

TOPLAMA

(Jurnal Komunikasi Dan Pengabdian Masyarakat)

E-ISSN: 3025-2652

<https://altinriset.com/journal/index.php/toplama>

Vol.3, No. 2, Januari 2026

MOBILE SECURITY PRACTICES AMONG MALAYSIAN CITIZENS: A SURVEY OF RISK AWARENESS AND PROTECTIVE BEHAVIORS

Qin Qin^{1*}, Nur Suhaili Mansor², Hapini Awang³, Huda Ibrahim⁴, Adi Permana Sidik⁵

Universiti Utara Malaysia^{1*, 2, 3, 4}

Universitas Sangga Buana YPKP⁵

Email: qin_qin@ahsgs.uum.edu.my^{1*}, nursuhaili@uum.edu.my²,

hapini.awang@uum.edu.my³, huda753@uum.edu.my⁴, adi.permana@usbykpk.ac.id⁵

Abstract

Mobile phones have become an important part of Malaysian youth's daily lives, and as easy as it is to get our hands on a mobile, the growing issues that follow raise alarms for cybersecurity. WordPress site. Although there has been a recent influx of online scam and privacy breach reports, little still exists on how ordinary users perceive mobile security, or if their behaviors are consistent with good risk mitigation practices. This study aims to examine the relationships that exist among mobile security confidence, user practices, and incident experiences with the gender of Malaysian youth. Using an eight-sectioned structured survey as an evaluation instrument, key findings are mainly gleaned from users who report medium levels of confidence in their mobile malware knowledge and overall adoption of protective behaviors such as keeping software updated, only using trusted sources to download apps, and using biometrics. A total of 38.1% of respondents, meanwhile, admitted to previous security incidents largely borne out of the presence of outdated systems and a lack of oversight elements in place for vetting third-party applications. in a rapidly digitizing society. Yet without habitual practice and supportive system design, awareness alone may not be enough.

Keywords: Cyber Threats, Malaysia, Gender Differences, Risk Awareness

Abstrak

Ponsel telah menjadi bagian penting dari kehidupan sehari-hari kaum muda Malaysia, dan meskipun mudah untuk mendapatkan ponsel, masalah yang semakin meningkat yang menyertainya menimbulkan kekhawatiran terkait keamanan siber. Situs WordPress. Meskipun belakangan ini marak laporan penipuan daring dan pelanggaran privasi, masih sedikit yang diketahui mengenai bagaimana pengguna awam memandang keamanan ponsel, atau apakah perilaku mereka sejalan dengan praktik mitigasi risiko yang baik. Penelitian ini bertujuan untuk mengkaji hubungan yang ada antara tingkat kepercayaan terhadap keamanan ponsel, praktik pengguna, dan pengalaman insiden dengan jenis kelamin kaum muda Malaysia. Dengan menggunakan survei terstruktur yang terdiri dari delapan bagian sebagai instrumen evaluasi, temuan utama terutama diperoleh dari pengguna yang melaporkan tingkat kepercayaan sedang terhadap pengetahuan mereka mengenai malware ponsel dan penerapan perilaku perlindungan secara keseluruhan, seperti memperbarui perangkat lunak, hanya menggunakan sumber tepercaya untuk mengunduh aplikasi, dan menggunakan biometrik. Sebanyak 38,1% responden, sementara itu, mengakui pernah mengalami insiden keamanan yang sebagian besar disebabkan oleh sistem yang sudah usang dan kurangnya elemen pengawasan dalam proses verifikasi aplikasi pihak ketiga. Dalam masyarakat yang semakin

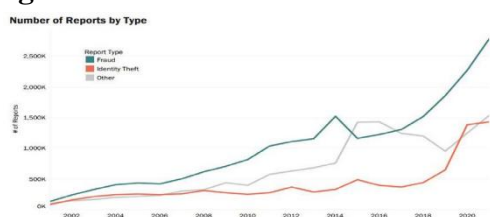
terdigitalisasi. Namun, tanpa praktik rutin dan desain sistem yang mendukung, kesadaran saja mungkin tidak cukup.

