variations in use patterns and/or device types. In the context of safe passwords, younger individuals may be more dependent on automated password generators [16, 51] and/or biometric authentication methods such as face identification and fingerprints. Consequently, there is a reduced

focus on individually creating a strong password. Regularly using information and communication technology and being too comfortable disclosing personal data may result in an inflated sense of confidence, complacency and security weariness. These characteristics have increased susceptibility to cybersecurity threats [52, 53, 54 & 55]. The diminished significance of a potential assault among younger individuals may be attributed to their limited exposure to personal experiences or anecdotes of friends and family being impacted, as shown by previous research [56].

About the observation that younger users exhibit a lower propensity to update their gadgets, it is worth noting that several devices nowadays can install software updates promptly and automatically. Establishing trust in automation may result in consumers experiencing a diminished sense of responsibility and a decreased inclination to verify the currency of their equipment. Nevertheless, it is crucial to acknowledge that the association between age and trust is intricate and contingent upon several variables [57, 58, 59 & 60]. Although several studies propose that older individuals may exhibit a higher inclination to place faith in automation [61 & 62], it's worth noting that age gaps may seem different in different places and situations [57, 58]. Further investigation is necessary in this domain to ascertain the underlying reason. According to our investigation into the mediation function, the self-efficacy variable plays a significant part in the connection between age and security-related behaviors. This suggests that younger users, potentially due to their reliance on automation, may exhibit lower levels of self-efficiency related to mature handlers. Additional qualitative and quantitative research is required to determine the elements contributing to age disparities and the significance of effectiveness, as revealed in this study. These observations may provide valuable guidance for future treatments' design to promote more secure behavior.

Limitations of the current study are discussed and suggestions for further research are offered. To begin, although we did have various ages represented, most of our participants were younger than 45. Hunsaker and Hargittai [7] advocate splitting up the older adult population into more specific age ranges in future studies (e.g., [63] divides people into three groups: "55–64" years old, "65–79" years old and "80–97" years old). Further group inequalities and more complicated correlations (patterns like the U observed in [26]) may become apparent with more thorough research of older age groups. Researchers at [56] found that people over the age of 59 were more susceptible to phishing, which might be further evidence of the U-shaped nature of this connection. Second, we acknowledge that this paper is inadequate for the reliability of self-reported data and advocate for using experimental and/or observational methodologies in future studies. In conclusion, it is worth noting that the participants in our study were using an online platform, which suggests they may possess a greater degree of technical proficiency than the broader community (as reported for m-Turk users; see, for example, [20]). It is essential to remember that they cannot reflect all people who utilize information and communication technologies.

It's interesting to note that we didn't find any indication of gender disparities in any cybersecurity behaviors people engage in. There was a considerable gap in the levels of computer self-efficacy between men and females, with males achieving much greater levels than girls. This should not be surprising, given that this pattern has been consistently documented in the literature [64]. The computer self-efficacy measure [40] is believed to assess self-efficacy specifically about activities often associated with higher confidence levels among males. This phenomenon arises from the observation that the level of self-efficacy may vary depending on the specific circumstances in which it is assessed [36]. Furthermore, as previously said, self-efficacy pertains to an individual's beliefs about their capacity and it may not necessarily reflect actual differences in skill or achievement [65, 69]. However, it is crucial to note that our findings contradict the existing research indicating a potential reduction in gender disparities in perceptions of computer self-efficacy in recent years [66]. Furthermore, it was found that male participants had significantly greater overall resilience. This finding aligns with earlier research studies [67]. Prior research [68] has shown that disparities in self-perception and cultural constructions of "masculinity" might account for the higher levels of resilience reported by men.

5. Conclusions

This study aims to examine dissecting generation gaps in cyber security practices, emphasizing the need to adopt a detailed and context-specific methodology to discover such variations. It cautions against generalizing the vulnerability of a particular age group as uniformly higher in terms of cyber security risks. The present study observed that older participants tended to engage in behaviors such as creating safe passwords, regularly upgrading their gadgets and actively monitoring potential risks. In contrast, participants were less likely to take measures to protect their devices to prevent unauthorized access, such as bolting the mobile or computer display.

