I.J. Wireless and Microwave Technologies, 2026, 3, 88-97
Published Online on June 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2026.03.06

The Confidence-Competence Gap in Senior Cybersecurity: An Exploratory Survey and Conceptual Framework

Kartika Purwandari*
Computer Science Department, School of Computer Science, Bina Nusantara University, Jakarta 11480, Indonesia
E-mail: kartika.purwandari@binus.ac.id
ORCID iD: https://orcid.org/0000-0002-0550-8861
*Corresponding Author

Join W.C. Sigalingging
The Agency for Meteorology, Climatology, and Geophysics, Centre for Database, Jakarta 10610, Indonesia
E-mail: join.wan.chanlyn@bmkg.go.id
ORCID iD: https://orcid.org/0000-0002-5625-6588

Received: 01 March, 2026; Revised: 01 April, 2026; Accepted: 23 April, 2026; Published: 08 June, 2026

Abstract: The accelerating pace of digital transformation has expanded dependency on online services, exposing a widening misalignment between technology adoption and cybersecurity competence. This study investigates generational disparities in digital security literacy, perceived risk, and protective behaviors, with a particular focus on senior citizens as high-risk end users within computer network and information security ecosystems. 112 participants from various age and professional cohorts were surveyed using a four-point Likert scale with minimal central tendency response bias followed by both descriptive and mean-comparison analyses. Results demonstrate that cybersecurity literacy is medium but uneven (mean = 2.02), with respondents from the oldest age group (age sixty and above) reporting the lowest composite security score and weakest preventive practices, including a Two-Factor Authentication penetration of only 35%. There is a clear confidence-competence gap (+0.47) among senior citizens, meaning they tend to overestimate their ability to deal with digital services but underestimate the challenge of acquiring technical knowledge. Building on these findings, the paper introduces the Digital Guardian for Seniors framework a conceptual, human-centric intervention model integrating adaptive, visually oriented pedagogy, an intergenerational cyber-buddy system, and suggested metrics for longitudinal evaluation. The study contributes to computer network and information security research by providing demographic-based empirical evidence and outlining a theoretical foundation for future empirical testing and targeted interventions for an aging digital population.

Index Terms: Digital security literacy, cybersecurity awareness, confidence-competence gap, senior citizens, phishing and social engineering, Two-Factor Authentication, human-centric cybersecurity

1. Introduction

Digital transformation has fundamentally reshaped socio-economic activities by moving essential services such as banking, healthcare, and government administration onto networked digital platforms [1-2]. This shift has improved efficiency and accessibility but simultaneously expanded the cyber-attack surface and redirected many threats from purely technical infrastructures toward human users who interact with online systems on a daily basis [2-3]. As a result, computer network and information security has evolved from a predominantly technical domain into a socio-technical challenge in which user awareness, behavior, and risk perception play a decisive role [2], [9].

While the importance of human-centric cybersecurity is well-recognized [2], [9], most existing studies predominantly examine digitally active populations operating within institutional environments, such as employees or students, who benefit from formal security policies and technical support [5], [10]. Older adults, by contrast, remain comparatively underexplored despite their increasing reliance on high-risk digital services [17-18]. Previous research on this demographic has largely focused on technology acceptance and digital inclusion, while systematic attention to cybersecurity literacy and susceptibility to network-borne attacks remains limited [20], [26].

This study addresses a critical research gap by examining the psychological phenomenon known as the confidence–competence gap. Existing empirical studies have documented overconfidence in general cybersecurity

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

contexts, showing how inflated self-perceptions can increase phishing susceptibility among younger users and corporate professionals [8], [12]. However, there is a lack of rigorous benchmarking that transposes these findings specifically to the senior citizen demographic [18], [26]. This group is particularly vulnerable due to the sudden loss of "institutional security buffers" such as workplace IT support and mandatory training upon retirement [3], [24].

Consequently, this study provides an empirical mapping of generational vulnerability by quantifying the confidence–competence gap among 112 participants across diverse age groups. We position this gap as a key indicator of cyber-risk susceptibility, particularly for retirees. Building on these descriptive findings, we introduce the Digital Guardian for Seniors (DGS) framework as a conceptual intervention model tailored to the cognitive and experiential needs of an aging population [17], [19].

In line with the scope of this journal, the study is guided by the following research questions:

RQ1: How do younger users differ from senior citizens regarding digital security literacy?

RQ2: How significant is the confidence–competence gap among senior's users concerning cyber threats?

RQ3: What conceptual intervention structuring can enable cybersecurity preparedness amid a digital immigrant-ageing demographic?