Kata Kunci: Ancaman Siber, Malaysia, Perbedaan Gender, Kesadaran Risiko

INTRODUCTION

Rising alongside the global penetration of smartphones, mobile banking services, and digital payments, mobile-driven financial fraud has emerged as a defining cybersecurity concern worldwide (Bwalya & Phiri, 2023). Fraudsters typically combine social engineering tactics, manipulative phishing links, and harmful apps to steal personal data and funds. According to the U.S. Federal Trade Commission (FTC) data in 2021, global fraud losses reached USD 5.9 billion increase of USD 2.4 billion from the previous year, with identity theft accounting for 25% of the reported incidents and imposter scams resulting in direct financial loss for nearly one in five victims (Figure 1).

Figure 1. Total Number of Financial Frauds Reported by FTC from Year 2002 to 2020

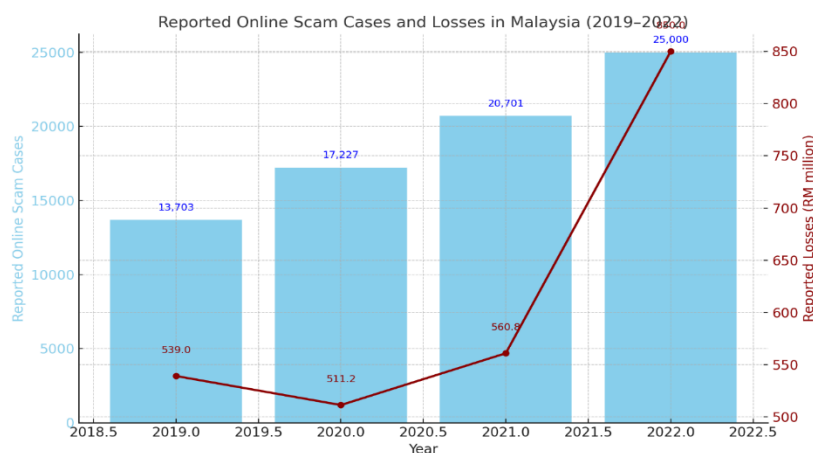


sources: Fraud Prevention Security Center: Fraud Facts

AND STATISTICS.

This global trend finds sharp echoes in Malaysia, where mobile scams have not only grown more common but also far more cunning. Between 2020 and 2022, Malaysians lost over RM5.2 billion to online scams, according to the National Scam Response Centre (David, 2022). From fake investment platforms to phishing links disguised as delivery texts, and rogue APKs slipping in through backdoors, the tactics have grown alarmingly sophisticated (MCMC, 2023). The surge in mobile e-wallets and fintech use has only widened the bullseye. Basyir and Harun (2022) note that scam reports jumped from 13,703 cases in 2019 to more than 25,000 by 2022 - with losses ballooning from RM539 million to RM850 million. (Figure 2) Numbers aside, the message is clear: mobile security in Malaysia is no longer a footnote-it's the frontline.

Figure 2. Reported Online Scam Cases and Losses in Malaysia(2019-2022)

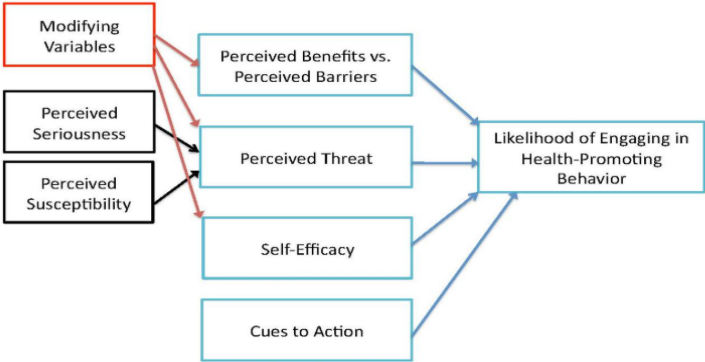


The Health Belief Model (Rosenstock, 1974), see Figure 3: According to this model, people are expected to be more likely to adopt protective behaviors if they think they themselves can contract a disease or if they perceive that the consequences of the threat impact them. In addition, people are more likely to act when they believe that taking a certain action can reduce

the threat effectively and perceive only low barriers to take such action, along with having enough confidence, called self-efficacy, in order to implement the behavior correctly.

