

Exploration of Factors Influencing Individual Information Security Behavior: A Study Based on Behavioral Models

Shuting Huang¹, Latif Rahman^{1*}, Haslinda Husaini¹

¹ School of Information Science College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Malaysia

*Corresponding Author: ablatif@uitm.edu.my

Received: 29 April 2025 | Accepted: 28 May 2025 | Published: 30 June 2025

DOI: <https://doi.org/10.55057/ajress.2025.7.5.29>

Abstract: *This study explores the impact of four demographic variables—gender, age, education level, and professional background—on individual information security behavior. Through questionnaire surveys and statistical analysis, it was found that differences in overall behavior scores among these demographic factors are not significant, with respondents demonstrating a certain consistency in password setting and online behavior adjustment. However, further analysis combined with existing literature reveals some trend differences in security awareness, risk perception, and behavioral practices across different genders and age groups.*

Keywords: Individual information security behavior, demographic factors, gender differences, education level, age groups, professional background

1. Introduction

In modern society, the rapid development of information technology and the internet has deeply integrated informatization and digitization into people's daily lives and work (Subach, 2024). However, this technological advancement has also brought new challenges and risks, particularly in the field of information security (Radchenko et al., 2023).

The rapid digital transformation and the increasing prevalence of smart devices have led to a surge in the collection, storage, and processing of individual data, making individual information security behavior a critical issue in the digital age. Various studies have emphasized the importance of establishing a legal framework to protect individual data and prevent cybercrimes such as phishing (Permana and Jamaludin, 2023). Selifanov et al. (2023) highlighted the necessity of improving digital literacy and skills for securely managing individual data. Countries like Russia are also working to ensure information security in the digital space through comprehensive legal measures (Kozyreva et al., 2022).

Cyberattacks, data breaches, and other information security incidents pose significant threats to individual privacy, property security, social stability, and national security, garnering widespread societal attention (Li and Liu, 2021). The globalization of the information space requires new approaches to ensure information security, emphasizing international cooperation and legal frameworks (Boyko, 2023). Implementing comprehensive risk management strategies, such as systems compliant with the ISO/IEC 27001 standard, employee training, security technologies, and incident response mechanisms, is crucial for effectively combating

cyber threats (Renvall, 2018). Information security, as a component of national security, highlights the importance of combating information threats and protecting information resources at both national and international levels (Mieier et al., 2023).

Understanding the determinants of individual information security behavior is crucial for enhancing overall security levels. Studies emphasize various factors influencing security behaviors at the individual and environmental levels, such as demographics, security awareness, experience with security incidents, national culture, industry type, and organizational security culture (de Bruin and Mersinas, 2024). Furthermore, the importance of human factors in risk management systems is highlighted, emphasizing the need to enhance the systematization and standardization of evaluation procedures (Khlaponin et al., 2024). Additionally, awareness of data collection significantly impacts perceived information security issues and information-sharing behavior on social media, indicating the necessity of establishing transparent privacy policies and clearly communicating data collection practices to mitigate security threats (Phan et al., 2023). By considering these factors and implementing tailored security training, organizations can effectively promote correct security practices and habits among individuals, ultimately reducing information security risks.

Studying the influencing factors of individual information security behavior is essential for enhancing public awareness and capabilities in information security (de Bruin and Mersinas, 2024; Susanto and Maulana, 2024; Dominguez-Dorado et al., 2023). National culture, industry type, organizational security culture, demographics, security awareness, and prior security incident experience all play significant roles at both the environmental and individual levels in shaping individual security behavior (de Bruin and Mersinas, 2024). In addition, the relationships between knowledge and information security behavior attitudes, the impact of training, and gender differences are important considerations in developing effective education and training programs to enhance information security awareness and skills across various sectors, including government organizations (Susanto and Maulana, 2024). By adopting targeted interventions to address these factors, organizations and policymakers can develop evidence-based strategies, policies, and regulations to enhance public awareness and skills in information security (Dominguez-Dorado et al., 2023). With the continuous emergence of new technologies (such as big data, artificial intelligence, and blockchain), the challenges and risks in the field of information security are also constantly evolving.