2. Related Works

2.1. Human Centric Cybersecurity and Security Awareness

Quite a number of research discuss that even in the presence of technical hardening, human factor is the weakest point related to computer network and information security [3-5]. To systemically measure knowledge, attitudes, and behaviors relating to information security the Human Aspects of Information Security Questionnaire (HAIS Q) was developed [6-7], [24]. User behavior and awareness are critical determinants of organizational security outcomes; as such a tool like this not only had practicality regarding end-user access but again demonstrated that user behaviors were significant determinates on an organization is security outcome. These findings support a larger body of human centric cybersecurity literature [3], [9], [19] which identifies the importance of integrating technological solutions (e.g., firewalls, antivirus software, encryption) with user focused education, risk communication and behavioral interventions to improve effective protection. From this perspective, end users are an active element of the security architecture, and their literacy and practices directly impact networked systems' resilience [3], [19]. More recently, practitioner-oriented work has also emphasized the need to convert tools like HAIS Q into implementable initiatives for strategic awareness and culture building [24], [29].

2.2. Older Adults, Phishing Vulnerability, and 2FA Adoption

Recent research has put a spotlight on the heightened vulnerability of older adults to online fraud, phishing and scam campaigns. Younger and older users have been compared in some experimental work, confirming that older age is related to more difficulty distinguishing between real emails and phishing emails, resulting in being more likely to fall victim to misleading parties and an increased risk for identity theft or monetary loss [11-14], [17-19]. Both review and guidance documents also relate the general finding that older adults have lower levels of digital literacy skills, less familiarity with web interfaces, and difficulty assessing the credibility of online information capabilities easily manipulated by malicious actors [11-12], [17]. Additional evidence from studies on digital competence and literacy suggests that self-assessments may not be reliable among older adults: many tend to over or underestimate their actual skills [20], [26].

In parallel, research on authentication practices shows that Two Factor Authentication (2FA) is very powerful for improving account security but under adopted by older users [15-16]. Studies on older adults using 2FA and security tokens show that usability, inclusive design, and technology anxiety play a fundamental role as (deterrents to) adoption [15-16]. Though interventions and educational programs to improve cyber safety for seniors have been suggested, these typically present general advice (e.g., "use strong passwords" or "be careful of scams") and do not systematically quantify security literacy, risk perception and behavioral gaps between age groups or the diversity in older adults' needs [11-12], [17-18], [26].

2.3. Research Gap and Motivation

The existing literature clearly shows that older adults are at increased risk of phishing and online fraud and that they face specific challenges in adopting protective measures such as 2FA [11-19]. However, several important gaps remain.

- First, most empirical studies concentrate on either phishing susceptibility or authentication usability in isolation, while few provide an integrated, quantitative mapping of digital security literacy, impact perception, and preventive behaviors across multiple generations [11-12].
- Second, although concepts related to self-efficacy and security awareness have been explored, the explicit quantification of a confidence–competence gap where perceived ability diverges from actual technical awareness has received limited attention in the context of older adults [8], [18].

- Third, prior work often stops at descriptive recommendations and does not translate findings into structured, measurable intervention frameworks that can be deployed by community organizations, financial institutions, or public agencies [11-12], [17-18].

This study addresses these gaps by (1) providing a generational comparison of cybersecurity literacy dimensions using a structured survey instrument inspired by HAIS Q [6-7], [19], [24], [26], (2) operationalizing and quantifying the confidence–competence gap for different age cohorts, with a focus on senior citizens, and (3) proposing the Digital Guardian for Seniors (DGS) framework as a targeted, human centric intervention model with clearly defined objectives, delivery methods, and Key Performance Indicators (KPIs). In doing so, the work contributes to the human centric security agenda of computer network and information security research and offers a practical pathway for mitigating age-related vulnerabilities in real world digital environments [3], [9], [19], [24].

3. Research Method

3.1. Data Collection

The current study adopts a quantitative, survey-based methodology, to investigate comparative differences in cybersecurity literacy and behavioral correlates across generations [30]. Data were collected using a structured online questionnaire delivered through a web-based form platform. 112 valid responses were gathered across a broad demographic spectrum covering diversity in both age, education level and occupational field thus providing a substantial overview of the modern-day device user population.
The participants were divided into four age groups: 18-25, 26-40, 41-59 and ≥60 years. In each sample there were variations in the sex breakdown and educational attainment and employment status (students, employees or professionals, retirees). Older adults (60 years and above), being the targeted population for this study, were intentionally included to ensure representation of a high-risk demographic group in cybersecurity research [17], [18]. Table 1 presents a summary of the general characteristics of respondents by age group, education, and occupation.

Table 1. Distribution of respondents by age group, education, and occupation

Age Group	Gender	Education	Occupation	Percentage
18-25	Mixed	Bachelor	Student	25%
26-40	Mixed	Bachelor/Master	Employee	30%
41-59	Mixed	Bachelor/Master	Professional	27%
>60	Mixed	High School/Bachelor	Retired	18%
Total				100%

3.2. Survey Instrument and Variables

The survey instrument was designed with reference to the Human Aspects of Information Security Questionnaire (HAIS-Q) framework to strengthen content validity and alignment with established human-centric cybersecurity constructs [6-7], [24]. To accommodate the target demographic, the instrument was deliberately streamlined into eight core items. While this design may appear simplistic, it was intentionally adopted to reduce cognitive load and prevent survey fatigue a well-documented methodological challenge when surveying senior citizens [26]. A longer, more complex instrument could have severely compromised the response quality from older adults. The eight core items covered four broad aspects of digital safety:

- Threat Awareness (Q1-Q2): measures the ability to recognize common cybers threats including phishing, malware and suspicious links.
- Impact (Q3-Q4): Asks what the respondent thinks would be the potential financial, privacy-related and reputational impact of a security incident
- Preventive behavior (Q5-Q7): It measures whether users actively try to protect themselves, for example they have a strong password and 2FA enabled, as well whether their software or systems are updated regularly.
- Self-Confidence (Q8): Measures perceived confidence in managing risks posed by digital security threats and responding to potentially suspicious situations online.

