Cyber hygiene awareness among Malaysian youth

Amily Fikry[1], Azreen Joanna Abdul[1], Khairul Nazlin Kamaruzaman[1], Asnawati[2]
[1]Department of Entrepreneurship and Marketing, Universiti Teknologi MARA, Selangor, Malaysia
[2]Faculty of Economics and Business, Mulawarman University, Samarinda, Indonesia

Article Info

Article history:

Received Aug 8, 2025
Revised Dec 1, 2025
Accepted Dec 13, 2025

Keywords:

Awareness
Cyber hygiene
Cybersecurity
Knowledge
Malaysia
Youth

ABSTRACT

The study examined cyber hygiene awareness among Malaysian youth by analyzing the roles played by individual knowledge, awareness, attitudes, gender differences, and educational level. An online survey was conducted with 414 respondents in Peninsular Malaysia. The results showed no significant differences in cyber hygiene awareness based on gender and educational level. This suggests equal access to cybersecurity information and training across genders and education levels in Malaysia. This study also found significant relationships between individual characteristics (knowledge, rationality, and attitude) and cyber hygiene awareness. These findings indicate that individuals who are more knowledgeable, have positive attitudes, and make rational decisions tend to have higher cyber hygiene awareness. The results highlight the importance of fostering rationality and consistency in approaches to cybersecurity practices. The study contributes to the thoughtfully reflective decision-making (TRDM) theory, providing insights for developing targeted cybersecurity training programs and policies. Future research could explore additional factors influencing cyber hygiene awareness and examine how these findings translate to actual cybersecurity behaviors in professional settings.

Corresponding Author:

Amily Fikry
Department of Entrepreneurship and Marketing, Universiti Teknologi MARA
Cawangan Puncak Alam, Selangor, Malaysia
Email: amily@uitm.edu.my

1. INTRODUCTION

In this era of digital connectivity, information sharing on social media platforms has become a norm. The liberty to share thoughts, images, preferences, and aversions contributes to the rapid increase in user-generated content on social media platforms. This widespread practice has reshaped privacy and security in cyberspace. Social media users now face inherent cybersecurity hazards [1], such as the deliberate deception of users by irresponsible parties, which is one of the most challenging threats to address [1]. Malicious software is transmitted during content sharing on social media applications, leading to the prevalence of security issues, including fraud, phishing, software loopholes, and unauthorized system intrusions [2].

Cloudflare reported that 78% of cybersecurity managers across 14 countries, including Malaysia, experienced at least one cyber incident in 2023. More than 60% of the respondents faced over four attacks in the past year [3]. This trend was supported by Surfshark's report, where Malaysia experienced a 144% increase in breach rates in the third quarter of 2023, ranking eighth in the most breached country [4]. Kaspersky also reported that Malaysia was the second-highest country in Southeast Asia to prevent mobile malware attacks in 2022 [5].

A survey conducted on several organizations has identified key challenges in cybersecurity, including a lack of awareness, resources, and expertise [6]. It was revealed that Malaysian employees exhibited a concerning level of ignorance and lack of accountability regarding cybersecurity practices [6]. This finding underscores the urgency for initiatives to enhance awareness and strengthen Malaysia's cybersecurity position in the face of escalating threats. Thus, this study aimed to diagnose the effect of individual knowledge, awareness and attitude, gender and educational level towards cyber hygiene awareness among Malaysians.

2. LITERATURE REVIEW

Cyber hygiene awareness is aimed at enhancing users' activities and can be associated with alertness in the system of instructions and recommendations. This awareness aids in equipping users with relevant knowledge and skills, besides instilling the attitude and behavior to maintain healthy network security and system through online safety measures and data privacy, protection, and prevention [7]-[12].

2.1. Gender, educational level, and cyber hygiene awareness

In the realm of cybersecurity, humans are considered the most vulnerable component [13]. Therefore, it is essential to understand the demographics relating to human security behavior, such as age, education, gender, knowledge, and profession [14], which significantly shape an individual's perceptions, attitudes, and performance. A study reported that managers recognize that more men demonstrated security misbehavior than women [15]. Nonetheless, studies on cyber hygiene awareness across various research settings exhibited that demographic factors (age, gender, education level) are unreliable predictors of cyber hygiene awareness [13], [16], [17].

Gender and age have been identified as significant predictors of cyber hygiene awareness, though findings are inconsistent. Some studies report males having greater awareness but indifferent attitudes toward cyber hygiene [18]-[20], while a Thai study found women, especially from generations X and Y, exhibit higher phishing awareness due to caution and vigilance [21]. Research from Malaysia indicates age and gender influence cyber hygiene awareness and practices, but academic qualifications do not [22]. Conversely, some internet users perceive education level as positively impacting awareness [19]. These mixed results highlight the need for further investigation into demographic influences on cyber hygiene [23]. Thus, the following hypotheses were postulated for this study:
(H1): there is a significant difference between gender and cyber hygiene awareness among youth in Malaysia.
(H2): there is a significant difference between educational level and cyber hygiene awareness among youth in Malaysia.