This study aims to evaluate the information security behaviors of college students in a digital environment and identify the key factors influencing their security practices. Through a questionnaire survey, the study will examine students' awareness of individual information security risks and utilize structural equation modeling (SEM) to analyze the potential factors affecting information security behavior and their interactions.

2. Literature Review

Frequent hacker attacks and data breaches, coupled with the abuse of social engineering tactics, have further exacerbated the risks to individual information security (Jamal, Algeelani, and Al-Sammarrhaie, 2024). However, existing laws and regulations often lag behind technological developments, resulting in regulatory gaps in individual data protection and making it urgent to establish a more comprehensive legal framework (Babikian, 2023). At the same time, the lack of user awareness regarding information security makes individuals more susceptible to cyber threats, highlighting the importance of strengthening education and training to enhance digital risk awareness and foster safe behaviors (Tsvyk and Tsvyk, 2023). Although

technologies such as artificial intelligence are seen as potential solutions to enhance information security, without raising user awareness and providing strong legal protections, relying solely on technological means remains insufficient to effectively address information security challenges.

The challenges faced by individual information security practices mainly stem from technical vulnerabilities, insufficient user awareness, organizational culture influences, and inadequate legal regulations. The widespread use of IoT devices and social media has increased the risk of data breaches, with some platforms lacking effective security measures (Ananthan and Zolkipli, 2022). Meanwhile, many users exhibit insufficient awareness of individual data protection, which may lead to the unintentional disclosure of sensitive information (Ananthan and Zolkipli, 2022). Organizational culture also plays a crucial role in security management; a corporate environment lacking security awareness may lead employees to neglect information security practices (Bekkevik et al., 2018). In addition, the inconsistency of regulations across countries complicates the implementation of data protection measures (Tang et al., 2024). In response to these challenges, research indicates that regular educational training can enhance user security awareness and strengthen the security culture within organizations (Chang and Lin, 2007). Moreover, technical measures such as encryption, access control, and data anonymization can effectively reduce the risk of data breaches (Ananthan and Zolkipli, 2022).

Demographic characteristics are important factors in predicting individual information security behavior. Research indicates that variables such as age, gender, and education level have a significant impact on security practices. Older adults often exhibit more pro-security behaviors, with studies indicating that users of healthcare information systems tend to be more cautious and less likely to engage in anti-security actions (Sari et al., 2023). However, some research findings suggest that older users may feel less secure in digital environments, indicating a complex relationship between age and perceived security (Bukovec and Antoliš, 2024). Gender differences are also significant, with women typically exhibiting higher pro-security behaviors than men (Sari et al., 2023). In terms of cybersecurity awareness, gender-specific factors have been shown to significantly influence behavior, suggesting that targeted training can enhance cybersecurity awareness among different genders (Zahid et al., 2023). Higher education levels are generally associated with improvements in individual security behavior, particularly in understanding the security measures of digital banking (Bukovec and Antoliš, 2024). However, education alone does not guarantee better security practices, as evidenced in healthcare institutions, where higher education has not fully translated into enhanced security behaviors (Sari et al., 2023). Although demographic factors play a crucial role in shaping individual information security behavior, environmental factors such as organizational culture and individual experiences must also be considered, as they can significantly influence security practices (de Bruin and Mersinas, 2024). It is important to note that higher education does not necessarily ensure adherence to best security practices, suggesting that security behavior is influenced not only by educational background but also by individual habits and environmental contexts.