3.3. Measurement Scale

All items were assessed using a four-point Likert style ranging from 1 (Strongly Disagree) to 4 (Strongly Agree). Opting for an even-numbered scale was a methodological decision designed to eliminate the neutral midpoint and reduce neutral response bias [30]. Older adults often exhibit a strong central tendency bias, defaulting to mid-scale choices when unsure. Eliminating the neutral midpoint was a deliberate choice to force discriminative responses and avoid ambiguity among senior participants, although we acknowledge this may introduce a degree of forced-choice bias as a limitation. We calculated a composite cybersecurity score for each respondent by averaging the mean item scores.

3.4. Data Analysis Techniques

Given the exploratory nature of the study, data analysis primarily relied on descriptive statistics and mean comparisons [30]. Descriptive statistics were calculated to summarize the response distribution of each item and dimension, including mean values and percentage frequencies. Second, we conducted comparative analyses of means across the four age categories to explore patterns in literacy levels and protective practices. Third, the primary analytical attention was given to quantifying the Confidence-Competence Gap (CCG), which is used as a descriptive proxy for psychological misalignment between perceptions of ability and technical knowledge [8]. The following expression operationalized the gap:

$$Gap = Self\text{-}Confidence\ Score\ (Q8) - Technical\ Awarness\ Score\ (Q1+Q2) \quad (1)$$

A substantially positive value of this gap indicates a descriptive state of overconfidence, in which the user's perceived capability exceeds their underlying technical literacy. This condition is interpreted as a psychological risk factor that may increase susceptibility to phishing, fraud, and other social engineering attacks [11-12], [19]. Finally, an occupational risk stratification analysis was conducted to contrast retirees with respondents who benefit from institutional security support.

4. Results

4.1. Descriptive Statistics of Cybersecurity Dimensions

Analysis at descriptive level of the 112 valid responses shows that the cybersecurity literacy among all respondents is mixed and generally moderate, however quite differentiated across age classes as well as for specific dimensions related to security. The knowledge of phishing (mean = 2.89) and malware identification (mean = 3.05), on the other hand, is comparatively constant, that most users could identify typical threats. Impact perception, on the other hand, is remarkably diminished (mean = 2.20), suggesting a certain ignorance about how catastrophic the aftermath of a cyber incident can be.

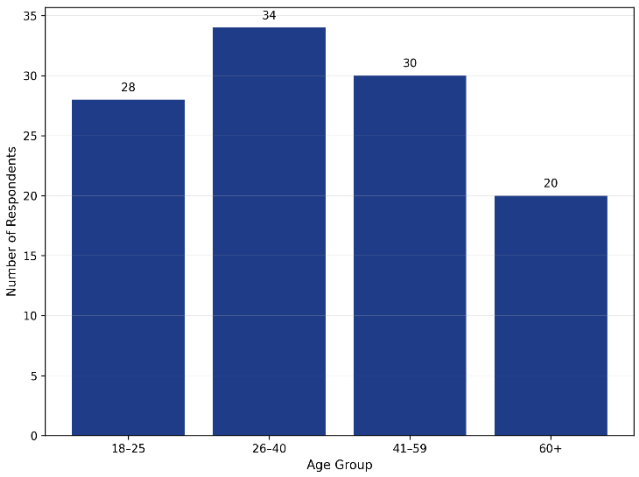


Fig.1. Distribution of respondents by age group.

Fig (respondent distribution=18-25,26-40,41-59 and≥60 years). 1. 26-40 years (46%), 41-59 years (20%) and 18-25 years. Older adults (≥60) makes up a small sample from the total but is one of the main targets of this study due to their higher vulnerability on cyber security risks [17], [19]. This distribution gives a wide generation range in order to enable descriptive comparison.

4.2. Generational Differences in Cybersecurity Literacy

The descriptive findings show a distinct downward trend in cybersecurity literacy as age increases. The average scores of younger respondents are higher, while scores systematically decrease among the older generation and reach the lowest levels among senior citizens. Hence, this pattern reinforces the existence of a generational security gap in our sample.

