IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/47ISM/2026/4721826/
Vol. 2026 (7), Article ID 4721826

Gen Z vs. Older Adults in Cybersecurity Self-Efficacy: A Quantitative Survey Study*

Grzegorz STRUPCZEWSKI, Magdalena ADAMCZYK-KOWALCZUK and Michał WŁODARCZYK

Krakow University of Economics, Krakow, Poland

Correspondence should be addressed to: Magdalena ADAMCZYK-KOWALCZUK, adamczym@uek.krakow.pl

*Presented at the 47th IBIMA International Conference, 29-30 June 2026, Madrid, Spain

Abstract

As cybercrime costs are projected to reach $10.5 trillion annually by 2025 and the human factor accounts for 68% of data breaches, understanding variation in cybersecurity self-efficacy (CSE) across demographic groups has become a pressing research priority. Despite a growing body of CSE literature, systematic reviews have identified a near-complete absence of intergenerational comparative frameworks - a significant gap in both theory and practice. This study examines differences in CSE and cyber risk perception between Generation Z (born 1997–2012) and older adults (aged 60+), with gender, income, and digital financial service usage as boundary conditions. A quantitative, cross-sectional survey was conducted in Poland (January 2026) with 307 respondents. Validated Likert-scale instruments measured CSE, risk perception, and attitudes toward digital financial services; hypotheses were tested using Mann-Whitney U tests and Spearman's rank correlation. Findings confirm that Generation Z exhibits significantly higher CSE than older adults, with the largest gaps concentrated in technically complex behaviors such as VPN use, multi-factor authentication configuration, and password manager utilization. Concurrently, older adults report substantially higher cyber risk perception despite lower self-efficacy, constituting a fear-capability asymmetry consistent with Protection Motivation Theory's coping deficit mechanism. The income-CSE association was significant only within the older adult subsample. Gender differences in CSE were cohort-specific, with the standard male advantage reversing direction among older adults. These findings highlight the necessity of differentiated, generationally tailored cybersecurity education and policy interventions.

Keywords: cybersecurity self-efficacy, Generation Z, older adults, intergenerational differences, digital financial services.

Introduction

With technology woven into everyday activities, users face evolving risks as technology users. Cybersecurity Ventures forecasts that the worldwide financial cost of cybercrime could reach $10.5 trillion annually by 2025, exceeding the GDP of most countries (Morgan, 2023). The leading vulnerability exploited by cybercriminals, the human element, remains the weakest link in cybersecurity. The 2024 Verizon Data Breach Investigations Report highlights that human error, misuse, or social engineering play a role in 68% of data breaches (Verizon, 2024). Trends and analyses point to a growing need to understand not only available security measures but also whether and how users engage with them.

At the same time, the demographics of digital users are shifting significantly. The UN estimates that one in six people worldwide will be aged 60 and above by 2030, an increase of 34% from today, to 1.4 billion individuals (World Health Organization, 2022). As this population grows rapidly, older adults are required to navigate increasingly digital spaces to fulfill daily activities such as banking, healthcare access and socializing. They

Cite this Article as: Grzegorz STRUPCZEWSKI, Magdalena ADAMCZYK-KOWALCZUK and Michał WŁODARCZYK Vol. 2026 (7) " Gen Z vs. Older Adults in Cybersecurity Self-Efficacy: A Quantitative Survey Study " Communications of International Proceedings, Vol. 2026 (7), Article ID 4721826, https://doi.org/10.5171/2026.4721826

generally lack extensive digital upbringing with networked technologies. In contrast, Generation Z (born roughly between 1997-2012) grew up entirely in networked digital environments, and Prensky (2001) coined the term "digital natives" for this demographic.

An individual's sense of cybersecurity self-efficacy (CSE), defined as one's perceived ability to perform protective cybersecurity behaviors, has been identified as an appropriate theory to explore such intergenerational differences. Rooted in Social Cognitive Theory (Bandura, 1977, 1986), self-efficacy beliefs are viewed as among the most important predictors of behavioral performance in any domain. Studies have shown CSE to be a predictor of defensive actions such as the secure creation and storage of strong passwords, effective use of two-factor authentication, phishing resistance and avoidance of malware (Nicholson et al., 2020; Vance et al., 2012). In a review of 174 studies regarding self-efficacy and security behavior, Raber et al. (2024) found few studies that focused specifically on intergenerational comparisons of self-efficacy or behavior, therefore indicating a research gap.