Although demographic characteristics can partially explain individual information security behaviors, they are not decisive factors and must be analyzed in conjunction with other psychological and environmental variables. First, the impact of age may be moderated by technological proficiency. Although older users tend to be more security-conscious, they may still be susceptible to cyber threats if they lack sufficient technical knowledge. Conversely, younger users, while taking fewer traditional security measures, may be more familiar with newer digital security tools, such as two-factor authentication or password managers. Second,

the role of gender factors may vary depending on cultural backgrounds and social roles. In some socio-cultural contexts, women may be more inclined to follow security rules, while men may be more willing to take risks with technological tools, affecting their information security practices (Anwar et al., 2017). Finally, although higher education can enhance information security awareness, individual motivation and practical ability remain key determinants. Merely possessing security knowledge does not necessarily translate into effective security behavior. Therefore, when formulating information security policies and training programs, relying solely on demographic characteristics is insufficient; it is also necessary to consider individual psychological cognition, behavioral habits, and the technological environment to develop more targeted information security management strategies.

Research on cybersecurity behavior across different age groups has revealed significant differences in information security practices. Older individuals tend to adopt technology more cautiously, and their information security behaviors are generally more conservative, emphasizing risk awareness (Bognár and Bottyán, 2024). In contrast, although young people are more open to adopting new technologies, they may lack sufficient awareness of information security risks, leading to less secure behaviors (de Bruin and Mersinas, 2024). These findings highlight that age not only affects technology usage patterns but also influences individuals' attitudes and behaviors toward information security. Compared to younger individuals, older adults generally exhibit more cautious practices (Sari, Handayani, and Hidayanto, 2023).

Research on information security behavior also highlights gender differences in individuals' attitudes toward cybersecurity. Some studies suggest that women exhibit higher levels of caution and awareness, such as using complex passwords and security software (McGill and Thompson, 2021), while other studies indicate that men may be more prone to taking risks and ignoring security warnings (Ting et al., 2024). Factors influencing these behaviors include demographic characteristics such as gender. Research further indicates that in China, there are no significant differences between men and women in cybersecurity awareness across various aspects such as malware, password usage, phishing, and social engineering (Ting et al., 2024). Moreover, the impact of gender on security decision-making remains a noteworthy area of concern, with empirical studies seeking to understand how demographic characteristics influence security judgments (Mbaka and Tuma, 2023). These findings collectively emphasize the importance of considering gender differences in information security behavior when developing effective cybersecurity awareness programs and interventions.

Research on the information security behaviors of individuals with different education levels reveals a subtle relationship. Although higher education is generally associated with improved information literacy and risk awareness (Bognár and Bottyán, 2024), it is also crucial to consider other factors such as technical literacy and psychological aspects when analyzing information security behaviors (de Bruin and Mersinas, 2024). Education level has been found to significantly impact information security behavior in medical information systems (Sari, Handayani, and Hidayanto, 2023). Therefore, while higher education can promote better information security behavior, a comprehensive understanding of various influencing factors is essential for accurately assessing individual cybersecurity practices.

The type of profession also significantly affects information security behavior, with practitioners in technical fields such as IT and information management exhibiting higher levels of security awareness and skills compared to those in non-technical fields (Alkhazi et al., 2022). Undergraduate students majoring in non-science disciplines demonstrate higher levels of problematic information security behavior (PISB) compared to those majoring in

science fields, indicating a correlation between academic background and PISB levels (Chen et al., 2021). These insights emphasize the importance of tailoring security training and awareness programs based on academic disciplines to enhance the overall cybersecurity posture.

3. Research Methods

The research on individual information security behavior proposes four primary objectives. It is necessary to develop a feasible approach to achieve these objectives, which are addressed through four corresponding hypotheses.

Research Questions:

Q1: How does age affect an individual's information security behavior?

Q2: Does gender play a significant role in the formation and practice of individual information security behavior?

Q3: In what ways does education level affect individual information security behavior?

Q4: Do individuals with different professional backgrounds exhibit significant differences in individual information security behavior?

Hypotheses:

H1: Age positively influences individual information security behavior.

H2: Gender positively influences individual information security behavior.