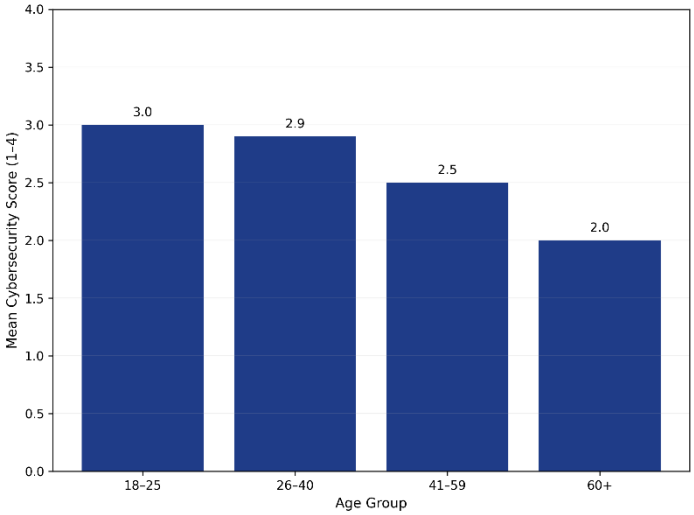


Fig. 2. Mean cybersecurity scores across age groups.

Table 2. Mean cybersecurity scores by dimension and age group.

Age Group	Threat Awareness	Impact Perception	Preventive Behavior	Composite Score
18-25	3.2	2.8	3.1	3.1
26-40	3.0	2.6	2.9	2.9
41-59	2.7	2.3	2.4	2.5
>60	2.2	1.9	1.8	2.02

As demonstrated in Table 2, seniors received the lowest composite security score (mean = 2.02). The most notable vulnerability in this population is in the Preventive Behavior domain (mean = 1.80), demonstrating low engagement in tangible protective behaviors. Notably, retirees recorded a Two-Factor Authentication adoption rate of only 35%, indicating that many older users access sensitive services with minimal additional security layers.

4.3. Identifying the Confidence-Competence Gap

The descriptive analysis reveals a pronounced psychological pattern described in this exploratory study as the confidence-competence gap. Elderly individuals give a relatively high score of confidence in self-execution of digital activities (mean = 2.50), however, their actual result for this area technical awareness is mainly lower with the average score of 2.02, so we have a difference between these scores +0.47 points. This is the largest gap of any generation, showing an overconfidence in description where perceived ability exceeds real technical literacy.

Table 3. Confidence-competence discrepancy by generation.

Generation & Age	Tech Score (Q1+Q2)	Confidence (Q8)	Gap (Conf - Tech)	Primary Info Source	Risk Level
Gen Z (13-28)	3.31 (High)	3.44 (High)	+0.13	Social media	Low-Risk
Gen Y (29-44)	3.10	3.20	+0.10	Social media /Online News	Medium
Gen X (45-60)	2.50	2.80	+0.30	Friends/Family	High-Risk
Boomers (60+)	**2.02 High Vulnerability (Descriptive)**	2.50	**+0.47**	TV/Newspaper	**High Vulnerability (Descriptive)**

These results suggest that the psychological risk associated with overconfidence is most acute among older adults, who combine lower technical literacy with inflated self-perceptions. Consequently, they are categorized as having a "High Vulnerability" in Table 3.

Table 4. Mean cybersecurity scores across profession groups.

Rank	Profession	Security Score (Avg)	2FA Adoption (Q6)	Description
1	Students	3.40	76%	Safety (Digital Native)
2	Private Employees	3.15	70%	Safety (Exposed to office policies)
3	Self-Employed/Freelance	2.50	25%	At Risk (No IT standards)
4	**Retired**	**1.86**	**35%**	**Highly Vulnerable** (Easy Target)

Cybersecurity risk is also not uniform across occupational groups. As summarized in Table 4, retirees have the lowest mean security score (mean = 1.86). The cohort does not have a huge amount of experience with formal security policies. However, students (mean = 3.40; 76% of the time adopted 2FA) and private-sector employees (mean=3.15) exhibit a more robust security posture due to their exposure to workplace security policies designed as organizational protections against digital threats. These results softly buttress the role of institutional support, and exposure to digital risk as major determinants of secure user behavior that other human centered studies have reported [3], [9], [24].

5. Discussion and the Conceptual Digital Guardian for Seniors (DGS) Framework

The findings of this study highlight a critical socio-technical vulnerability in the contemporary cybersecurity landscape: the disproportionate risk borne by senior citizens, which is consistent with prior work showing heightened exposure of older adults to phishing and online scams [11-14, 17-19]. While digital transformation is often framed as a story of technological adoption and efficiency, the results indicate that, for older adults, it has also generated a form of security debt that manifests in low digital security literacy, weak preventive behavior, and heightened susceptibility to online fraud.