2.2. Knowledge, rationality, attitude and cyber hygiene awareness

Knowledge significantly influences cyber hygiene awareness, with higher cybersecurity knowledge correlating to better awareness despite some insufficiency in risk mitigation [19]. Knowledgeable individuals are less vulnerable to cybercrime [24], while neglecting manufacturer guidelines results in poor awareness and increased cyberattack risk [25]. In healthcare, lack of cyber hygiene knowledge fosters risky behaviors [26]. Enhanced knowledge and positive cybersecurity attitudes improve awareness and practices at work, encouraging employees to model good habits for colleagues [27], [28]. Internet users with proactive attitudes toward cyber hygiene are more likely to adopt preventive measures [29]. Based on these findings, the following hypotheses were postulated for this study:
(H3): knowledge significantly influences cyber hygiene awareness among youth in Malaysia.
(H4): rationality significantly influences cyber hygiene awareness among youth in Malaysia.
(H5): attitude significantly influences cyber hygiene awareness among youth in Malaysia.

2.3. Cyber hygiene awareness through the lens of TRDM

The thoughtfully reflective decision-making (TRDM) theory was utilized to comprehensively understand cyber hygiene awareness among Malaysians by integrating knowledge and attitude variables [30]. This framework enables researchers to evaluate holistically the determinants of cybersecurity behavior (technical knowledge and attitudes) and decision-making processes when facing potential threats in the workplace. The integration of cognitive, emotional, and behavioral aspects of cybersecurity awareness could aid in the establishment of effective strategies to enhance cyber hygiene practices in the workplace. In summary, the study outcomes will shed light on the interaction between an individual's knowledge about cybersecurity threats, their attitudes towards security practices, and their rational decision-making processes and its impact on overall cyber hygiene awareness.

3. RESEARCH METHOD

This study used the purposive sampling method to distribute an online survey powered by SurveyMonkey targeted to 414 Malaysians in Peninsular Malaysia. The survey contained a multi-item scale of Cyber Hygiene Inventory (CHI) developed by [31] to measure cyber hygiene awareness and the Human Aspect of Information Security Questionnaire (HAISQ) [32] to assess an individual's knowledge, attitude, and rationality [10]. Upon finalizing the data collection process, the researchers utilized SPSS version 28 to conduct the statistical analysis of all responses gathered through the online survey.

4. RESULTS

4.1. Respondents' profiles

The study sample comprised 414 respondents of Malaysian nationality who reside in Peninsular Malaysia. Table 1 shows a significant gender imbalance, with females representing more than two-thirds of the sample (72.0%) and only 28.0% males. Most respondents belonged to the <20 years age group (51.9%), suggesting that the data represents a predominantly younger demographic. The second largest group were 21 to 25 years old (179 respondents, 43.2%). When combined with the previous age group, it can be inferred that the overwhelming majority of respondents (95.1%) are 25 years old or younger. Only a small fraction of the population falls within the 26–30 age bracket, accounting for just 2.9%, while the 31 to 35-year-old category only included three respondents (0.7%). Lastly, participants aged 36 years and above represented 1.2% of the total population (5 individuals). This study data is heavily skewed towards younger respondents, with a sparse representation of those older than (4.8%), reflecting the specific characteristics of the sample population (youth).

Most respondents possess a certificate/diploma (173 respondents, 41.8%), followed by SPM/STPM (121 respondents, 29.2%), bachelor's degree (117 respondents, 28.3%), and postgraduate qualifications (3 respondents, 0.7%). This distribution indicates that the population is composed mainly of early-career individuals or students. Meanwhile, a majority of the respondents resided in Selangor (50% (207 individuals), possibly attributed to the state's population size and economic activities, followed by Pahang (77 individuals, 18.6%), Federal Territory of Kuala Lumpur with (31 individuals, 7.5%), and Perak (32 individuals, 7.7%). A small percentage of the respondents resided across other states in Malaysia, including Johor (3.6%), Kedah (3.4%), and Melaka (1.0%). An overwhelming majority (87.2%) of the population are tertiary-level students, with only a small percentage employed in clerical (31 respondents, 7.5%), executive (14 respondents, 3.4%), and managerial positions (8 respondents, 1.9%).

4.2. Descriptive analysis of major variables

The major variables of this research include knowledge, attitude, and rationality related to cyber hygiene awareness among Malaysian youth, as presented in Table 2. Respondents were asked to indicate their views using a five-point Likert scale ranging from 1 (strongly agree) to 5 (strongly disagree).