H3: Education level positively influences individual information security behavior.

H4: Profession positively influences individual information security behavior.

3.1 The impact of Gender on personal information security behavior

The relationship between age and individual information security behavior is complex, with impacts observed by different studies varying considerably. Older adults tend to support increased government involvement in cybersecurity, while younger individuals often exhibit more proactive security behaviors. This nuanced understanding highlights the importance of age as a factor influencing information security practices. Older adults strongly support government intervention in cybersecurity and advocate for punitive measures against cybercrime (Lyon, 2025). Research indicates that compared to the older generation, younger employees (millennials) exhibit more positive attitudes and behaviors toward information security (Nguyen and Le, 2024). Furthermore, the "Big Five" personality traits moderate this relationship, suggesting that younger groups may possess traits that enhance their information security behaviors (Warrington et al., 2021).

A higher level of education is also associated with increased information security awareness, particularly among younger individuals (Nguyen and Le, 2024). Understanding organizational policies significantly affects the cybersecurity behaviors of different age groups, indicating that education and policy knowledge are crucial for enhancing security practices (Jalali, 2024). Conversely, while younger individuals may be more actively engaged in individual information security behaviors, the stronger support for government measures among older adults reflects differing approaches to risk reduction. These findings suggest that age-related vulnerabilities require tailored strategies in cybersecurity education and policy development.

H1: Age positively influences individual information security behavior.

3.2 The impact of Age on Personal Information Security Behavior

The relationship between gender and individual information security practices reveals significant differences in behavior and cognition. Research indicates that men typically exhibit higher levels of security behavior compared to women, which may impact the overall security practices of households and organizations. This gender difference is crucial for understanding how different groups manage and perceive individual information security. Studies show that men are generally more proactive in adopting security measures, while women tend to exhibit lower levels of security behavior (McGill and Thompson, 2018). Men often exert greater influence on ICT-related decisions within households, contributing to the creation of a safer digital environment (Kohlberg and Kävrestad, 2020). Protection Motivation Theory (PMT) and Social Bond Theory (SBT) emphasize that self-efficacy and perceived vulnerability significantly influence information security behavior, with notable gender differences observed (Berthevas, 2018). Women may demonstrate lower self-efficacy in security practices, which can affect their willingness to engage in protective measures (McGill and Thompson, 2018). Understanding these differences can enhance the effectiveness of safety initiatives in both individual and organizational contexts (Rea and Chen, 2008). Conversely, some researchers argue that focusing solely on gender may overlook other key factors influencing information security practices, such as age, experience, and socioeconomic status, all of which play important roles in shaping security behaviors.

H2: Gender positively influences individual information security behavior.

3.3 The impact of education level on personal information security behavior

Multiple studies have shown that education level significantly affects individual information security behavior. Higher education is associated with improvements in information security knowledge, attitudes, and behaviors, indicating that individuals with higher education levels are more likely to adopt security measures. This relationship is particularly evident in environments involving technology use and cybersecurity. Research indicates that individuals with higher education levels demonstrate greater awareness of information security issues, which positively impacts their behavior (Bostan and Akman, 2015). The Knowledge-Attitude-Behavior (KAB) model emphasizes that education enhances the connection between knowledge and positive information security attitudes (Nguyen and Le, 2024). Compared to older individuals, younger and more educated individuals tend to exhibit more proactive security behaviors (Nguyen and Le, 2024). Conversely, although education level is a strong predictor of security behavior, it is important to recognize that other factors, such as age and socioeconomic status, also influence individual information security practices. This highlights the need for a multifaceted approach to enhance security awareness among different demographic groups.

H3: Education level positively influences individual information security behavior.