5.1. The Confidence-Competence Paradox

One of the most salient findings is the confidence-competence gap of +0.47 observed in the Boomer generation. Senior citizens report a self-confidence score of 2.50 in navigating digital services, yet their technical awareness score is only 2.02, reflecting a classic overconfidence effect. In the case of older adults, this gap is particularly dangerous: a false sense of security diminishes their perceived need to verify suspicious requests, making them prime targets for social engineering attacks that exploit psychological comfort rather than technical vulnerabilities **[11-14, 17-19].**

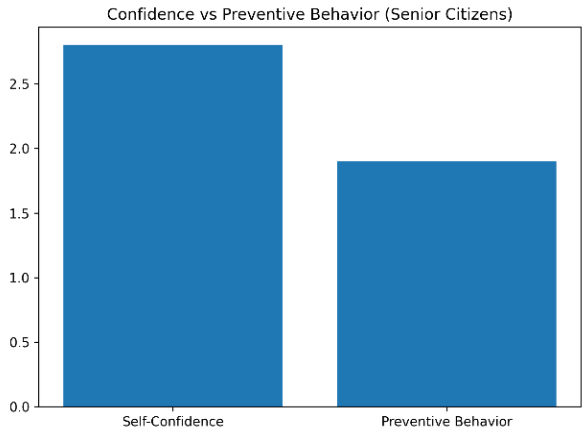


Fig. 3. Confidence-competence gap among senior citizens.

5.2. Low Impact Perception as a Behavioral Barrier

A second important insight is the disconnect between threat recognition and impact perception among senior users. Although older adults in the sample can identify basic threats such as malware with relatively adequate scores (mean = 3.05), their understanding of the financial and personal consequences of cyber incidents remains alarmingly low (mean = 2.20), echoing previous reports that many users underestimate the real world impact of cybercrime until they experience a loss themselves [11-12]. Cyber threats are thus perceived as abstract or distant problems rather than immediate risks to pensions, savings, or personal data.

This limited impact perception acts as a behavioral barrier to the adoption of preventive measures. When the perceived severity of a breach is low, security controls are likely to be seen as optional or burdensome rather than necessary, which helps explain the modest 2FA adoption rate of only 35% among seniors, despite evidence that 2FA provides a strong additional layer of protection against account compromise [15-16]. Without a clear mental model of what is at stake, even users who have heard of security mechanisms are unlikely to invest the effort required to implement and maintain them [3], [19], [24], [29].

5.3. Socio-Economic Vulnerability of Retirees

The occupational analysis further refines this picture by identifying retirees as the most vulnerable group, with an average security score of 1.86 and the lowest preventive compliance. During their working lives, many individuals benefit from what can be termed institutional security buffers formal IT policies, periodic awareness trainings, enforced password standards, and access to helpdesks or security teams which human centric cybersecurity research has shown to be

important in shaping secure behavior [3], [6-7], [19], [24]. Upon retirement, these institutional protections effectively disappear, yet digital exposure does not; retirees continue to rely on electronic banking, e government services, health platforms, and messaging applications for daily needs [11-12], [17-18].

This loss of institutional support, combined with potential age-related cognitive decline and reduced opportunities for informal peer learning about technology, produces a "soft target" profile that malicious actors can easily exploit [11-14], [17-19]. Self-employed and freelance workers are also at elevated risk for different reasons, but they often lack standardised IT policy or dedicated support, which has inconsistent and sometimes ad hoc security practices. In contrast, students and non-publics who have generally higher literacy scores and 2FA adoption rates use digital tools regularly, have peer pressure to perform better, and employees also engage definitively in continuing organizational security policies [3], [7], [19], [24].

5.4. The Conceptual Digital Guardian for Seniors (DGS) Framework

The generational gaps identified in this study highlight the need for a shift from generic, one-size-fits-all awareness campaigns toward targeted, intergenerational resilience strategies [3, 9, 24]. Consequently, this study proposes the Digital Guardian for Seniors (DGS) framework as a conceptual and theoretical intervention model tailored specifically for elderly users. The framework is designed to address the confidence–competence paradox and low impact perception by emphasizing hands-on technical validation and peer-supported learning [17-18], [26].

The "buddy system" is also a central theoretical pillar of DGS, where older users are combined with younger more tech-savvy ones (like Gen Z volunteers or family members). Since Gen Z participants in this study demonstrated the highest level of technical awareness (mean = 3.31), the intergenerational pairing may be utilized to rely on specific skills that can aid seniors with high-priority areas, including using Two-Factor Authentication and recognizing potential phishing, as well as confirming authenticity for requests received online.Beyond technical support, the buddy system is intended to serve as a mechanism to recalibrate risk perception, helping older users align their self-confidence with their actual technical skills through guided feedback and practice [17-18].

The conceptual DGS framework comprises three core components aimed at building foundational cybersecurity resilience:

- **Program Objectives:** To enhance threat recognition, increase the adoption of basic security controls (particularly 2FA), and reduce susceptibility to social engineering attempts [11-14], [23].
- **Delivery Methods:** Utilizing visual-based learning materials, scenario-driven demonstrations, and one-on-one assistance to accommodate the cognitive and experiential needs of older adults [17], [26].
- **Evaluation Metrics:** Utilizing measurable indicators, such as pre- and post-training security scores and changes in 2FA adoption rates, to assess theoretical program effectiveness [30].

Table 5. The proposed Digital Guardian for Seniors framework.