The aim of this study is to examine differences in cybersecurity self-efficacy between Generation Z and older adults (60+), and to explore the boundary conditions - including gender, income, and attitudes to digital finance - under which these differences operate. The study addresses the following research questions:

- **RQ1:** Do Generation Z and older adults differ in cybersecurity self-efficacy?
- **RQ2:** Do Generation Z and older adults differ in risk perception related to digital threats?
- **RQ3:** Is cybersecurity self-efficacy associated with gender, and does this association differ by cohort?
- **RQ4:** Is cybersecurity self-efficacy associated with socioeconomic indicators (household income, savings)?

Literature Review and Theoretical Background

Cybersecurity Self-Efficacy

Self-efficacy, introduced by Bandura (1977) as part of Social Learning Theory and subsequently developed within Social Cognitive Theory (Bandura, 1986), refers to "people's beliefs about their capabilities to produce designated levels of performance that exercise influence over events that affect their lives" (Bandura, 1997, p. 3). The construct is domain-specific: efficacy beliefs in one area do not generalize automatically to another. In the context of information technology, Compeau and Higgins (1995) operationalized computer self-efficacy as "a judgment of one's capability to use a computer," demonstrating its predictive power over computer use intentions and outcomes.

Cybersecurity self-efficacy extends this framework to the domain of security-protective behaviors. Individuals who believe they can successfully configure privacy settings, recognize phishing attempts, or manage authentication credentials are more likely to engage in these behaviors and persist in the face of obstacles (Anderson & Agarwal, 2010). Raber et al. (2024), in their systematic review of 174 empirical studies published between 2010 and 2021, found that CSE is consistently positively associated with a broad range of protective security behaviors - including password strength, software updating, and avoidance of risky online practices - across diverse populations. Critically, the authors noted a near-complete absence of intergenerational comparative frameworks in this literature, identifying this as a primary gap.

Social Cognitive Theory

Social Cognitive Theory (SCT) posits that behavior is determined by a triadic interaction among personal factors (including cognitive, affective, and biological events), behavioral patterns, and environmental influences. Within this framework, self-efficacy operates as a cognitive mechanism that regulates goal-setting, effort allocation, persistence, and resilience in the face of adversity (Bandura, 1986). Critically for the present study, SCT predicts that high self-efficacy leads to approach behavior (in this case, the adoption of cybersecurity measures), while low self-efficacy tends to produce avoidance. This prediction is particularly relevant for older adults, for whom low CSE may translate directly into non-engagement with digital protective tools (Morrison et al., 2020).

Protection Motivation Theory

Rogers' (1975, 1983) Protection Motivation Theory (PMT) provides a complementary framework, focusing on how individuals appraise threats and their own capacity to respond. PMT posits two cognitive appraisal processes: threat appraisal (comprising perceived severity and perceived vulnerability) and coping appraisal (comprising

response efficacy - belief that the protective behavior is effective - and self-efficacy - belief that one can perform it). Research has consistently shown that the relative weighting of these appraisals differs across populations: for younger users, coping appraisal (particularly self-efficacy) is the dominant driver of protective behavior, while for older adults, threat appraisal tends to predominate (Vance et al., 2012). This asymmetry has important implications: it suggests that fear-based messaging may be more effective for older cohorts, while competence-building interventions are more effective for younger ones.

Technology Acceptance Model

Davis's (1989) Technology Acceptance Model (TAM) proposes that perceived usefulness and perceived ease of use are the primary determinants of technology adoption. Subsequent extensions of TAM have incorporated self-efficacy as an antecedent of perceived ease of use (Compeau & Higgins, 1995), establishing a theoretical pathway from CSE to technology adoption. This pathway is especially relevant for digital financial services: individuals who believe themselves capable of using security features (e.g., two-factor authentication for mobile banking) are more likely to perceive the technology as usable, and thus to adopt it.

Generational Differences in Digital Competence and Cybersecurity

Generation Z (born 1997-2012) is widely described as "digital natives" due to lifelong exposure to networked technologies (Prensky, 2001; Twenge, 2017). While this fosters fluency in digital tools, it does not ensure cybersecurity competence. Goliath et al. (2024), studying university students (N = 266), found that younger undergraduates - largely Generation Z - showed weaknesses in password management and email security despite general proficiency. This reflects the "overconfidence paradox", i.e. high self-reported competence paired with objective skill deficits. Similarly, De Bruin (2024) observed that younger cohorts report higher competence without corresponding security behaviors, indicating inflated CSE relative to actual capability.

Older adults (60+) face distinct cybersecurity challenges. Vrhovec et al. (2024), analyzing 782 UK mobile users, found modest competence weakly linked to device proficiency ($R^2 = 0.082$), highlighting the role of psychological factors such as self-efficacy. Morrison et al. (2020) showed that retirement disrupts support structures (e.g., workplace IT, routines), increasing vulnerability. Pacheco (2024) further confirmed persistent low confidence and negative attitudes toward digital technologies in this group, despite rising digital engagement.