We give several suggestions for new lines of inquiry that may be taken up in the future to investigate further the influence that age, self-efficacy and resilience have on cybersecurity behavior. Despite gender differences in self-perceived computer self-efficacy (comparable to [65]) and general resilience, no gender differences were found in cybersecurity practices. Based on these findings, it seems that gender does not play a part in the motivations behind cybersecurity conduct. This lends some credence to the research conducted by [56], which discovered that there were no gender differences in susceptibility to phishing across most of their conditions (Apart from banking phishing emails, it was found that males exhibited more sensitivity). It should be highlighted, however, that the research that has been done thus far on gender differences has produced contradictory results. For example, a study by [65] revealed significant disparities in cybersecurity behavior across genders, indicating the need for more research to explore the potentially intricate impact of gender.

The correlation between age and security behavior was impacted by computer effectiveness in three of the four behaviors, except device securement. This suggests that elderly users' failure to safeguard their devices might be attributed to several factors, such as a perceived low danger of physical access by hostile individuals and a deliberate decision to provide access to family members. Additionally, it was shown that general resilience had a mediating role in three of the four behaviors examined and acted as a moderator in the case of the fourth behavior, namely proactive risk assessment. The correlation between age and proactive checking had the highest magnitude among those who scored high on resilience measures.

It is suggested that this phenomenon may indicate a transition from an optimistic bias seen in younger users to the acquisition of acquired experience and subsequent development of defensive mechanisms in older users. This statement aligns with a study by [65], which concluded that younger individuals exhibit lower awareness of cyber threats. Additionally, another study by [56] highlights that acquiring knowledge via experience is a significant determinant of secure behavior in the context of phishing attacks. The need to assess cybersecurity behavior variations at a more nuanced level is emphasized, as this has significant implications for the future design and implementation of targeted cybersecurity interventions and the formulation of policy and practice.

Declarations

Acknowledgments

Thanks to our families and colleagues, who provided moral support.

Ethics Approval and Consent to Participate

The results/data/figures in this manuscript have not been published elsewhere, nor are they under consideration by another publisher. All the material is owned by the authors, and/or no permissions are required.

Consent for Publication

This article does not contain any studies with human participants or animals performed by any of the authors.

Availability of Data and Materials

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Competing Interests

The authors declare no competing interests in the research.

Funding

This research was not supported by any funding agency or institute.

References

1. United Nations (2017) World Population Prospects: The 2017 Revision, Key Findings and Advance Tables (ESA/P/WP/248). New York: Department of Economic and Social Affairs, Population Division.
2. Coughlin JF (2017) The Longevity Economy: Unlocking the World's Fastest-Growing, Most Misunderstood Market. New York: PublicAffairs.
3. Anderson M and Perrin A (2017) Tech adoption climbs among older adults. Pew Research Center: Internet, Science & Technology. Available at: <https://www.pewresearch.org/internet/2017/05/17/tech-adoption-climbs-among-older-adults/> (accessed 28 August 2017).
4. Center for the Digital Future (2016) The World Internet Project: International Report. 6th ed. USC Annenberg School. Available at: <http://www.digitalcenter.org/wp-content/uploads/2013/06/2015-World-Internet-Report.pdf> (accessed 4 September 2017).
5. Munir, Muhammad Sohail, et al. "Use of Different Machine Learning Algorithms for Hate Speech Detection." 2022 International Conference on Cyber Resilience (ICCR). IEEE, 2022.
6. E. Hargittai, "Second-level digital divide: differences in people's online skills," First Monday, vol. 7, no. 4, 2002.
7. A. Hunsaker and E. Hargittai, "A review of Internet use among older adults," New Media & Society, vol. 20, no. 10, pp. 3937–3954, 2018.
8. T. Mendel and E. Toch, "My mom was getting this Popup," Proc ACM Interact Mob Wearable Ubiquitous Technol, vol. 3, no. 4, pp. 1–20, 2019.
9. Internet Users, UK, Office for National Statistics, 2021.
10. Pew Research Center, Demographics of Internet and Home Broadband Usage in the United States, Pew Research Center, 2021.
11. A. Frik, L. Nurgalieva, J. Bernd, J. Lee, F. Schaub, and S. Egelman, Privacy and security threat models and mitigation strategies of older adults, Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), 2019.
12. M. Tyler, V. Simic, and L. De George-Walker, "Older adult Internet super-users: counsel from experience," Activities, Adaptation, & Aging, vol. 42, no. 4, pp. 328–339, 2018.
13. J. Kropczynski, Z. Aljallad, N. J. Elrod, H. Lipford, and P. J. Wisniewski, "Towards building community collective efficacy for managing digital privacy and security within older adult communities," Proc ACM Hum-Comput Interact, vol. 4, pp. 1–27, 2021.
14. M. Anderson and A. Perrin, Tech adoption climbs among older adults, Pew Research Center, 2017.
15. M. Tyler, L. De George-Walker, and V. Simic, "Motivation matters: older adults and information communication technologies," Stud Educ Adults, vol. 52, no. 2, pp. 175–194, 2020.
16. B. Morrison, L. Coventry, and P. Briggs, "How do older adults feel about engaging with cyber-security?" Hum Behav Emerg Technol, vol. 3, no. 5, pp. 1033–1049, 2021.
17. R. W. Berkowsky, J. Sharit, and S. J. Czaja, "Factors predicting decisions about technology adoption among older adults," Innovation in Aging, vol. 2, article igy002, 2017.
18. T. Page, "Touchscreen mobile devices and older adults: a usability study," Int J Hum Factors Ergon, vol. 3, no. 1, p. 65, 2014.