Objective	Delivery Method	Evaluation Metric
Threat Recognition	Visual training	Pre/Post test score
Increase 2FA Adoption	Hands-on assistance	2FA usage rate
Reduce Phishing Risk	Scenario simulation	Incident reports

Table 6. The "Digital Guardian for Seniors" Framework: A Multi-Pillar Intervention Model.

Rank	Profession
Target Audience	Senior Citizens (Baby Boomers; age 60+), which constitutes a high-risk demographic segment (n=29; 25.9% of the study population)
Core Educational Materials	1. Elderly-Friendly Workshops: 'Identification and Prevention of Internet Scams'; large letters, simplified grammatical constructs 2. Technical Demos: Live enablement of Two-Factor Authentication (2FA) on banking and messaging applications (WhatsApp, etc.) 3. Quick-Reference Cards: '5 Signs of Phishing Emails/Chats' pocket guides 4. Buddy System: Young volunteers provide 1-on-1 mentorship to help close technical knowledge gaps.
Distribution Channels	1. Seminars at local health centers (Posyandu), neighborhood halls, and places of worship. 2. Partnerships with social security agencies (BPJS), financial institutions, and retiree communities. 3. YouTube tutorial videos in crisp large subtitles & dedicated helpdesk hotlines for digital outreach
Suggested Key Performance Indicators (for future pilot testing)	1. Primary Goal: Measurable increase in Two-Factor Authentication usage among retirees. 2. Meta-KPI: Observable improvement in digital security literacy scores over a 6-month timeframe. 3. Implementation Priority: High priority for community-based pilot deployment.

Table 5 and 6 summarizes these elements by aligning each objective with a concrete delivery method and corresponding evaluation metric, emphasizing practicality and measurability within community or institutional training settings.

By combining clear objectives, tailored pedagogy, and intergenerational support mechanisms, the conceptual DGS framework offers a theoretical blueprint for addressing the security debt accumulated by older adults [3, 9, 11-19, 24, 26, 29].

5.5. Limitations of the Study

Although this research highlights important perspectives toward generational cybersecurity differences, several methodological limitations deserve comment. Firstly, the sample (n=112) was small and distribution across demographic sectors, in particular the senior citizen group is narrow these limits necessarily how widely findings can be generalised. Second, this survey design included a simplified 8-item assessment and a forced-choice 4-point Likert scale. While this deliberately reduced neutral response bias and survey fatigue among older adults, it may oversimplify complex psychological constructs [30]. Third, the study relies on descriptive statistics and mean comparisons. The "confidence-competence gap" is operationalized as a descriptive mathematical proxy rather than a normalized, rigorously validated psychological construct [8]. Therefore, the findings and the proposed DGS framework should be interpreted strictly as an exploratory baseline. Future research should employ larger, more representative sampling, inferential statistical models (e.g., ANOVA, regression), and empirical pilot testing to validate the efficacy of the DGS framework [30].

6. Conclusion

This study confirms that senior citizens constitute a highly vulnerable demographic segment in the digital ecosystem, primarily due to a pronounced descriptive confidence–competence gap of +0.47 observed between their perceived digital confidence and actual technical awareness. This psychological discrepancy, where high self-confidence masks low cybersecurity proficiency, is reflected in critical behavioral shortcomings, including a Two-Factor Authentication (2FA) adoption rate of only 35% among retirees. The transition of older adults from institutionally managed environments into unmanaged digital spaces generates a security debt that conventional, generic awareness campaigns are poorly equipped to address.

In response to these descriptive findings, this study introduces the Digital Guardian for Seniors (DGS) framework as a conceptual and theoretical intervention model tailored specifically to the needs of elderly users. Combining adaptive and visually oriented pedagogy with an intergenerational buddy system makes, we believe, DGS a theoretical framework for addressing the key tasks of threat recognition, uptake of core safeguards such as 2FA but also recall of risk assessment around these.

Further studies are needed to test and longitudinally assess the DGS framework in practice, including whether it achieves behavior change over time for older adults. Importantly, additional delineation of the interaction between cognitive processes and age on detecting threats is required to tailor these neuro-aware protective strategies towards older users in a digital world.

All the Declarations and Statements

Author Contribution Statement

Kartika Purwandari - Conceptualization, Methodology, Writing (Original Draft), and Supervision.
Join W.C. Sigalingging - Data Curation, Formal Analysis, Validation, and Review.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

This research received no external funding.

Data Availability Statement

Data available on request due to privacy restrictions regarding the human subjects involved.

Ethical Declarations

This study involving human subjects was conducted according to the ethical guidelines of the authors' institution.

Acknowledgements

We sincerely thank Bina Nusantara University and the Agency for Meteorology, Climatology, and Geophysics (BMKG) for their institutional support.

Declaration of Generative AI in Scholarly Writing

During the preparation of this work, the authors used AI-assisted tools strictly for language refinement and formatting assistance. After using this service, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

Abbreviations

The following abbreviations are used in this manuscript:

DGS - Digital Guardian for Seniors
2FA - Two-Factor Authentication
CCG - Confidence-Competence Gap

Appendix A\B\C…, with appendix tile

None.