The findings indicate that respondents tended to report only a moderate level of awareness regarding cyber hygiene, with many leaning toward the lower end of the scale (mean score=3.9878). As the score of 3 on the Likert scale represents neutrality and is close to a score of 4, the mean score for this variable indicates some concerns about awareness levels among respondents. The low standard deviation (0.48212) implies that there is relatively little variation in responses, suggesting consistency among individuals in their perceptions of cyber hygiene awareness.

The respondents also have moderate self-assessed knowledge about cyber hygiene (mean score=3.6373), indicating a tendency towards neutrality. A score of slightly above 3 suggests the respondents may have doubts about their proficiency in this area. Meanwhile, the low standard deviation (0.35442) reflects that most respondents had similar responses, indicating little diversity in their self-reported knowledge levels.

The study sample is moderately neutral regarding their attitudes towards cyber hygiene (mean score=3.4213), reflecting their ambivalence or reluctance to have a positive attitude towards cyber hygiene practices. The standard deviation is relatively low (0.34362), indicating the consistency in attitude among respondents.

Most respondents disagreed with statements related to the rational decision-making aspect of cyber hygiene (mean score=4.1335). A score above 4 is closer to the "Disagree" option, implying that the study population lack confidence or does not base their cyber hygiene practices on rational thought processes, suggesting the need for improvement in this area. The higher standard deviation (0.56735) indicates more variability in how respondents view the rationality component of their cyber hygiene behavior, reflecting differing levels of logical reasoning behind their actions.

Table 1. Demographic characteristics of the study sample (N=414)

Demographics	Frequency (n)	Percentage (%)
Gender		
Male	116	28
Female	298	72
Total	414	100
	Age Group	
18-20 years	215	51
21-25 years	179	43.2
26-30 years	12	2.9
31-35 years	3	0.7
>36 years	5	1.2
Total	414	100
	Academic qualification	
SPM/STPM or below	121	29.2
Certificate/diploma	173	41.8
Bachelor's degree	117	28.3
Master/doctor of Philosophy/doctor of Business administration	3	0.7
Total	414	100
	Occupation level	
Clerical	31	7.5
Executive	14	3.3.44
Managerial	8	19
Unemployed/tertiary level student	361	87.2
Total	414	100
	Current place of residence	
Federal Territory of Kuala Lumpur	31	7.5
Selangor	207	50
Melaka	4	1
Negeri Sembilan	9	2.2
Pulau Pinang	5	1.2
Kedah	14	3.4
Perlis	1	0.2
Johor	15	3.6
Terengganu	5	1.2
Kelantan	6	1.4
Pahang	77	18.6
Sabah	6	1.4
Sarawak	2	0.5
Perak	32	7.7
Total	414	100

Table 2. Descriptive analysis of major variables

Variable	Mean	Standard deviation
Cyber hygiene awareness	3.9878	0.48212
Individual characteristics		
Knowledge	3.6373	0.35442
Attitude	3.4213	0.34362
Rationality	4.1335	0.56735

4.3. Hypotheses testing

The potential differences between gender and cyber hygiene awareness (H1) were determined using the independent sample T-test. Meanwhile, the differences between educational level and cyber hygiene awareness (H2) were evaluated via the one-way analysis of variance (ANOVA). Subsequently, H3, H4, and H5 were assessed using the regression analysis. The hypotheses testing outcomes are detailed in the following subsections.

4.3.1. Differences between gender, educational level and cyber hygiene awareness among youth in Malaysia

(H1): there is a significant difference between gender and cyber hygiene awareness among youth in Malaysia.

The results obtained from the independent-samples t-test demonstrated no significant difference in scores for males (*M*=4.0041, *SD*=0.51727) and females (*M*=3.9815, *SD*=0.46849; *t* (412)=0.428, *p*=.67, two-tailed). The small differences in means between genders (Eta squared, η^2=0.002) indicated that this variable did not significantly influence cyber hygiene awareness levels in the study sample. Therefore, the H1 was rejected.

(H2): there is a significant difference between educational level and cyber hygiene awareness among youth in Malaysia.

The study categorized respondents into four education levels—SPM/STPM and below, certificate/diploma, bachelor's degree, and postgraduate qualifications—to assess educational effects on cyber hygiene awareness. Results from the between-groups one-way ANOVA showed no meaningful statistical difference among the categories at *p*<.05 in cyber hygiene awareness between education levels: *F* (3, 410)=0.808, *p*=.490. Thus, H2 was rejected.

4.3.2. Relationship between individual characteristics of knowledge, rationality, and attitude towards cyber hygiene awareness among youth in Malaysia

Table 3 shows an R2 of 0.319 for cyber hygiene awareness, indicating that 31.9% of the cyber hygiene awareness variance was explained by all three variables tested in this study. Therefore, the proposed model was significant (F=63.888, p<0.01). A closer examination revealed that individual characteristics, including rationality (β=0.488, p<0.01), knowledge (β=0.113, p<0.05), and attitude (β=0.115, p<0.05), were positively related to cyber hygiene awareness. Thus, H3, H4, and H5 were accepted.