19. J. C. Marquié, L. Jourdan-Boddaert, and N. Huet, "Do older adults underestimate their actual computer knowledge?" *Behaviour & Information Technology*, vol. 21, no. 4, pp. 273–280, 2002.
20. S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions," pp. 373–382, Association for Computing Machinery.
21. M. D. Grilli, K. S. McVeigh, Z. M. Hakim et al., "Is this phishing? Older age is associated with greater difficulty discriminating between safe and malicious emails," *J Gerontol Ser B*, vol. 76, no. 9, pp. 1711–1715, 2021.
22. D. M. Sarno, J. E. Lewis, C. J. Bohil, and M. B. Neider, "Which phish is on the hook? Phishing vulnerability for older versus younger adults," *Human Factors*, vol. 62, no. 5, pp. 704–717, 2020.
23. D. Oliveira, H. Rocha, H. Yang 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," pp. 6412–6424, Association for Computing Machinery.
24. S. L. Jones, E. I. Collins, A. Levordashka, K. Muir, and A. Joinson, 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, Association for Computing Machinery, New York, NY, USA, 2019.
25. M. Kezer, B. Sevi, Z. Cemalcilar, and L. Baruh, "Age differences in privacy attitudes, literacy and privacy management on Facebook," *Cyberpsychology J Psychosoc Res Cyberspace*, vol. 10, no. 1, 2016.
26. L. Little, P. Briggs, and L. M. Coventry, Who knows about me? An analysis of age-related disclosure preferences, 2011.
27. J. Coker, "Elderly people in the UK lost over £4m to cybercrime last year," *Infosecurity Mag*, vol. 3, 2020.
28. B. Lebek, J. Uffen, M. Neumann, B. Hohler, and H. M. Breitner, "Information security awareness and behavior: a theory-based literature review," *Management Research Review*, vol. 37, no. 12, pp. 1049–1092, 2014.
29. T. N. Friemel, "The digital divide has grown old: determinants of a digital divide among seniors," *New Media & Society*, vol. 18, no. 2, pp. 313–331, 2016.
30. R. Ayyagari and A. Crowell, "Risk and demographics' influence on security behavior intentions," *J South Assoc Inf Syst*, vol. 7, no. 1, 2020.
31. K. E. Pearce and R. E. Rice, "Digital divides from access to activities: comparing mobile and personal computer Internet users," *The Journal of Communication*, vol. 63, no. 4, pp. 721–744, 2013.
32. H.-S. Rhee, C. Kim, and Y. U. Ryu, "Self-efficacy in information security: its influence on end users' information security practice behavior," *Computers & Security*, vol. 28, no. 8, pp. 816–826, 2009.
33. P. Nintachan, Resilience and risk-taking behavior among Thai adolescents living in Bangkok, Thailand, Theses Diss, 2007.
34. M. Rutter, "Implications of resilience concepts for scientific understanding," *Annals of the New York Academy of Sciences*, vol. 1094, no. 1, pp. 1–12, 2006.
35. M. Harbach, A. De Luca, N. Malkin, and S. Egelman, "Keep on lockin' in the free world: A multi-national comparison of smartphone locking," pp. 4823–4827, Association for Computing Machinery.
36. C. Tømte and O. E. Hatlevik, "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," *Computers in Education*, vol. 57, no. 1, pp. 1416–1424, 2011.
37. A. Vance, P. B. Lowry, and D. Eggett, "Using accountability to reduce access policy violations in information systems," *Journal of Management Information Systems*, vol. 29, no. 4, pp. 263–290, 2013.
38. F. Alotaibi and A. Alshehri, "Gender differences in information security management," *J Comput Commun*, vol. 8, no. 3, pp. 53–60, 2020.
39. S. Egelman and E. Peer, Scaling the Security Wall Developing a Security Behavior Intentions Scale (SeBIS), 2015.
40. M. C. Howard, "Creation of a computer self-efficacy measure: analysis of internal consistency, psychometric properties, and validity," *Cyberpsychology, Behavior and Social Networking*, vol. 17, no. 10, pp. 677–681, 2014.