3.4 The impact of the profession on personal information security behavior

By fostering a culture of ethical behavior and commitment among IT professionals, individual information security practices have been significantly enhanced. Research indicates that organizational commitment positively impacts IT professionals' information security protection behaviors (Ma, 2022). The ethical dilemmas in the IT industry require balancing innovation with user privacy, highlighting the importance of integrity and honesty in professional conduct (Zebua and Zebua, 2025). Research further shows that clear cybersecurity policies can positively influence employees' behavior in addressing information security risks (Li et al., 2014). Conversely, although professional competence can enhance security practices, a lack of awareness or training may lead to negligence in adhering to these standards, potentially undermining the effectiveness of security measures.

H4: Professionalism positively influences individual information security behavior.

4. Results and Analysis

Information security behavior is one of the key dimensions for measuring the actual protective measures users take in response to cybersecurity threats. This study evaluates individuals' specific practices in password setting, password complexity, and online behavior adjustment through four indicators. As shown in Table 1. The data show that users particularly excel in device password setting. BE2 (setting a password on a mobile phone, $M = 4.06$, $SD = 0.874$) and BE3 (setting a password for a computer, $M = 4.05$, $SD = 0.856$) received the highest ratings, reflecting widespread awareness of basic device protection. In contrast, BE4 (using a complex password to protect an account, $M = 3.83$, $SD = 0.867$) and BE1 (adjusting online behavior due to security concerns, $M = 3.49$, $SD = 0.827$) scored slightly lower, indicating that there is still room for improvement in more proactive security behaviors. Overall, the average score for this variable is 3.857, suggesting that most users have already demonstrated a strong tendency toward cybersecurity behaviors in their daily lives, particularly in password protection, where they exhibit a high level of self-protection capability.

Table 1

	Items	Min	Max	Mean	Std. Error	Std. Dev	Var
BE1	I modify my internet usage habits because of security concerns.	1	5	3.49	0.042	0.827	0.684
BE2	I set passwords for my mobile phone.	1	5	4.06	0.045	0.874	0.764
BE3	I set passwords for my computer.	1	5	4.05	0.044	0.856	0.734
BE4	I use complex passwords to protect my accounts.	1	5	3.83	0.044	0.867	0.752

Adjustment was conducted through four indicators. To further explore the impact of demographic characteristics on information security behavior, the study employed an independent samples t-test and a one-way ANOVA to analyze four demographic variables: age, gender, education level, and major. As shown in Table 2 and Table 3, the t-test was used to assess the differences between two independent groups (such as gender), while ANOVA was applied to compare statistical differences among three or more independent groups (such as different age groups or education levels). This analysis aims to determine whether there are significant differences in information security behavior among different groups, thereby providing a basis for subsequent clustering strategies or personalized intervention measures.

Table 2

		Descriptive		Levene's Test for Equality of Variances		t-test for Equality of Means			Result	
		Mean	Std. Dev	F	Sig.	t	df	Sig. (2-tailed)		
Behavior	Gender	Male	3.25	0.84	2.072	0.151	-0.745	382	0.457	Not Sig.
		Female	3.32	0.92						
	Major	IT-related	3.25	0.87	0.323	0.57	-0.761	382	0.447	Not Sig.
		Non-IT-related	3.32	0.86						

In the analysis of the gender variable, the average behavior score for males was 3.25 (standard deviation = 0.84), and for females, it was 3.32 (standard deviation = 0.92). The result of Levene's test for equality of variances was $F = 2.072$, $p = 0.151$, meeting the assumption of homogeneity of variances. Further independent samples t-test analysis showed that $t(382) = -0.745$, $p = 0.457$, indicating that the difference in information security behavior between genders was not statistically significant. Similarly, in terms of professional background, the average score for IT-related majors was 3.25 (standard deviation = 0.87), while for non-IT-related majors it was 3.32 (standard deviation = 0.86). Levene's test results ($F = 0.327$, $p = 0.567$) also supported the assumption of homogeneity of variances. The independent samples t-test result was $t(382) = -0.761$, $p = 0.447$, indicating that an IT background does not significantly affect behavior scores. Overall, these results suggest that neither gender nor professional background has a statistically significant impact on individuals' information security behavior.