A strong positive relationship between rationality and cyber hygiene awareness suggests more rational individuals tend to have higher awareness. The strength of this relationship is notable, indicating that rationality is a critical predictor of cyber hygiene awareness. Meanwhile, higher knowledge levels were associated with increased cyber hygiene awareness in this study. Despite the statistically significant relationship, the small coefficient value suggests knowledge has a modest impact on cyber hygiene awareness compared to reliability. Similarly, attitude is positively associated with cyber hygiene awareness with a small effect size (β=0.115), suggesting a positive disposition or proactive stance towards cybersecurity contributes to higher awareness with limited impact.

Table 3. Relationship between individual characteristics (knowledge, rationality, attitude) and cyber hygiene awareness

Variable	Standardized beta
Individual characteristic	
Rational	0.488***
Knowledge	0.113**
Attitude	0.115**
F value	63.888***
R^2	0.319
Adjusted R^2	0.314

*p < 0.10, **p<0.05, ***p<0.01

5. DISCUSSION

Results indicated that cyber hygiene awareness did not vary significantly across gender or education levels, implying that Malaysian youth generally receive similar opportunities for cybersecurity-related information and learning. This parity may result from workplace environments offering comprehensive cybersecurity resources and awareness campaigns. These findings align with earlier research [33] but contrast with studies reporting higher awareness among men [19], [20], [34]. Additionally, the results differ from a Thai study where females showed greater awareness of phishing threats [21], possibly due to higher self-consciousness. Another study suggested women's heightened cyber hygiene awareness stems from distrust in government and telecom cybersecurity policies [35]. Furthermore, [36] found females to be more proactive in managing privacy settings compared to males, which contradicts the current study's findings.

This study also revealed that cyber hygiene awareness among youth in Malaysia is significantly influenced by their level of knowledge, rationality, and attitudes. The analysis of individual characteristics revealed compelling results. For instance, rationality, knowledge, and attitude collectively explained 31% of the variance in cyber hygiene awareness. Among these factors, rationality emerged as the strongest predictor with a substantial positive relationship to awareness levels. This finding shows the importance of fostering rationality and consistency in individuals' approach to cybersecurity practices. Knowledge and attitude also demonstrated positive, albeit modest, relationships with cyber hygiene awareness. While these factors contribute to increased awareness, their impact appears to be less pronounced compared to rationality. This outcome reflects that knowledgeable individuals with positive attitudes and rational decision-makers tend to be more aware of cyber hygiene than those who do not exhibit these characteristics.

An earlier study revealed that most Malaysians lack knowledge and exhibit poor attitudes towards cybersecurity awareness, delegating the majority of responsibilities related to cybersecurity practices to the technical department and top management in their organization [37]. In contrast, another study found a significant relationship between knowledge and cybersecurity awareness but not attitude [24]. In a different study, a significant relationship between knowledge and cyberhygiene awareness was reported [38], [39], which in turn influences protective behaviors and compliance with security policies [38], [40]. Likewise, this study found a significant relationship between attitude and intention to adopt cybersecurity hygiene [41] in the organization and conduct specific training programs that caters to the diverse discipline and needs of engineers [42]-[46]. This observation was supported by another research, where internet users with positive and proactive attitudes toward cyber hygiene awareness have a higher tendency to adopt preventive measures [29]. Besides, continuous education on cyberhygiene [47], [48], monetary incentives given to employees [49] and organization’s policy revision [50] that support cybersecurity practices will further enhance cyberhygiene awareness and practices among employees.

6. CONCLUSION

This study findings contribute to the literature on cyber hygiene awareness among Malaysian youth, revealing that gender and education level do not significantly influence awareness levels. The results suggest gender- and education-specific cybersecurity training may be unnecessary and support for more unified training strategies. Nevertheless, there is a need to explore other factors that potentially impact cyber safety knowledge among Malaysians.

Future research on cyber hygiene awareness should investigate specific behaviors and knowledge variations across demographic groups, including gender, as subtle differences may exist despite no significant findings in the current study. Employing qualitative methods such as case studies and interviews can uncover motivations and perceptions influencing cybersecurity practices, potentially revealing gender-specific challenges or strengths. Additionally, conducting meta-analyses of existing literature would clarify inconsistencies and identify moderating factors. Exploring other predictors across cultures and professional contexts is essential to enhance understanding of cyber hygiene awareness and behavior.

The current study also discovered a lack of significant differences in gender and education level of respondents in determining cyber hygiene awareness, suggesting that interventions do not necessarily have to be gender-oriented among Malaysian youth. Nonetheless, future studies could explore how other variables, such as age, field of study, or profession, interact with gender and influence cyber hygiene awareness. The study outcomes could aid in developing more targeted and effective interventions in the future.