Research hypotheses

Based on the theoretical framework and prior literature, the following hypotheses are advanced:

H1: Generation Z exhibits significantly higher cybersecurity self-efficacy than older adults.
Rationale: Consistent with SCT (Bandura, 1986) and evidence from Goliath et al. (2024), digital exposure from childhood should produce higher domain-specific self-efficacy in younger cohorts.

H2: Cybersecurity self-efficacy is associated with gender, with this association potentially differing across cohorts.
Rationale: Gender differences in computer self-efficacy are well documented (Compeau & Higgins, 1995); however, the direction of the effect may vary by generation.

H3: Older adults exhibit significantly higher risk perception despite lower self-efficacy than Generation Z.
Rationale: PMT predicts that for older adults, threat appraisal dominates coping appraisal (Rogers, 1983; Vance et al., 2012), producing a profile of high fear alongside low perceived capability.

H4a: Higher household income is positively associated with cybersecurity self-efficacy.
H4b: Higher savings relative to income are positively associated with cybersecurity self-efficacy.
Rationale: Socioeconomic resources facilitate access to technology training, updated devices, and security software, thereby supporting higher CSE.

Methodology

Research design

This study employs quantitative, cross-sectional survey design. The conceptual model positions generational cohort (Generation Z vs. older adults) as the primary independent variable, with cybersecurity self-efficacy as the

principal dependent variable. Data were collected using structured Likert-scale questionnaires covering four domains: (1) cybersecurity self-efficacy, (2) risk perception, (3) attitudes toward digital financial services, and (4) demographic characteristics. Non-parametric statistical tests (Mann-Whitney U, Spearman's rank correlation) were selected a priori given the ordinal nature of the measurement scales (Field, 2018).
The survey was conducted in an online form on January 2026 in Poland.

Sample demographics

The study sample comprises 307 respondents collected via purposive sampling. Purposive sampling was employed to ensure sufficient representation of both target groups. Generational boundaries follow established cohort definitions (Prensky, 2001; Twenge, 2017), with Generation Z characterized by digital nativity and older adults by pre-digital socialization histories (Howe & Strauss, 2000).

The sample is predominantly female (71.3%, n = 219), with male respondents accounting for 28.7% (n = 88). Ages ranged from 17 to 83 years (overall M = 34.8 years), reflecting the deliberate inclusion of two generationally distinct cohorts: young adults aged 17–26 (Generation Z) and older adults aged 60–83. Gen Z represents 71,0% of the sample (n=218) and older adults 29,0% (n=89).

In terms of education, the majority held secondary education (64.2%, n = 197), followed by higher education (33.9%, n = 104). Education profiles diverge sharply by cohort: 64.0% of elderly hold higher education vs. only 21.6% of Gen Z (75.7% of whom have secondary education, consistent with their student status).

Household monthly net income was distributed across seven brackets. The most frequently reported range was 3,001-5,000 PLN (21.5%), followed by 5,001-7,000 PLN (17.9%) and the above-15,000 PLN bracket (14.7%). Elderly respondents cluster in lower income brackets (37.1% at 3,001-5,000 PLN), while Gen Z is more evenly distributed with 17.9% earning above 15,000 PLN - reflecting household income rather than personal earnings. The savings variable, expressed as a multiple of monthly household income, revealed that the largest share of respondents (40.7%) held savings below one monthly income equivalent, while 16.9% reported savings exceeding five monthly incomes.

Digital literacy was measured by count variable (0-6) indicating the number of currently used digital financial services (e.g., mobile banking, contactless payments, investment platforms). Digital literacy was moderate to high across the sample. The dominant response for this question was use of three types of online financial services (43.0%, n = 132), with 16.0% using four types. Only 2.9% (n = 9) reported using no digital financial services at all, indicating that most respondents had at least some experience with online financial tools. Digital literacy is markedly lower among the elderly: 39.3% use 0-1 services vs. only 0.9% of Gen Z; 49.1% of Gen Z use 3 types compared to 28.1% of elderly respondents.
The demographic composition of the sample is summarized in Table 1.

Table 1: Sample demographic profile

Variable	Category	n	%
Q1. Cohort	Gen Z	218	71,0%
	Elderly	89	29,0%
Q2. Gender	Female	219	71,3%
	Male	88	28,7%
Q4. Education	Primary	2	0,7%
	Secondary	197	64,2%
	Vocational	4	1,3%
	Higher	104	33,9%
Q5. Household monthly net income (PLN)	< 3,000	32	10,4%
	3,001–5,000	66	21,5%
	5,001–7,000	55	17,9%
	7,001–9,000	44	14,3%
	9,001–11,000	37	12,1%

	11,001–15,000	28	9,1%
	>15,000	45	14,7%
Q6. Savings relative to monthly income (× income)	Less than 1×	125	40,7%
	1×	35	11,4%
	2×	31	10,1%
	3×	36	11,7%
	4×	17	5,5%
	5×	11	3,6%
	More than 5×	52	16,9%
Q7. Number of types of online financial services used	0 types	9	2,9%
	1 type	28	9,1%
	2 types	55	17,9%
	3 types	132	43,0%
	4 types	49	16,0%
	5 types	23	7,5%
	6+ types	11	3,6%

Source: own dataset and calculations.