Figure 3. The Health Belief Model (Rosenstock, 1974)

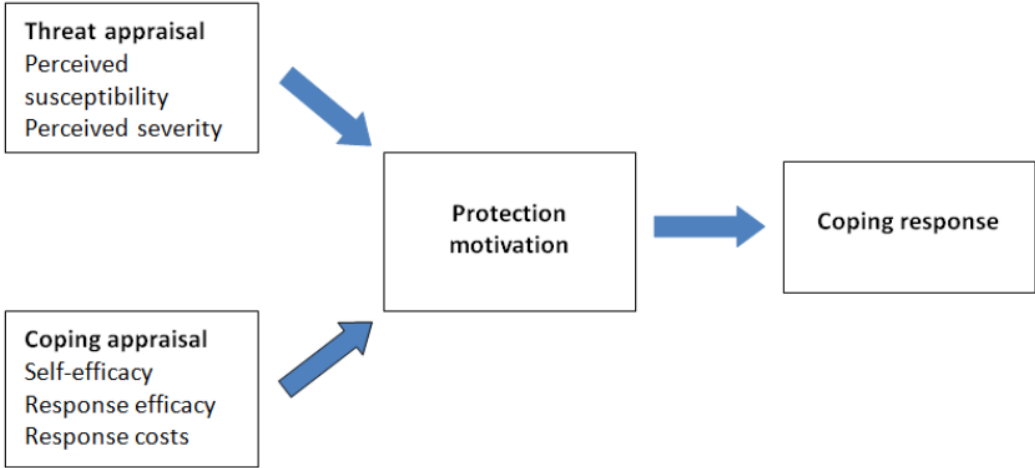
The Health Belief Model



There are a few conceptual alignments that arise in the context of mobile security. Security confidence encompasses self-efficacy individual's confidence in dealing with digital threats. Perceived susceptibility and severity are partially shaped by security awareness (how likely you think it is that a cyberattack will actually happen to you) or previous experience with an incident. On the other hand, behavioral frequency relates to need-blindness because people will engage in protective behavior if it is perceived as useful and multiple cues to action are present (e. We also include gender as a moderator, and examine how risk perceptions and efficacy judgments are homogenized by male or female users, respectively.

The Protection Motivation Theory (Rogers, 1983), seen in Figure 4, provides an expansion of the HBM by incorporating two cognitive processes: threat appraisal and coping appraisal. Threat appraisal includes perceptions of vulnerability to threat and the severity of a potential threat (Yanti et al., 2024), and coping appraisal includes perceived efficacy from a protective response and confidence in capability to respond (Luo et al., 2021).

Figure 4. Protection motivation theory. Adapted from Rogers et al. (1983)



In recent literature on cybersecurity, PMT has been utilised to determine the compliance of users in safeguarding behaviours for password security, app permission control, and two-factor authentication (Zou et al., 2024). Studies demonstrate that self-efficacy and response efficacy are powerful predictors of behaviour, whereas perceived costs or inconvenience may inhibit the motivation to engage in a given action. It is in this context that users who are not only aware of the threat of mobile risks, but also understand their own position to address them, are more likely to continue practising safe behaviours.

While gender plays a significant role in much of the technology adoption or digital literacy research, limited scholarship has zoomed in on gender-based differences in cybersecurity behavior. However, previous studies both in IT use and user psychology have shown that gender can facilitate changes in how people perceive, think about, or act to protect themselves from dangers in the digital world. Women are more likely than men to experience anxiety during technology use, and generally perceive digital systems as less user-friendly, but far more useful (Keyes & Platt, 2024)(Venkatesh & Morris 2000)(Hopcan et al., 2024) .These associations have been further identified with lower levels of technology self-efficacy, less hands-on experience, and decreased confidence in IT-related activities(Morán-Soto & González-Peña, 2022) (Zhou et al., 2023).

Many gendered patterns have been recognized in the cybersecurity context. Studies show that women are more prone to phishing (Lebek et al., 2014)(Jagatic, Johnson, and Jakobsson 2007), and they do much less about password management (Gratian et al. They are also less likely to enact privacy protective behaviors, such as adjusting the settings on security or data sharing (Patel & Doshi, 2022). Ironically as well, women show higher rates of concern for the risks of security on the internet (Debb & McClellan, 2021), which shows a contrast between actual behavior and perceived risk in reality.