Table 3

Sources/Factor	Dependent Variable	df	Levene's Test for Equality of Variances		F-value	P-value	Result*
			F	Sig.			
Age	Between Groups	5	0.511	0.728	1.88	0.113	Not Sig.
	Within Groups	379					
Education level	Between Groups	4	1.007	0.39	0.033	0.992	Not Sig.
	Within Groups	380					

When conducting a one-way ANOVA on the two variables of age and education level, the results did not show any statistically significant differences. Specifically, age was divided into five groups, and the analysis results were $F(5, 379) = 1.880$, $p = 0.113$ (> 0.05), indicating that there were no significant differences in information security behavior scores across different age groups. Levene's test for homogeneity of variances yielded $F = 0.511$, $p = 0.728$, satisfying the assumption of homogeneity of variances required for the ANOVA.

Similarly, regarding education level, the differences in behavior scores among the five groups of respondents were also not statistically significant [$F(4, 380) = 0.033$, $p = 0.992$], and Levene's test result was $F = 1.007$, $p = 0.390$, again supporting the assumption of homogeneity of variances. These results indicate that neither age nor educational background has a statistically significant impact on individual information security behavior.

5. Conclusion

This study focused on four demographic factors—gender, professional background, age, and education level—to explore their differences in information security behavior. The analysis results showed that the differences in behavior scores across these variables did not reach statistical significance, indicating that respondents' security behaviors—such as password setting, the use of password complexity, and online behavior adjustment—were relatively consistent. The findings suggest that information security behavior may not be directly influenced by demographic attributes but is more likely related to individual security awareness and daily habits.

Future research could expand the research perspective by exploring psychological and behavioral factors that influence information security behavior, such as risk perception,

security responsibility, and behavioral motivation. Additionally, comparisons across different industries, cultural backgrounds, or organizational environments could be conducted to enhance the universality and practical value of the findings. It is also recommended that future studies employ methods such as long-term tracking or experimental interventions to observe the evolution of individual security behaviors, thereby providing more targeted support for the development of cybersecurity education and practice strategies.

References

- Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior. *IEEE Access*, 10, 132132-132143.
- Ananthan, T. R., & Zolkipli, M. F. (2022). Challenges and Issues in Implementing Personal Data Protection. *Int. J. Recent Contributions Eng. Sci. IT*, 10(2), 53-61.
- Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437-443.
- Babikian, J. (2023). Securing Rights: Legal Frameworks for Privacy and Data Protection in the Digital Era. *Law Research Journal*, 1(2), 91-101.
- Berthevas, J.-F. (2018). Students' computers safety behaviors, under effects of cognition and socialization: when gender and job experience influence information security behaviors. <https://doi.org/10.1109/ITMC.2018.8691175>
- Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences*, 14(6), 588.
- Bostan, A., & Akman, I. (2015). Impact of education on security practices in ICT. *Tehnicki Vjesnik-Technical Gazette*, 22(1), 161-168. <https://doi.org/10.17559/TV-20140403122930>
- Boyko, S. M. (2023). Political and Legal Framework of the International Information Security System: Russian Approaches and Initiatives. *Russian Journal of World Politics and Law of Nations*, 1(1-2), 4-22.
- Bukovec, M., & Antoliš, K. (2024). The Impact of Age and Education on Cyber Security in Digital Banking. *Medijska Istraživanja*, 30(2), 129-152. <https://doi.org/10.22572/mi.30.2.6>
- Chen, Y. T., Shih, W. L., Lee, C. H., Wu, P. L., & Tsai, C. Y. (2021). Relationships among undergraduates' problematic information security behavior, compulsive internet use, and mindful awareness in Taiwan. *Computers & Education*, 164, 104131.
- De Bruin, M., & Mersinas, K. (2024). Individual and Contextual Variables of Cyber Security Behaviour--An empirical analysis of national culture, industry, organization, and individual variables of (in) secure human behavior. *arXiv preprint arXiv:2405.16215*.
- Domínguez-Dorado, M., Calle-Cancho, J., Galeano-Brajones, J., Rodríguez-Pérez, F. J., & Cortés-Polo, D. (2023). Detection and mitigation of security threats using virtualized network functions in software-defined networks. *Applied Sciences*, 14(1), 374.
- Ernest Chang, S., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial management & data systems*, 107(3), 438-458.
- Jalali, F. (2024). Cybersecurity Behavior During COVID-19 and the Impact of Policy Awareness and Demographics on Information Security Behavior and Its Determinants. <https://doi.org/10.32920/25418173>
- Jamal, H., Algeelani, N. A., & Al-Sammarraie, N. (2024). Safeguarding data privacy: strategies to counteract internal and external hacking threats. *Computer Science and Information Technologies*, 5(1), 46-54.