Operationalization of Variables

Attitude toward digital financial services (Q8). A 6-item scale assessing positive appraisal of digital banking and payment tools. Items were rated on a 5-point Likert scale (1=*strongly disagree*, 5=*strongly agree*). Scale reliability was acceptable (Cronbach's α = 0.802) (Cronbach, 1951).

Cybersecurity Self-Efficacy (Q9). Measured using a 10-item scale assessing confidence in specific protective behaviors (e.g., creating strong passwords, configuring privacy settings, setting up two-factor authentication, using a VPN, recognizing phishing). Items were rated on a 5-point Likert scale (1=*not at all confident*, 5=*fully confident*). Scale reliability was excellent (Cronbach's α = 0.935).

Risk perception (Q10). Measured using an 8-item scale assessing perceived severity of and vulnerability to digital threats (e.g., unauthorized access to accounts, identity theft, financial fraud). Items were rated on a 5-point Likert scale (1=*strongly disagree*, 5=*strongly agree*). Scale reliability was high (Cronbach's α = 0.895).

Table 2 shows details of the survey items described above.

Table 2: Key survey items (Q8-Q10)

Item Code	Survey Item
Q8. ***To what extent do you agree with the following statements?***	
Q8_1	I feel that I am in control of my own money
Q8_2	I prefer handling important banking matters at a branch
Q8_3	Digital financial services are quicker and more convenient
Q8_4	I have difficulty understanding the language or complexity of digital services
Q8_5	Digital services give me independence
Q8_6	I trust cash more than digital payments
Q9. ***To what extent do you agree with the following statements?***	
Q9_1	I can recognize phishing attempts
Q9_2	I can create and manage strong passwords
Q9_3	I can protect my devices from malware
Q9_4	I regularly update systems and applications
Q9_5	I can configure privacy and security settings
Q9_6	I can set up and use multi-factor authentication (MFA)

Q9_7	I know what to do in case of a cyberattack
Q9_8	I can avoid risky online behaviors
Q9_9	I have sufficient knowledge to use financial services safely
Q9_10	I can use a password manager effectively
Q10. ***To what extent do you agree with the following statements?***	
Q10_1	I am afraid of losing access to my funds due to system failure
Q10_2	I doubt the reliability of financial applications
Q10_3	I am concerned about data interception during transactions
Q10_4	I am concerned about how institutions process my personal data
Q10_5	I fear theft from my bank account
Q10_6	I believe I am at risk of becoming a victim of fraud
Q10_7	I feel uneasy using online banking services
Q10_8	I feel social pressure to use digital financial tools

Source: own work.

Results

The six Q8 items probing attitudes toward digital financial services revealed a nuanced pattern of cohort differences, with elderly respondents scoring consistently higher on items reflecting caution and traditional preferences (see Fig. 1). The largest and most significant gap emerged on branch preference: elderly respondents showed a substantially stronger inclination to handle important banking matters in person (Mean=4.18 vs. Gen_Z Mean=3.15, p<.001). Similarly, elderly respondents reported a stronger subjective sense of financial control (Mean=4.28 vs. Gen_Z Mean=3.89, p<.001) and greater difficulty with the language and complexity of digital services (Mean=2.87 vs. Gen_Z Mean=2.14, p<.001).

Two items yielded no statistically significant cohort differences: perceived speed and convenience of digital services (Gen_Z Mean=4.39 vs. elderly Mean=4.18, p>.05) and trust in cash over digital payments (Gen_Z Mean=2.69 vs. elderly Mean=2.84, p>.05). This indicates that both cohorts broadly recognise the practical advantages of digital finance and neither group exhibits a markedly stronger preference for cash; divergence is concentrated on complexity perceptions and channel preferences rather than on utility judgments. The sense of independence gained from digital services also did not differ significantly between groups (diff=-0.15, p=.077), suggesting that the motivational appeal of digital autonomy is similarly distributed across generations.