41. B. W. Smith, J. Dalen, K. Wiggins, E. Tooley, P. Christopher, and J. Bernard, "The brief resilience scale: assessing the ability to bounce back," *International Journal of Behavioral Medicine*, vol. 15, no. 3, pp. 194–200, 2008.
42. J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," *Journal of the Academy of Marketing Science*, vol. 43, no. 1, pp. 115–135, 2015.
43. D. George and P. Mallery, *SPSS for Windows Step by Step: A Simple Guide and Reference*, 17.0 Update - Darren George, Paul Mallery - Google Books, Allyn & Bacon, 2010.
44. M. Whitty, J. Doodson, S. Creese, and D. Hodges, "Individual differences in cyber security behaviors: an examination of who is sharing passwords," *Cyberpsychology, Behavior and Social Networking*, vol. 18, no. 1, pp. 3–7, 2015.
45. C. J. Hoofnagle, J. King, S. Li, and J. Turow, "How different are young adults from older adults when it comes to information privacy attitudes and policies?" *Social Science Research Network*, vol. 4, pp. 10–10, 2010.
46. A. Hunsaker, M. H. Nguyen, J. Fuchs, G. Karaoglu, T. Djukaric, and E. Hargittai, "Unsung helpers: older adults as a source of digital media support for their peers," *The Communication Review*, vol. 23, no. 4, pp. 309–330, 2020.
47. M. Jiang, H. S. Tsai, S. R. Cotten, N. J. Rifon, R. LaRose, and S. Alhabash, "Generational differences in online safety perceptions, knowledge, and practices," *Educational Gerontology*, vol. 42, no. 9, pp. 621–634, 2016.
48. L. Mecke, S. Prange, D. Buschek, M. Khamis, M. Hassib, and F. Alt, "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.
49. N. Nthala and I. Flechais, *Informal Support Networks: An Investigation into Home Data Security Practices*, 2018.
50. T. L. Mitzner, J. B. Boron, C. B. Fausset et al., "Older adults talk technology: technology usage and attitudes," *Computers in Human Behavior*, vol. 26, no. 6, pp. 1710–1721, 2010.
51. H. Ray, F. Wolf, R. Kuber, and A. J. Aviv, "Why older adults (don't) use password managers," *Proceedings of the 30th USENIX Security Symposium*, 2021.
52. S. Furnell and K.-L. Thomson, "Recognising and addressing 'security fatigue'," *Comput Fraud Secur*, vol. 2009, no. 11, pp. 7–11, 2009.
53. S. Livingstone and E. Helsper, "Balancing opportunities and risks in teenagers' use of the Internet: the role of online skills and internet self-efficacy," *New Media & Society*, vol. 12, no. 2, pp. 309–329, 2010.
54. B. Stanton, M. F. Theofanos, S. S. Prettyman, and S. Furman, "Security fatigue," *IT Prof*, vol. 18, no. 5, pp. 26–32, 2016.
55. J. E. Brodsky, A. K. Lodhi, K. L. Powers, F. C. Blumberg, and P. J. Brooks, "'It's just everywhere now': middle-school and college students' mental models of the Internet," *Hum Behav Emerg Technol*, vol. 3, no. 4, pp. 495–511, 2021.
56. T. Daengsi, P. Pornpongtechavanich, and P. Wuttidittachotti, "Cybersecurity awareness enhancement: a study of the effects of age and gender of Thai employees associated with phishing attacks," *Education and Information Technologies*, vol. 27, no. 4, pp. 4729–4752, 2022.
57. R. Pak, E. Rovira, A. C. McLaughlin, and N. Baldwin, "Does the domain of technology impact user trust? Investigating trust in automation across different consumer-oriented domains in young adults, military, and older adults," *Theoretical Issues in Ergonomics Science*, vol. 18, no. 3, pp. 199–220, 2017.
58. K. A. Hoff and M. Bashir, "Trust in automation," *Human Factors*, vol. 57, no. 3, pp. 407–434, 2015.
59. X. Hu and M. Bashir, "Toward designing trustworthy autonomous systems: probing the role of humans' ethical perspectives," in *2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pp. 974–979, Hangzhou, China, 2022.
60. H. Y. Huang and M. N. Bashir, "Users' trust in automation," *Adv Hum Factors Robots Unmanned Syst - Proc AHFE 2017 Int Conf Hum Factors Robots Unmanned Syst 2017*, pp. 282–289, 2018.
61. E. Rovira, A. C. McLaughlin, R. Pak, and L. High, "Looking for age differences in self-driving vehicles: examining the effects of automation reliability, driving risk, and physical impairment on trust," *Frontiers in Psychology*, vol. 10, p. 800, 2019.