The findings emphasize the importance of continuous, tailored cybersecurity training programs that address the specific needs and behaviors of diverse employee profiles, particularly engineers who handle sensitive data and complex systems. Awareness initiatives should target all employees regardless of gender or education, focusing on rational decision-making, relevant knowledge, and positive cybersecurity attitudes. Innovative methods such as apps, gamified training, and simulations—including spear phishing exercises—can enhance engagement and provide real-time insights into cyber hygiene practices, enabling organizations to customize training effectively. Continuous education on emerging threats and best practices like strong passwords and phishing recognition is essential. Additionally, senior management support and fostering a culture that normalizes cybersecurity practices are critical for successful implementation. Incentives can motivate adherence to best practices, embedding cyber hygiene into organizational culture. Regular updates and reviews of cybersecurity measures—including system updates, new technologies, and policy revisions—are necessary to keep pace with evolving threats. Together, these strategies improve cybersecurity awareness and practices, ultimately strengthening organizational security in the engineering sector.

ACKNOWLEDGMENTS

This study was funded by the *Geran Penyelidikan Dana Fakulti Pengurusan Perniagaan* RIG (DDF RIG) [RMC File Number: 600-TNCPI 5/3/DDF (FPP) (006/2024)]. The authors would like to convey their appreciation to the Faculty of Business and Management and the Islamic Digital Marketing Research Interest Group for their endless support in ensuring the completion of this research.

FUNDING INFORMATION

This study was funded by the *Geran Penyelidikan Dana Fakulti Pengurusan Perniagaan* RIG (DDF RIG) [RMC File Number: 600-TNCPI 5/3/DDF (FPP) (006/2024)].

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Amily Fikry	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azreen Joanna Abdul	✓	✓		✓		✓	✓	✓	✓	✓	✓			
Khairul Nazlin Kamaruzaman	✓	✓	✓	✓	✓	✓			✓	✓	✓			
Asnawati	✓		✓	✓			✓		✓	✓	✓			

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis

I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting

Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

The authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

ETHICAL APPROVAL

The ethics committee of Universiti Teknologi MARA REC/08/2023 (ST/MR/222) approved this study.

DATA AVAILABILITY

The authors confirm that the data supporting the findings of this study are available within the article.

REFERENCES

[1] E. van der Walt, J. H. P. Eloff, and J. Grobler, “Cyber-security: identity deception detection on social media platforms,” *Computers &amp; Security*, vol. 78, pp. 76–89, Sep. 2018, doi: 10.1016/j.cose.2018.05.015.

[2] B. Bhatti, “Cyber security and privacy in the age of social networks,” in *Cyber Security Standards, Practices and Industrial Applications*, IGI Global, pp. 57–74.

[3] https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity- threatscape-2022-2023/, cited from PIKOM. (2024). Growing threat Cybersecurity Landscape in Malaysia 2024. PIKOM. https://www.pikom.org.my/2024/FOCS/PIKOM_Cybersecurity_Report.pdf

[4] https://www.thestar.com.my/tech/tech-news/2023/12/06/cybersecurity- report-ranks-malaysia-as-eighth-most-breached-country-in-q3-2023, cited from PIKOM. (2024). Growing threat Cybersecurity Landscape in Malaysia 2024. PIKOM. https://www.pikom.org.my/2024/FOCS/PIKOM_Cybersecurity_Report.pdf

[5] https://www.nst.com.my/news/nation/2023/07/935644/kaspersky- malaysia-ranks-second-southeast-asia-mobile-malware-attacks, cited from PIKOM. (2024). Growing threat Cybersecurity Landscape in Malaysia 2024. PIKOM. https://www.pikom.org.my/2024/FOCS/PIKOM_Cybersecurity_Report.pdf

[6] PIKOM, Cybersecurity Landscape in Malaysia 2024, PIKOM, Damansara, Malaysia, 2024.

[7] C. Ugwu, M. Ezema, U. Ome, L. Ofusori, C. Olebera, and E. Ukwandu, “A study on the impact of gender, employment status, and academic discipline on cyber-hygiene: a case study of University of Nigeria, Nsukka,” in *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*, Springer Nature Singapore, 2023, pp. 389–407.

[8] A. Irei, “What is cyber hygiene and why is it important?,” *Informa TechTarget,* 2023. https://www.techtarget.com/searchsecurity/definition/cyber-hygiene

[9] B. Mednikarov, “Cyber hygiene issues in the naval security environment,” *Information &amp; Security: An International Journal*, vol. 53, pp. 205–218, 2022, doi: 10.11610/isij.5314.

[10] C. J. Howell, Self-protection in cyberspace: Assessing the processual relationship between thoughtfully reflective decision making, protection motivation theory, cyber hygiene, and victimization. University of South Florida, 2021.