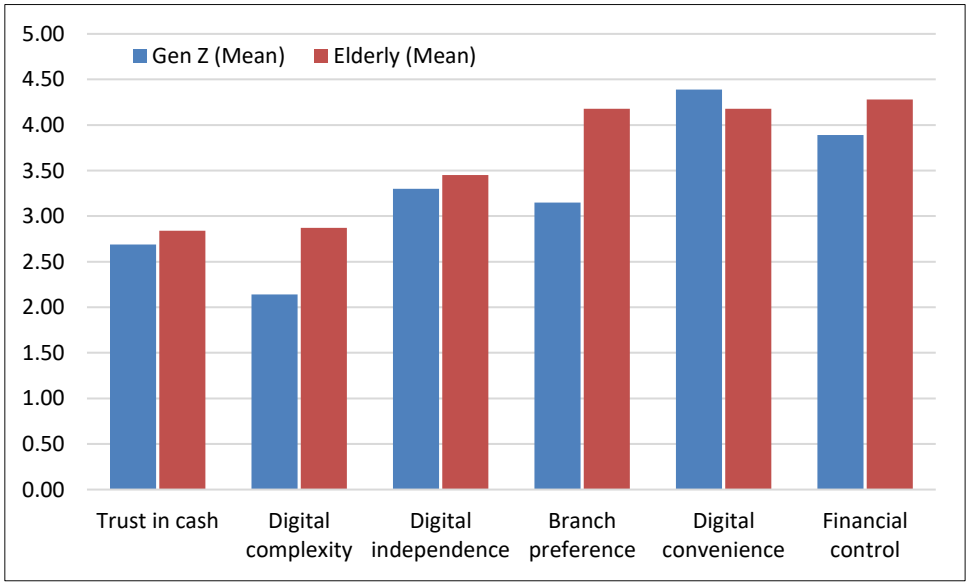

Fig. 1. Attitude toward digital financial services (Q8) by cohort – mean score (1-5)

Source: own work.

The ten individual CSE items (Q9) revealed a consistent pattern of superiority in Generation Z, with the largest gaps on technically complex tasks: password manager use (Gen_Z Mean=4.03 vs. elderly Mean=2.20), MFA setup (diff=1.32), and configuring privacy settings (diff=1.27). The only non-significant inter-group difference

was observed on basic password creation (p>.05), indicating a preserved baseline skill in the older cohort (see Fig. 2). The results suggest statistically robust gap in cybersecurity self-efficacy between the two cohorts. The composite CSE score (mean of all Q9 items) was 3.81 for Gen Z versus 2.84 for Elderly (diff=0.98), with the difference statistically significant at p<.001 (Mann-Whitney U=14,297).

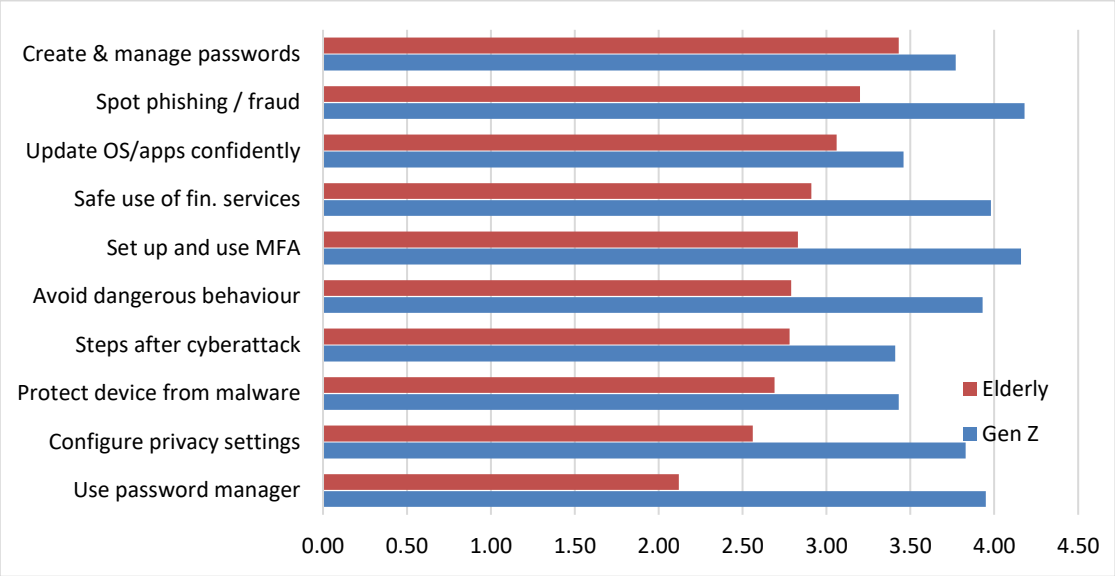

Fig 2. Cybersecurity Self-Efficacy (Q9) by cohort – mean score (1-5)

Source: own work.