62. S. E. McBride, W. A. Rogers, and A. D. Fisk, "Understanding the effect of workload on automation use for younger and older adults," *Human Factors*, vol. 53, no. 6, pp. 672–686, 2011.
63. E. Hargittai and K. Dobransky, "Old dogs, new clicks: digital inequality in skills and uses among older adults," *Canadian Journal of Communication*, vol. 42, 2017.
64. E. Hargittai and S. Shafer, "Differences in actual and perceived online skills: the role of gender," *Social Science Quarterly*, vol. 87, no. 2, pp. 432–448, 2006.
65. F. B. Fatokun, S. Hamid, A. Norman, and J. O. Fatokun, "The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities," *Journal of Physics Conference Series*, vol. 1339, no. 1, article 012098, 2019.
66. O. E. Hatlevik, I. Throndsen, M. Loi, and G. B. Gudmundsdottir, "Students' ICT self-efficacy and computer and information literacy: determinants and relationships," *Computers in Education*, vol. 118, pp. 107–119, 2018.
67. B. Rahimi, M. Baetz, R. Bowen, and L. Balbuena, "Resilience, stress, and coping among Canadian medical students," *Can Med Educ J*, vol. 5, no. 1, pp. e5–12, 2014.
68. J. R. Overholt and A. Ewert, "Gender matters: exploring the process of developing resilience through outdoor adventure," *The Journal of Experimental Education*, vol. 38, pp. 41–55, 2015.
69. Sherazi, Hafiz Husnain Raza, Sharif Arif, Muhammad Sohail Munir, Mubashir Ali, Bilal Hassan, and Yusra Siddiqi. "Utilizing Internet of Things for Automating Food Security and Savvy Agriculture: A Review." In 2023 28th International Conference on Automation and Computing (ICAC), pp. 1-6. IEEE, 2023.

Received: 24 Jan 2025, **Revised:** 31 May 2025,

Accepted: 21 Nov 2025, **Available online:** 23 Nov 2025.



© 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

Disclaimer/Publisher's Note: The perspectives, opinions, and data shared in all publications are the sole responsibility of the individual authors and contributors, and do not necessarily reflect the views of Sciences Force or the editorial team. Sciences Force and the editorial team disclaim any liability for potential harm to individuals or property resulting from the ideas, methods, instructions, or products referenced in the content.