The Protection Motivation Theory (PMT) has often been used It refer to the use of this theory to account for these behavioural propensities. PMT, introduced by Rogers, was initially designed to explain health behavior 1975 and posits that threat appraisal, involving perceived severity, vulnerability, and coping responses and is central to the adoption of individual protective actions, response efficacy, self-efficacy, as well as cost-benefit appraisalscaffold decision-making on whether a person should or not adopt any change strategy. Similarly, research that brought the PMT inherent to its application in cybersecurity found these cognitive constructs also ignited protection motivation for punitive action (Sulaiman et al., 2022). Also, social norms--subjective and descriptive types have led to shaping online security behavior, as studied (Ogden, 2023). Nevertheless, the specific manner in which gender fits into these theoretical frameworks is not entirely clear. Gender in the context of cybersecurity. Some studies treat gender as a direct predictor of cybersecurity intentions(Daengsi et al., 2022) while others conceptualize it as an antecedent to psychological constructs like perceived risk, privacy concern, and security efficacy (Alsharida et al., 2023). Gender has also been modeled as a moderator, that is, a construct which influences the strength or direction of relationships between other constructs, such as perceived vulnerability and behavioral intention.

This is especially crucial in seeking to engage young Malaysians- similar to young people globally, they are digital natives but lack digital and cybersecurity awareness across society. Information on where male and female users diverge in their perception of risk, confidence in

response strategies, and real protective behaviors may help inform more targeted awareness campaigns, policy interventions, or digital literacy training. Ergo, this research also aims to discuss how these differences affect mobile security behavior in light of rising cyber threats and dependence on mobiles among young populations.

Several key gaps exist despite the extensive research done on mobile security from both a technical and psychological perspective: First, Malaysian youth-specific behavioral data is lacking. Previous research has either combined age groups or investigated general adult users. Second, while gender differences are frequently recognized, few studies provide quantitative comparisons of male with female users regarding the number of real mobile security incidents. Third, we know very little about the association between behavioral intentions and outcomes (eg, whether bad behavior really leads to more events). This research aims to fill these voids by exploring the youth users' mobile security confidence, their claimed behavior, and their direct experiences with security threats, taking into consideration the signalment of gender.

METHOD

It was essential for the questionnaire to capture different facets of mobile security behavior and perceptions among Malaysian youth. By borrowing from established models, such as the Health Belief Model and Protection Motivation Theory, the instrument emphasized both cognitive and behavioural constructs, specifically perceived risk, self-efficacy, protective actions, and incident experience. As a consequence, the questionnaire was founded on some overarching dimensions:

Threat Scenario: in order to understand the types of security threats that the participants have experienced with mobile. Self-Protective Behavior: This considers metrics like the frequency and consistency of taking actions like updating software, using app permission controls, and clicking on suspicious links. Confidence: a measure of how confident those surveyed feel about securing mobile. Security Awareness provides a measure of overall understanding of the types and best practices of Mobile Security General Knowledge. Tool Adoption and Willingness: Evaluates the utilization of security tools, in addition to interest in implementing further or replacing existing protective systems.

The experience of an incident recognizing instances where the participant has experienced a scam, malware, or any other digital threats fell under this criterion. Demographic and Psychographic Moderators (e.g., gender) to investigate distinct behavioral or experiential aspects. Using a five-point Likert-type scale, most elements of the questionnaire were quantified (i.e., from "Strongly Disagree" to "Strongly Agree" and sometimes even further (e.g., from "Never" to "Always"). On the other hand, more granularity is desired when assessing behavioral incidents taking place in specific items (e.g. Figure 6), serving a seven-point Likert scale from "Never happened" to "Frequently happened". The instrument was prepared in English, and a pilot test was performed for clarity, internal reliability, and cultural relevance among the youth population of Malaysia.

RESULTS AND DISCUSSION

Users' Confidence in Mobile Security and Actual Protective Behaviors

Table 1 presents the results of confidence in protecting the mobile devices against cybersecurity threats among Malaysian youth, and it confirms a sort of carelessly confident attitude. The single largest group of people, 42.8%, ranked their confidence at a middling level (level 3), but

a solid 35.7% expressed low faith in the government or international organizations to protect them (selecting either level one or two). That means a large segment of the online population still either can't or won't address mobile security risks that leave them susceptible to threats ranging from phishing, malware, and unauthorized data access.

Table 1. What is your level of confidence in your ability to protect your mobile device from security threats?

VALID	PERCENT(%)	VALID PERCENT(%)
1	9.5	9.5
2	26.2	26.2
3	42.8	42.8
4	16.7	16.7
5	4.8	4.8
TOTAL	100	100

Strikingly, despite these reservations reportedly perceived Table 2 demonstrates high levels of adoption of a number of protection measures. Fingerprint or facial recognition biometric authentication methods were reportedly in high use, specifically by 80% of female respondents and only 20% of males. This could be to do with convenience as well as an increasing trust in the security that they find within their phones.