An internal hierarchy of CSE items within each cohort reveals a theoretically important distinction between **reactive competencies** (recognizing a threat after encountering it) and **proactive/preventive competencies** (independently configuring security before threat exposure). For Gen Z, the lowest-scoring CSE items were cyberattack response (Mean=3.41) and malware protection (Mean=3.43) - both reactive/preventive. Phishing detection (reactive, threat-proximate) scored highest (Mean=4.18), suggesting that Gen Z self-efficacy is strongest in direct threat contexts and weakest in background maintenance behaviors. For Elderly respondents, password creation (Mean=3.43) was the strongest CSE item - a relatively low-complexity task requiring no technical configuration, while password manager (Mean=2.12) and privacy settings (Mean=2.56) were weakest. This pattern suggests that elderly CSE is partially preserved for simple, familiar tasks but collapses for multi-step or interface-dependent operations.

The inverse of the CSE pattern emerges in **cyber risk perception** (Q10). Elderly respondents report systematically *higher* levels of worry, concern, and threat appraisal across all eight items. The composite risk score was 2.53 for Gen Z versus 3.37 for Elderly (diff=-0.85, p<.001).

Items measuring general unease with digital financial infrastructure showed the largest generational gaps, indicating technology skepticism of the elderly.

Online banking unease: Gen_Z Mean=2.00 vs. Elderly Mean=3.00 (p<.001). The response distribution reveals structural divergence: 72% of Gen Z respondents rated banking unease as 1 or 2 ("disagree"), while 37% of elderly respondents rated it 4 or 5 ("agree").

Social pressure to use digital finance despite discomfort: Gen_Z Mean=1.62 vs. Elderly Mean=2.82 (p<.001). This is the highest-gap item in the entire Q10 battery. Among Gen Z, 61% selected "1-strongly disagree" (no felt social pressure), compared to only 26% of elderly. A substantial 25% of elderly respondents selected "5-strongly agree", reporting active discomfort coupled with external pressure to digitize (see Fig. 3).

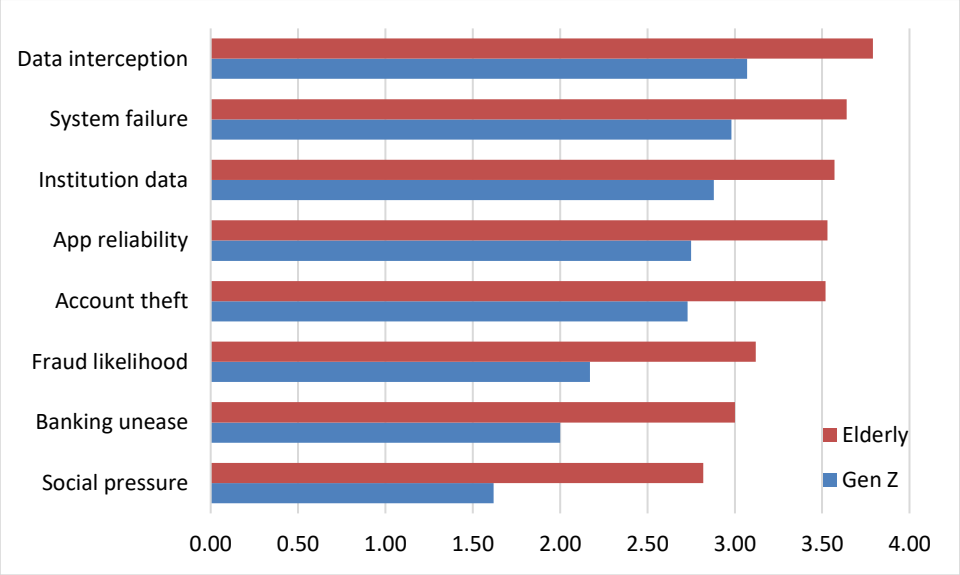

Fig. 3. Risk perception (Q10) by cohort – mean score (1-5)

Source: own work.

Further Q10 items point to financial threat appraisal.

Perceived likelihood of falling victim to fraud: Gen_Z Mean=2.17 vs. Elderly Mean=3.12 ($p<.001$). Among Gen Z, 68% rated this probability as 1 or 2 (low), while 42% of elderly rated it 4 or 5 (high). This constitutes a calibration inversion: elderly respondents with *lower* CSE paradoxically perceive *higher* personal fraud risk - consistent with the Protection Motivation Theory mechanism wherein threat appraisal compensates for reduced coping appraisal.

Account theft worry: Gen_Z Mean=2.73 vs. Elderly Mean=3.52 ($p<.001$). The distribution among elderly adults is right-skewed with 50% selecting ratings 4 or 5, indicating prevalent concrete financial threat appraisal.