References

[1] B. Hammoda and S. Foli, "A Digital Competence Framework for Learners (DCFL): A Conceptual Framework for Digital Literacy," Knowledge Management & E-Learning, vol. 16, no. 3, pp. 477–500, 2024. https://doi.org/10.34105/j.kmel.2024.16.022.

[2] T. Schaltegger, B. Ambuehl, N. Bosshart, A. Bearth, and N. Ebert, "Human Behavior in Cybersecurity: An Opportunity for Risk Research," Journal of Risk Research, vol. 28, no. 8, pp. 843–854, 2025. https://doi.org/10.1080/13669877.2025.2539109

[3] D. Humphreys, A. Koay, D. Desmond, and E. Mealy, "AI hype as a cyber security risk: the moral responsibility of implementing generative AI in business," AI and Ethics, vol. 4, no. 3, pp. 791–804, 2024. https://doi.org/10.1007/s43681-024-00443-4.

[4] N. Y.-R. Douha, K. Renaud, Y. Taenaka, and Y. Kadobayashi, "Smart home cybersecurity awareness and behavioral incentives," Information & Computer Security, vol. 31, no. 5, pp. 545–575, 2023. https://doi.org/10.1108/ICS-03-2023-0032.

[5] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," Journal of Computer Information Systems, vol. 62, no. 1, pp. 82–97, 2022. https://doi.org/10.1080/08874417.2020.1712269.

[6] A. R. Pradipta and R. G. Utomo, "Enhancement of the Human Aspects of Information Security Questionnaire (HAIS-Q) for Indonesia Educational Institutions," in 2025 3rd International Conference on Software Engineering and Information Technology (ICoSEIT), pp. 1–6, 2025. 10.1109/ICoSEIT67010.2025.11290747.

[7] P. Kathryn, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans. "The human aspects of information security questionnaire (HAIS-Q): two further validation studies." Computers & Security, vol. 66, pp. 40-51, 2017. https://doi.org/10.1016/j.cose.2017.01.004.

[8] S. Masmoudi, "Unveiling the Human Factor in Cybercrime and Cybersecurity: Motivations, Behaviors, Vulnerabilities, Mitigation Strategies, and Research Methods," in Cybercrime Unveiled: Technologies for Analysing Legal Complexity, pp. 41–91, Springer, 2025. https://doi.org/10.1007/978-3-031-80557-8_3

[9] A. Sutton and L. Tompson, "Towards a Cybersecurity Culture-Behaviour Framework: A Rapid Evidence Review," Computers & Security, vol. 148, p. 104110, 2025. https://doi.org/10.1016/j.cose.2024.104110

[10] J. Iqbal, S. H. Soroya, and K. Mahmood, "Financial Information Security Behavior in Online Banking," Information Development, vol. 40, no. 4, pp. 550–565, 2024. https://doi.org/10.1177/02666669221149346

[11] J. Klütsch, L. Haehn, A. Kreuder, C. Böffel, U. Frick, and S. J. Schlittmeier, "InstaTrust or InstaTrap: How Relationships and Developmental Tasks Affect Young Adults' Phishing Susceptibility on Instagram," International Journal of Human-Computer Studies, vol. 197, p. 103456, 2025. https://doi.org/10.1016/j.ijhcs.2025.103456

[12] A. Kavvadias and T. Kotsilieris, "Understanding the Role of Demographic and Psychological Factors in Users' Susceptibility to Phishing Emails: A Review," Applied Sciences, vol. 15, no. 4, p. 2236, 2025. https://doi.org/10.3390/app15042236

[13] D. Pehlivanoglu et al., "Phishing Vulnerability Compounded by Older Age, Apolipoprotein E e4 Genotype, and Lower Cognition," PNAS Nexus, vol. 3, no. 8, p. pgae296, 2024. https://doi.org/10.1093/pnasnexus/pgae296

[14] S. Kemp and N. Erades Pérez, "Consumer Fraud Against Older Adults in Digital Society: Examining Victimization and Its Impact," International Journal of Environmental Research and Public Health, vol. 20, no. 7, p. 5404, 2023. https://doi.org/10.3390/ijerph20075404

[15] T. Taffese, F. Chavez, A. Fernandez-Reyes, and M. Byrne, "Redesigning and Evaluating Interfaces for Two-Factor Authentication: Performance of Younger and Older Adults," 2025. https://doi.org/10.31234/osf.io/vtx7u_v1

[16] W. K. Bong and Y. J. Li, "How Many Times Do I Need to Say, 'It Is Me'? Investigating Two-Factor Authentication with Older Adults in Norway," in ICT4AWE, pp. 25–34, 2025. https://doi.org/10.5220/0013206500003938

[17] B. A. Morrison, J. Nicholson, L. Coventry, and P. Briggs, "Recognising Diversity in Older Adults' Cybersecurity Needs," in Proceedings of the 2023 ACM Conference on Information Technology for Social Good, pp. 437–445, 2023. https://doi.org/10.1145/3582515.3609565