Table 2. Which of the following security measures do you use on your mobile device?

GENDER	BIOMETRIC AUTHENTICATION(FINGERPRINT, FACE RECOGNITION, ETC.)	PASSWORD LOCK	TOTAL
Female	80%	54.5%	66.7%
Male	20%	45.5%	33.3%
TOTAL	100%	100%	100%

Yet still, we are not doing well with more fundamental security practices such as creating strong passwords or PINs. Conclusion behavior gap still exists in basic protection strategies-only 54.5% of females said they always use passwords. This backs up previous research, which shows that while perceptions of certain tools are more fashionable among youth (like biometrics), less “fashionable” or user-friendly habits, such as changing passwords every few months and disabling auto-login options, can be overlooked.

That sounds to me like a fairly significant discrepancy between perceived confidence and actual protective behavior. While end users may think they can handle the security of their devices, their behavior, particularly around some core behaviors, does not measure up to this belief. One explanation for this inconsistency could be that adopting a lot of the right practices relies on automated tools or functions of default security in infrastructure, with limited recognition of its limitations. This emphasises the need for policy and educational campaigns in digital literacy, more specifically around password hygiene, app permissions, and spotting phishing attacks. In fact, programs that help bridge the confidence-behavior gap might not only protect them from harm - they could also reduce the security risks faced by this younger cohort of mobile users.

Relationship Between Security Incident Experience and Behavioral Patterns

The results of Tables 3, 4, and 5 illustrate a significant relationship between users’ mobile security behaviors as well as the number of cybersecurity incidents reported by them. Key

among the findings was that 38.1% of respondents reported experiencing at least one type of mobile security incident, which might include phishing attacks, unauthorized access, or malware infections. This subgroup of individuals exhibited markedly different patterns of behavior from users who did not have such experiences.

Table 3. How often do you update your mobile device's operating system and apps?

VALID	PERCENT(%)	VALID PERCENT (%)
1	7.1	7.1
2	9.5	9.5
3	14.3	14.3
4	35.7	35.7
5	11.9	11.9
6	9.5	9.5
7	11.9	11.9
TOTAL	100	100

Table 4. Have you ever experienced a mobile security incident (e.g., malware infection, unauthorized access, data breach)?

VALID	PERCENT (%)	VALID PERCENT (%)
No	61.9	61.9
YES	38.1	38.1
Total	100	100

Table 5. Have you ever downloaded apps from unofficial sources (outside of the official app stores)?

GENDER	NO	YES	TOTOL
FEMALE	69.6%	63.2%	66.7%
MALE	30.4%	36.8%	33.3%
TOTAL	100%	100%	100%

An especially interesting trend that emerged is in the case of system update behavior. The data from those refusing to upgrade the OS of their devices did not look good: 66.7% said that they had run into a security issue at some point in the past. In contrast, the group that continued with periodic updates had a lower rate of occurrence. This is a clear indication that the process of updating software has become slow or ignored, which in turn may be associated with higher susceptibility, as many historical systems are currently not provided with updates for newly detected vulnerabilities (Hong & Furnell, 2021).

It also seems some of the behavioral factors could stem from where the mobile apps are coming from. This was admitted by a good share of users, including males and females, while downloading applications from unofficial places or third-party platforms. Female users actually had slightly higher rates with these types of downloads, but their overall experience was roughly the same as males regarding security incidents. This could suggest that female users tend to engage in compensatory behaviors, such as seeking increased levels of care or protection, but