- Khlaponin, Y., Izmailova, O., Krasovska, H., Krasovska, K., Bodnar, N., & Abbas, S. Q. (2024, April). The base of models of the information security risks assessment system. In 2024 35th Conference of Open Innovations Association (FRUCT)(pp. 352-366). IEEE.
- Kozyreva, A., Rustikova, G., Pirozhkova, T., Shelmenkov, V., & Belyavskiy, A. (2022). Legal support of information security of the individual in the conditions of digital transformation of society. In SHS Web of Conferences (Vol. 134, p. 00043). EDP Sciences.
- Li, L., He, W., Xu, L., Ivan, A., Anwar, M., & Yuan, X. (2014). Does Explicit Information Security Policy Affect Employees' Cyber Security Behavior? A Pilot Study. 169–173. <https://doi.org/10.1109/ES.2014.66>
- Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176-8186.
- Lyon, G. (2025). Information sharing, investment, and retaliatory posture: the role of age in preferences toward information security governance. *Information, Communication & Society*, 1–16. <https://doi.org/10.1080/1369118x.2025.2451401>
- Ma, X. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing and Management*, 59(1), 102744. <https://doi.org/10.1016/J.IPM.2021.102744>
- Mbaka, W., & Tuma, K. (2023). Impact of gender on the evaluation of security decisions. *arXiv preprint arXiv:2310.04097*.
- McGill, T., & Thompson, N. (2018). *Gender Differences in Information Security Perceptions and Behaviour*. University of Technology Sydney ePress. <https://doi.org/10.5130/ACIS2018.CO>
- McGill, T., & Thompson, N. (2021). Exploring potential gender differences in information security and privacy. *Information & Computer Security*, 29(5), 850-865.
- Nguyen, B. H., & Le, H. N. Q. (2024). Investigation on information security awareness based on KAB model: the moderating role of age and education level. <https://doi.org/10.1108/ics-09-2023-0152>
- Nguyen, B. H., & Le, H. N. Q. (2024). Investigation on information security awareness based on KAB model: the moderating role of age and education level. <https://doi.org/10.1108/ics-09-2023-0152>
- Nohlberg, M., & Kävrestad, J. (2020). Exploring Information Security and Domestic Equality (pp. 224–232). Springer, Cham. https://doi.org/10.1007/978-3-030-57404-8_17
- Permana, F. A., & Jamaludin, A. (2023). Personal Data Vulnerability in the Digital Era: Study of Modus Operandi and Mechanisms to Prevent Phishing Crimes. *Jurnal Al-Hakim: Jurnal Ilmiah Mahasiswa, Studi Syariah, Hukum dan Filantropi*, 201-216.
- Pham, T. H., Phan, T. A., Trinh, P. A., Mai, X. B., & Le, Q. C. (2024). Information security risks and sharing behavior on OSN: the impact of data collection awareness. *Journal of Information, Communication and Ethics in Society*, 22(1), 82-102.
- Radchenko, O., Bielai, S., Kovach, V., Hrabar, N., & Yevtushenko, I. (2023). Formation of Information Security Systems of the State: Current Status, Trends, and Problems. In *National Security Drivers of Ukraine: Information Technology, Strategic Communication, and Legitimacy* (pp. 93-112). Cham: Springer Nature Switzerland.
- Rea, A., & Chen, K. (2008). Privacy Control and Assurance: Does Gender Influence Online Information Exchange? (pp. 165–189). IGI Global. <https://doi.org/10.4018/978-1-60566-012-7.CH008>
- Renvall, A. (2018). Improving cybersecurity through ISO/IEC 27001 information security standard in the context of SMEs.