Finally, two items measure concern about how organizations handle personal data.

Data interception by third parties: Gen_Z Mean=3.07 vs. Elderly Mean=3.79 ($p<.001$).

Financial institutions' data processing: Gen_Z Mean=2.88 vs. Elderly Mean=3.57 ($p<.001$).

Both items are among the higher-scoring risk items for Gen Z as well, suggesting that institutional data concern is more universally held than personal operational risk. This pattern aligns with the privacy cynicism documented in the qualitative literature on younger digital users.

Hypothesis testing

H1 Confirmed. A Mann-Whitney U test confirmed that Generation Z exhibits significantly higher cybersecurity self-efficacy than older adults (Spearman's $r_s=.372$, $p<.001$). This effect size is classified as moderate-to-large, indicating a meaningful and practically significant generational gap.

H2 Partially confirmed. A statistically significant association between gender and CSE was found across the full sample ($r_s=.289$, $p<.001$), with male respondents scoring higher overall. However, cohort-specific analysis revealed a critical moderating interaction: in Generation Z, males scored substantially higher than females (diff=0.62 scale points), while in the older adult cohort, the gender gap was reversed in direction, with female seniors scoring slightly higher than males - though this reversal was not statistically significant at $p<.05$. This pattern suggests that the standard gender gap in CSE is a cohort-specific, not universal, phenomenon.

H3 Confirmed. Older adults scored significantly higher on risk perception ($r_s=.386$, $p<.001$) despite lower self-efficacy. This inversion constitutes the core empirical finding of the study: older adults simultaneously perceive higher threats and feel less capable of responding to them - a profile consistent with PMT's prediction of a coping deficit under high threat appraisal (Rogers, 1983). The item with the largest discrepancy was "social pressure to

use digital financial services despite discomfort" (elderly Mean=2.82 vs. Gen_Z Mean=1.62), where 25% of older adults selected "5-strongly agree" indicating coerced digital adoption.

H4a Partially confirmed. The association between household income and CSE was significant across the full sample (r_s=.197, p<.01). However, cohort stratification revealed that this effect was confined entirely to the older adult subsample (r_s=.283, p<.001), while in Generation Z the association was non-significant (r_s=.093, p=.24). This asymmetry suggests that income serves as a resource constraint for CSE development specifically in older adults - likely via access to devices, internet connections, and informal technical support, but not in Generation Z, where digital access is near-universal.

H4b Not confirmed. Savings relative to income showed no significant association with CSE in either cohort (overall r_s=-.010, p=.86), failing to support H4b. This null finding suggests that accumulated financial wealth, in the absence of active income, does not translate into enhanced cybersecurity self-efficacy.

Discussion

The finding that Generation Z scores significantly higher on CSE replicates and extends prior evidence (Goliath et al., 2024; de Bruin, 2024). However, the large gap on technically complex items (VPN use, password manager, MFA configuration) alongside the absence of a significant gap on basic password creation suggests that Gen Z's advantage is concentrated in intermediate-to-advanced behaviors, not in foundational ones. This is consistent with the "overconfidence paradox", i.e. while Gen Z holds higher efficacy beliefs, these beliefs may outpace actual capability in some domains, creating calibration errors with security consequences (Raber et al., 2024).

The simultaneous presence of high-risk perception and low self-efficacy in older adults constitutes what may be termed a *coping deficit profile* under PMT (Rogers, 1983). Individuals in this profile are aware of threats but feel incapable of responding to them - a psychological state associated with defensive avoidance rather than protective engagement (Vance et al., 2012). Morrison et al.'s (2020) qualitative findings illuminate the structural origins of this deficit: the loss of workplace IT support, routines, and sociotechnical networks upon retirement creates an environment of technological vulnerability that erodes self-efficacy over time. The particularly high endorsement by older adults of the "coerced digitalization" item (25% strongly agreeing that social pressure forces them to use uncomfortable digital tools) signals an ethical dimension: digital inclusion policies must address not only access but also the quality and autonomy of that inclusion (Pacheco, 2024).

The reversal of the gender gap in CSE within the older adult cohort is a theoretically important finding that has received no prior attention in the literature. One interpretive framework draws on social role theory: older female adults, having historically managed household finances and administrative tasks (including utility bill payments, correspondence, and later online banking), may have accumulated informal competencies that partially offset lower formal technical training. This explanation is speculative and warrants dedicated investigation.

The finding that income predicts CSE in older adults but not in Generation Z is consistent with a resource-access model: older adults with limited income may lack the newest devices, broadband connectivity, and informal technical assistance networks (Morrison et al., 2020; Vrhovec et al., 2024), all of which support CSE development. For Generation Z, near-universal smartphone ownership and social peer networks largely neutralize income as a barrier to digital access, explaining the null effect.