[11] Kaspersky, "Top tips for cyber hygiene to keep yourself safe online," May 16, 2022. https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

[12] S. Kalhoro, M. Rehman, V. Ponnusamy, and F. B. Shaikh, “Extracting key factors of cyber hygiene behaviour among software engineers: a systematic literature review,” *IEEE Access*, vol. 9, pp. 99339–99363, 2021, doi: 10.1109/access.2021.3097144.

[13] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, “Gender difference and employees’ cybersecurity behaviors,” *Computers in Human Behavior*, vol. 69, pp. 437–443, Apr. 2017, doi: 10.1016/j.chb.2016.12.040.

[14] W. N. A. Ibrahim, N. S. Saharudin, and D. F. Lestari, “Knowledge, attitude, and practice of computer vision syndrome among office workers in UiTM Puncak Alam,” *Environment-Behaviour Proceedings Journal*, vol. 8, no. 24, pp. 315–322, May 2023, doi: 10.21834/ebpj.v8i24.4644.

[15] L. Giddens, L. C. Amo, and D. Cichocki, “Gender bias and the impact on managerial evaluation of insider security threats,” *Computers &amp; Security*, vol. 99, p. 102066, Dec. 2020, doi: 10.1016/j.cose.2020.102066.

[16] T. B. G. Herath, P. Khanna, and M. Ahmed, “Cybersecurity practices for social media users: a systematic literature review,” *Journal of Cybersecurity and Privacy*, vol. 2, no. 1, pp. 1–18, Jan. 2022, doi: 10.3390/jcp2010001.

[17] M. H. Alsulami *et al.*, “Measuring awareness of social engineering in the educational sector in the Kingdom of Saudi Arabia,” *Information*, vol. 12, no. 5, p. 208, May 2021, doi: 10.3390/info12050208.

[18] N. Kshetri and M. Chhetri, “Gender asymmetry in cybersecurity: socioeconomic causes and consequences,” *Computer*, vol. 55, no. 2, pp. 72–77, Feb. 2022, doi: 10.1109/mc.2021.3127992.

[19] 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, Feb. 2020, doi: 10.1080/08874417.2020.1712269.

[20] A. A. Cain, M. E. Edwards, and J. D. Still, “An exploratory study of cyber hygiene behaviors and knowledge,” *Journal of Information Security and Applications*, vol. 42, pp. 36–45, Oct. 2018, doi: 10.1016/j.jisa.2018.08.002.

[21] T. Daengsi, P. Pornpongtechavanich, and P. Wuttidittachotti, “Cybersecurity awareness enhancement: a study of the effects of age and gender of thai employees associated with phishing attacks,” *Education and Information Technologies*, vol. 27, no. 4, pp. 4729–4752, Nov. 2021, doi: 10.1007/s10639-021-10806-7.

[22] F. B. Fatokun, S. Hamid, A. Norman, and J. O. Fatokun, “The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian Universities,” *Journal of Physics: Conference Series*, vol. 1339, no. 1, p. 12098, Dec. 2019, doi: 10.1088/1742-6596/1339/1/012098.

[23] A. Adholiya and S. Adholiya, “A study on cyber security practices and tips awareness among e-banking services users of udaipur, Rajasthan,” *International Journal of Scientific Research in Multidisciplinary Studies*, vol. 5, no. 8, 2019.

[24] N. C. Zainal, M. H. M. Puad, and N. F. M. Sani, “Moderating effect of self-efficacy in the relationship between knowledge, attitude and environment behavior of cybersecurity awareness,” *Asian Social Science*, vol. 18, no. 1, p. 55, Dec. 2021, doi: 10.5539/ass.v18n1p55.

[25] C. Banasiński and M. Rojszczak, “Cybersecurity of consumer products against the background of the EU model of cyberspace protection,” *Journal of Cybersecurity*, vol. 7, no. 1, Jan. 2021, doi: 10.1093/cybsec/tyab011.

[26] K. Kioskli, T. Fotis, S. Nifakos, and H. Mouratidis, “The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0,” *Applied Sciences*, vol. 13, no. 6, p. 3410, Mar. 2023, doi: 10.3390/app13063410.

[27] K. Parsons, 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 &amp; Security*, vol. 66, pp. 40–51, May 2017, doi: 10.1016/j.cose.2017.01.004.

[28] Z. Zulkifli, N. N. Abdul Molok, N. H. Abd Rahim, and S. Talib, “Cyber security awareness among secondary school students in Malaysia,” *Journal of Information Systems and Digital Technologies*, vol. 2, no. 2, pp. 28–41, Nov. 2020, doi: 10.31436/jisdt.v2i2.151.

[29] D. S. Kuraku, D. Kalla, and F. Samaah, “Navigating the link between internet user attitudes and cybersecurity awareness in the era of phishing challenges,” *IARJSET*, vol. 9, no. 12, Dec. 2023, doi: 10.17148/iarjset.2022.91224.