[18] A. Sheil et al., "Enhancing Personalised Cybersecurity Guidance for Older Adults in Ireland," in Companion Publication of the 2024 Conference on Computer-Supported Cooperative Work and Social Computing, pp. 478–484, 2024. https://doi.org/10.1145/3678884.3681894
[19] H. Chen, M. He, X. Xu, and D. Atkin, "Examining Older Adults' Vulnerability to Online Health Scams: Insights from Routine Activity Theory," Frontiers in Public Health, vol. 13, p. 1585851, 2025. https://doi.org/10.3389/fpubh.2025.1585851
[20] M. D. Marzan, A. Stamate, and L. Spiru, "Digital Competence Among Older Adults: Is Self-Assessment Reliable?" Cureus, vol. 16, no. 11, 2024. https://doi.org/10.7759/cureus.73543
[21] F. R. Castillo-Villar and R. G. Castillo-Villar, "Mobile Banking Affordances and Constraints by the Elderly," Marketing Intelligence & Planning, vol. 41, no. 1, pp. 124–137, 2023. https://doi.org/10.7759/cureus.73543
[22] M. Kritika, "Neuro-Cognitive Approaches to Cybersecurity: A Systematic Review Integrating Neuroscience and Cognitive Psychology for Human Factor Analysis," Information & Computer Security, pp. 1–29, 2026. https://doi.org/10.1108/ics-03-2024-0076
[23] K. Khadka, A. B. Ullah, W. Ma, E. M. Marroquin, and Y. Alem, "A Survey on the Principles of Persuasion as a Social Engineering Strategy in Phishing," in 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1631–1638, 2023. https://doi.org/10.1109/trustcom60117.2023.00222
[24] G. Lyon, "Informational Inequality: The Role of Resources and Attributes in Information Security Awareness," Information & Computer Security, vol. 32, no. 2, pp. 197–217, 2024. https://doi.org/10.1108/ics-04-2023-0063
[25] A. Al Zaidy et al., "Measuring Cybersecurity Awareness of Students: A Study of State College Students," Journal of Information Technology, Cybersecurity, and Artificial Intelligence, vol. 2, no. 3, pp. 17–40, 2025. https://doi.org/10.70715/jitcai.2025.v2.i3.030
[26] J. Choi et al., "Everyday Digital Literacy Questionnaire for Older Adults: Instrument Development and Validation Study," Journal of Medical Internet Research, vol. 25, p. e51616, 2023. https://doi.org/10.2196/51616
[27] S. Kim, "Impact of Cybersecurity Self-Efficacy on Digital Economic Behaviors Among Older Adults," INQUIRY: The Journal of Health Care Organization, Provision, and Financing, vol. 62, 2025. https://doi.org/10.1177/00469580251370933
[28] M. J. Al Ansari, Y. Al Ahmed, and H. H. El Bahnaswi, "Balancing Usability and Protection in AI and Data Security: A Human-Centric Approach," in 2024 11th International Conference on Software Defined Systems (SDS), pp. 80–88, 2024. https://doi.org/10.1109/sds64317.2024.10883898
[29] X. Xu, W. C. H. Hong, K. Kolletar-Zhu, Y. Zhang, and C. Chi, "Validation and Application of the Human Aspects of Information Security Questionnaire for Undergraduates: Effects of Gender, Discipline and Grade Level," Behaviour & Information Technology, vol. 43, no. 12, pp. 2799–2820, 2024. https://doi.org/10.1080/0144929x.2023.2260876
[30] R. P. Dalka, D. Sachmpazidi, C. Henderson, and J. P. Zwolak, "Network Analysis Approach to Likert-Style Surveys," Physical Review Physics Education Research, vol. 18, no. 2, p. 020113, 2022. https://doi.org/10.1103/PhysRevPhysEducRes.18.020113

Authors' Profiles



Kartika Purwandari Kartika Purwandari received her master's degree in the field of computer science from National Central University, Taiwan. She currently serves as a Faculty Member at the Computer Science Department, Bina Nusantara University, Jakarta, Indonesia. Her current research interests include artificial intelligence, natural language processing, information system and sentiment analysis. Ms. Purwandari is the corresponding author for this research and can be reached via her professional committee affiliations.



Join W.C. Sigalingging earned his master's degree from his respective institution in the field of database management and computer science. He currently works at the Agency for Meteorology, Climatology, and Geophysics (BMKG) within the Centre for Database, Jakarta, Indonesia. His professional experience includes managing large-scale database systems and technical data security. His research interests focus on cybersecurity awareness and data protection frameworks. Mr. Sigalingging is a professional member of his respective national agency and contributes to database security standards.

How to cite this paper

Kartika Purwandari, Join W.C. Sigalingging, "The Confidence-Competence Gap in Senior Cybersecurity: An Exploratory Survey and Conceptual Framework", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.16, No.3, pp. 88-97, 2026. DOI:10.5815/ijwmt.2026.03.06