Conclusion

This study demonstrates that cybersecurity self-efficacy differs substantially, and consequentially, across generational lines. Generation Z enters the digital environment with higher CSE on nine of ten measured behaviors, but this advantage is accompanied by potential overconfidence, particularly in intermediate and advanced security tasks. Older adults, by contrast, face a compounding challenge: lower CSE alongside higher perceived threat, creating a fear-capability asymmetry that drives defensive avoidance rather than protective engagement. The income-CSE link in older adults, the cohort-specific reversal of the gender gap, and the disproportionate role of CSE as a gateway to digital participation for the elderly collectively point toward the need for differentiated, cohort-specific cybersecurity education and policy.

From a theoretical perspective, these findings enrich the application of PMT and Social Cognitive Theory to the cybersecurity domain by demonstrating that the relative weighting of coping vs. threat appraisal, and the social antecedents of self-efficacy, are not constants but are modulated by generational socialization histories.

Practically, they support a shift from generic cybersecurity awareness campaigns toward targeted, evidence-based interventions calibrated to the specific vulnerability profiles of each generational group.

This study is subject to three principal limitations. Purposive sampling from a single national context (Poland) limits population representativeness and cross-cultural generalizability. Self-reported measures introduce the risk of social desirability bias and overconfidence inflation, particularly for CSE items among Gen Z respondents (Raber et al., 2024). Finally, the cross-sectional design precludes causal inference regarding whether observed cohort differences reflect developmental trajectories, generational socialization, or period effects such as COVID-19-accelerated digitalization.

Acknowledgement

The paper presents the result of Project no 030/EFZ/2023/POT financed from the subsidy granted to the Krakow University of Economics.

References

- Anderson, C.L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643. https://doi.org/10.2307/25750694
- Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191-215. https://doi.org/10.1037/0033-295X.84.2.191
- Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall.
- Bandura, A. (1997). *Self-efficacy: The exercise of control*. W.H. Freeman.
- Compeau, D.R., & Higgins, C.A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*(2), 189-211. https://doi.org/10.2307/249688
- Cronbach, L.J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297-334. https://doi.org/10.1007/BF02310555
- Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340. https://doi.org/10.2307/249008
- de Bruin, M. (2024). *Individual and contextual variables of cyber security behaviour: An empirical analysis of national culture, industry, organisation, and individual variables of (in)secure human behaviour*. arXiv preprint arXiv:2405.16215.
- Field, A. (2018). *Discovering statistics using IBM SPSS statistics* (5th ed.). SAGE Publications.
- Goliath, S., Tsibolane, P., & Snyman, D. (2024). Exploring the cybersecurity-resilience gap: An analysis of student attitudes and behaviors in higher education. arXiv preprint arXiv:2411.03219.
- Howe, N., & Strauss, W. (2000). *Millennials rising: The next great generation*. Vintage Books.
- IBM. (2024). *Cost of data breach report 2024*. IBM Corporation. https://www.ibm.com/reports/data-breach
- Morgan, S. (2023). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybersecurity Ventures. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
- 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*, 623. https://doi.org/10.3389/fpsyg.2020.00623
- Nicholson, J., Coventry, L., & Briggs, P. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Frontiers in Psychology, 11*, 546546. https://doi.org/10.3389/fpsyg.2020.546546
- Pacheco, E. (2024). Older adults' safety and security online: A post-pandemic exploration of attitudes and behaviors. *Journal of Digital Media & Interaction, 7*(17). https://doi.org/10.34624/jdmi.v7i17.37825
- Prensky, M. (2001). Digital natives, digital immigrants. *On the Horizon, 9*(5), 1-6. https://doi.org/10.1108/10748120110424816
- Raber, F., Gerber, N., Knauer, S., & Volkamer, M. (2024). Self-efficacy and security behavior: Results from a systematic review of research methods. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (Article 967). ACM. https://doi.org/10.1145/3613904.3642432
- Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

- Rogers, R.W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J.T. Cacioppo & R.E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153-176). Guilford Press.
- Twenge, J.M. (2017). *iGen: Why today's super-connected kids are growing up less rebellious, more tolerant, less happy-and completely unprepared for adulthood*. Atria Books.
- Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(3-4), 190-198. https://doi.org/10.1016/j.im.2012.04.002
- Verizon. (2024). *2024 data breach investigations report*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/
- Vrhovec, S., Bernik, I., Fujs, D., & Vavpotič, D. (2024). *Cybersecurity competence of older adult users of mobile devices*. arXiv preprint arXiv:2403.02459.
- World Health Organization. (2022). *Ageing and health*. WHO. https://www.who.int/news-room/fact-sheets/detail/ageing-and-health