[30] R. Paternoster and G. Pogarsky, “Rational choice, agency and thoughtfully reflective decision making: the short and long-term consequences of making good choices,” *Journal of Quantitative Criminology*, vol. 25, no. 2, pp. 103–127, Mar. 2009, doi: 10.1007/s10940-009-9065-y.

[31] A. Vishwanath *et al.*, “Cyber hygiene: the concept, its measure, and its initial tests,” *Decision Support Systems*, vol. 128, p. 113160, Jan. 2020, doi: 10.1016/j.dss.2019.113160.

[32] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, “Determining employee awareness using the Human Aspects of information security questionnaire (HAIS-Q),” *Computers &amp; Security*, vol. 42, pp. 165–176, May 2014, doi: 10.1016/j.cose.2013.12.003.

[33] M. Zaoui and Y. Sadqi, “Toward understanding the impact of demographic factors on cybersecurity awareness in the moroccan context,” in *Artificial Intelligence and Green Computing*, Springer Nature Switzerland, 2023, pp. 207–214.

[34] J. Du, A. Kalafut, and G. Schymik, “Phishing: gender differences in email security perceptions and behaviors,” *Cybersecurity Pedagogy and Practice Journal;*, vol. 3, no. 2, pp. 35–47, 2024, doi: 10.62273/pelx2965.

[35] M. O. Vilceanu and K. Johnson, “Gender and cybersecurity: consumer awareness, experience and trust,” in *Association of Marketing Theory and Practice Proceedings*, 2018, vol. 1, doi: 10.20429/amtp.2018.46.

[36] C. C. Hudson, L. Lambe, D. J. Pepler, and W. M. Craig, “Coping while connected: the association among cybervictimization, privacy settings, and reporting tools in youth,” *Canadian Journal of School Psychology*, vol. 31, no. 1, pp. 3–16, Dec. 2015, doi: 10.1177/0829573515619623.

[37] F. H. Nikel and A. O. Amaechi, “An assessment of employee knowledge, awareness, attitude towards organizational cybersecurity in cameroon,” *Network and Communication Technologies*, vol. 7, no. 1, p. 1, Feb. 2022, doi: 10.5539/nct.v7n1p1.

[38] C. Gerdenitsch, D. Wurhofer, and M. Tscheligi, “Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees’ security behavior,” *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 17, no. 4, Sep. 2023, doi: 10.5817/cp2023-4-7.

[39] D. Van Tran, P. Van Nguyen, D. Vrontis, S. T. N. Nguyen, and P. U. Dinh, “Unraveling influential factors shaping employee cybersecurity behaviors: an empirical investigation of public servants in Vietnam,” *Journal of Asia Business Studies*, vol. 18, no. 6, pp. 1445–1464, Jun. 2024, doi: 10.1108/jabs-01-2024-0058.

[40] D. Van Tran, P. V Nguyen, L. P. Le, and S. T. N. Nguyen, “From awareness to behaviour: understanding cybersecurity compliance in Vietnam,” *International Journal of Organizational Analysis*, vol. 33, no. 1, pp. 209–229, May 2024, doi: 10.1108/ijoa-12-2023-4147.

[41] L. C. de Kok, D. Oosting, and M. Spruit, “The influence of knowledge and attitude on intention to adopt cybersecure behaviour,” *Information &amp; Security: An International Journal*, vol. 46, no. 3, pp. 251–266, 2020, doi: 10.11610/isij.4618.

[42] S. Alotaibi, S. Furnell, and Y. He, “Towards a framework for the personalization of cybersecurity awareness,” in *Human Aspects of Information Security and Assurance*, Springer Nature Switzerland, 2023, pp. 143–153.

[43] T. Chanussot and C. Schürmann, “Cyber awareness training for election staff using constructive alignment,” in *Electronic Voting*, Springer International Publishing, 2021, pp. 63–74.

[44] E. Blancaflor, T. D. Bilbao, V. I. P. Casas, and I. P. Mapue, “A cybersecurity awareness/training system customized for an organizational needs: an e-learning portal,” in *Proceedings of the 2024 15th International Conference on E-business, Management and Economics*, Jul. 2024, pp. 388–394, doi: 10.1145/3691422.3691473.

[45] S. Alahmari, K. Renaud, and I. Omoronyia, “Moving beyond cyber security awareness and training to engendering security knowledge sharing,” *Information Systems and e-Business Management*, vol. 21, no. 1, pp. 123–158, Oct. 2022, doi: 10.1007/s10257-022-00575-2.

[46] A. S. Abdullah and M. Mohd, “Spear phishing simulation in critical sector: telecommunication and defense sub-sector,” in *2019 International Conference on Cybersecurity (ICoCSec)*, Sep. 2019, pp. 26–31, doi: 10.1109/icocsec47621.2019.8970803.

[47] S. Armoogum *et al.*, “A comprehensive review of cyber hygiene practices in the workplace for enhanced digital security,” *JOIV : International Journal on Informatics Visualization*, vol. 9, no. 1, p. 137, Jan. 2025, doi: 10.62527/joiv.9.1.3787.