- Sari, P. K., Handayani, P. W., & Hidayanto, A. N. (2023). Demographic Comparison of Information Security Behavior Toward Health Information System Protection: Survey Study. *JMIR Formative Research*, 7. <https://doi.org/10.2196/49439>
- Sari, P. K., Handayani, P. W., & Hidayanto, A. N. (2023). Demographic Comparison of Information Security Behavior Toward Health Information System Protection: Survey Study. *JMIR Formative Research*, 7(1), e49439.
- Selifanov, V., Anikeeva, V. V., & Ognev, I. A. (2023). Issues of assessing the credibility of the risk management system. *Безопасность Цифровых Технологий*, 1, 69–82. <https://doi.org/10.17212/2782-2230-2023-1-69-82>
- Subach, T. (2024). The main aspects of the digital development of society. *Teoretičeskā Ēkonomika*, 0(4), 24–35. <https://doi.org/10.52957/2221-3260-2024-4-24-35>
- Susanto, T. D., & Maulana, M. D. (2024). Evaluating the Influence of Attitude versus Knowledge and Individual Factor versus Intervention Factor on Information Security Awareness in Local Government. *Procedia Computer Science*, 234, 1428-1434.
- Susanto, T. D., & Maulana, M. D. (2024). Evaluating the Influence of Attitude versus Knowledge and Individual Factor versus Intervention Factor on Information Security Awareness in Local Government. *Procedia Computer Science*, 234, 1428-1434.
- Ting, T. T., Lee, M. Y., Chok, S. X., Huang, Y. H., Choy, X. N., Lee, K. T., ... & Olugbade, T. O. (2024). Digital government: Social media as a mediator in technology acceptance with political knowledge, interest, and participation. *Online Journal of Communication and Media Technologies*, 14(4), e202454.
- Tsvyk, V. A., & Tsvyk, I. V. (2023). Personal information security is a social problem. *Вестник Российского университета дружбы народов. Серия: Социология*, 23(3), 590-599.
- Warrington, C., Syed, J., & Tappin, R. M. (2021). Personality and Employees' Information Security Behavior among Generational Cohorts. *Computer and Information Science*, 14(1), 44. <https://doi.org/10.5539/CIS.V14N1P44>
- Zahid, I., Hussein, S., & Mahdi, S. (2023). Measuring Individual's Cybersecurity Awareness Based on Demographic Features. *Al-Mağalla' al-‘irāqīyya' al-Handasa' al-Kahrabā'iyya' Wa-al-Iliktrūniyya'*. <https://doi.org/10.37917/ijeee.20.1.6>
- Zebua, D. Y., & Zebua, A. P. (2025). Tantangan Etika Dalam Profesi Teknologi Informasi. *Jurnal Ilmu Ekonomi, Pendidikan Dan Teknik.*, 2(1), 35–44. <https://doi.org/10.70134/identik.v2i1.162>
- Мієр, Т. І., Дика, Н. М., Третяк, О. П., Журба, К., Голодюк, Л. С., Стецик, С. П., & Цибульська, С. М. (2023). Information and information resources as social and personal values of education and of subjects of the educational process in the information era. *AD ALTA. Journal of Interdisciplinary Research*, 13(1), 6-12.