[48] I. Tikanmäki, T. Blek, J. Niskakangas, and K. Varamäki, “Enhancing cybersecurity in healthcare: the KyberSoTe project’s approach to mitigating cyber threats,” *European Conference on Cyber Warfare and Security*, vol. 24, no. 1, pp. 665–673, Jun. 2025, doi: 10.34190/eccws.24.1.3477.

[49] S. Chaudhary, “Driving behaviour change with cybersecurity awareness,” *Computers &amp; Security*, vol. 142, p. 103858, Jul. 2024, doi: 10.1016/j.cose.2024.103858.

[50] T. Karayel and A. Akbıyık, “Managing cyber security risks and cyber hygiene in organizations: improving cyber resilience,” in *Digital Transformation and Innovation in Emerging Markets*, IGI Global, 2024, pp. 205–226.

BIOGRAPHY OF AUTHORS

Amily Fikry is an Associate Professor in Department of Entrepreneurship and Marketing, Universiti Teknologi MARA, Cawangan, Selangor, Malaysia. She graduated with a Diploma in business studies, UiTM Arau, Perlis, BBA (Hons) marketing, UiTM Shah Alam, Master in business administration (multimedia marketing), Multimedia University Cyberjaya and Ph.D. (consumer behavior) from Universiti Sains Malaysia. Her current research interest is in consumer technology behavior, user experience and digital marketing. She can be contacted at email: amily@uitm.edu.my.

Azreen Joanna Abdul is a senior lecturer in the Department of Entrepreneurship and Marketing, Universiti Teknologi MARA, Cawangan, Selangor, Malaysia. A marketing enthusiast, she hailed from Kuala Lumpur and is a seasoned lecturer with a remarkable 18-year tenure at Universiti Teknologi MARA. An alumna of UiTM Shah Alam, Joanna holds an MBA majoring in marketing, and a BBA (Hons) in marketing, establishing a robust foundation for her illustrious career. Since November 2006, she has been a guiding force at UiTM Puncak Alam, not only as an educator but as a marketing advocate fostering the development of exceptional Bumiputera graduates. Before her academic journey, she served as a Money Market Dealer at Malaysia Discounts Berhad, now MIDF Investment Bank, gaining valuable insights into the financial sector. Joanna's recent achievement of the Chartered Institute of Marketing (CIM) Level 6 Diploma in Professional Digital Marketing, under the Peneraju SPEED scholarship, highlights her commitment to staying abreast of the evolving digital landscape. Currently pursuing Chartered Marketer status from CIM UK, Joanna specializes in consumer behavior, digital marketing, and marketing communications, showcasing her dedication to mastering the nuances of contemporary marketing. She can be contacted at email: azreen890@uitm.edu.my.

Khairul Nazlin Kamaruzaman received Bachelor’s Hons. office systems, Master in office systems and Ph.D. degrees in business and management all from the Universiti Teknologi MARA, Malaysia in 2012, 2013, and 2022 respectively. As a Senior Lecturer with the Department of Entrepreneurship and Marketing Studies, Faculty of Business and Management faculty, Universiti Teknologi MARA, Puncak Alam Campus (specifically for entrepreneurship) focused her research interest on consumer behavior, information technology, entrepreneurship, innovation, and others. She can be contacted at email: khairulnazlin@uitm.edu.my.

Asnawati born in Magelang, Central Java, Indonesia on March 7 1972. Completed undergraduate studies (S1) at the Satya Wacana Christian University, Salatiga, Indonesia, Faculty of Economics, majoring in marketing management in 1997 with an SE (Sarjana Ekonomi) degree. Then continued her Bachelor Degree (S2) at Atmajaya University Yogyakarta, Indonesia, Magister Management Program graduating in 1999 with an MM (Magister Management) degree. She once worked as an account officer at PT. BPR Shinta Daya Yogyakarta, Indonesia (1999-2000). In 2005 she joined the Faculty of Economics and Business, Mulawarman University, Samarinda, Indonesia as a lecturer until now. Books ever written Kewirausahaan, Teori dan Contoh-contoh Rencana Bisnis (CV. Literasi Nusantara, Malang Indonesia, 2021). Analisis Inovasi Produk dan Orientasi Pasar Terhadap Kinerja Pemasaran (CV. Literasi Nusantara, Malang Indonesia, 2022). The last article published in the journal How Real – time Interactivity Influences Impulse Buying Behaviour in Generation Z's During Live Streaming Shopping: The Mediating Role of Perceived Enjoyment (Innovative and Economics Research Journal, Volume 12, No. 3,2024). She joined the Forum Manajemen Indonesia as a member and as a member of the Ikatan Sarjana Ekonomi Indonesia. She can be contacted at email: asnawati@feb.unmul.ac.id.