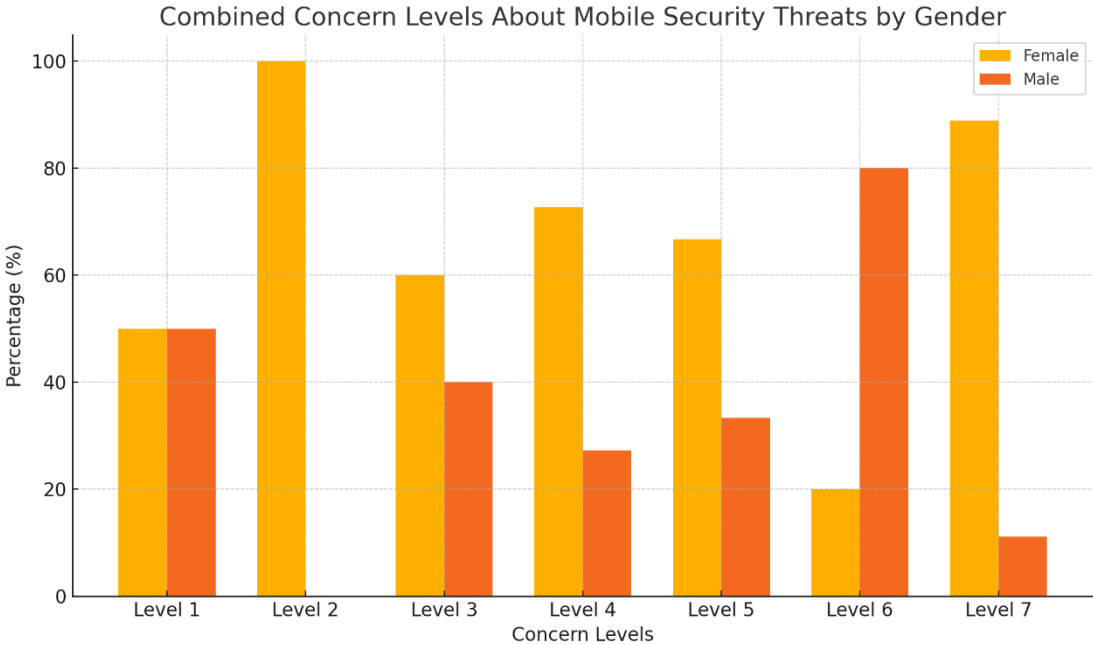
this requires empirical investigation. These behavioural insights support existing literature suggesting that user practices like not updating systems or downloading software from untrusted sources cover major predictors in escalating cybersecurity risk factors (Yadav et al., 2022);(Das et al., 2020;). While neither set of data supports a causal claim, the associational structure suggests that users who are more likely to engage in less secure digital behaviors - such as responding to spam or downloading apps from unknown developers - are also most at risk of experiencing an incident.

These findings have important practical implications regarding the importance of focused behavioral work. Reminder campaigns and in-app prompts should educate users not only about keeping systems up to date, but should also reach to some extent into higher privacy layers by warning against using unauthorized app sources. Real-time risk feedback mechanisms could be embedded into operating systems and app stores to preemptively influence user behavior about safer practices.

Gender-Based Disparities in Security Practices

Whereas the gender gap in mobile security behaviors may be more transparent from a cursory look at the data (Tables 2, 5, and 6), a deeper analysis reveals structural inequalities and discrepancies of practices in digital security between male and female users as well. These differences subtly illuminate more systemic problems beyond just person-specific taste or knowledge.

Figure 6. How concerned are you about the following mobile security threats? (From level1-7)



Noted types include : Mairare attacks, Data beaches, Phishing attempts.. Female users appear more engaged in visible security actions, such as biometric authentication and app permission checks. However, this behavioral engagement often coexists with heightened emotional volatility in perceived risk levels. Notably, female respondents were overrepresented in both low and high ends of the security concern scale (particularly at levels 2 and 6), suggesting a lack of consistent risk calibration. This pattern may reflect broader

societal narratives that associate digital insecurity with anxiety or vulnerability, disproportionately affecting women's psychological framing of mobile threats.

More specifically, female users participated more in visible security actions such as biometric authentication and app permission checks. But this behavioral part of the engagement usually coincides with a greater emotional volatility in risk perception. Females were overrepresented at both low and high ends of the security concern scale (in particular levels 2 and 6), which is indicative of low to no risk calibration. This pattern might be because of the more general societal narratives that associate fear or menace with digital insecurity and consequently, contribute to women's psychological framing of mobile threats.

On the other end, male users display a more functional and less holistic butting strategy, resulting in slightly higher system update frequencies but dramatically lower multi-layered protective method use. By doing so, it promotes the illusion of sufficiency-equating technical maintenance with full security, while ignoring far more subtle elements like app source verification, permission control, or behavioral vigilance. This overconfidence in system defaults means these latent links to high-risk vectors will be obscured.

Most importantly, both groups have serious blind spots. On the other hand, this does not mean that female users are becoming high risk: they are proactive but at the same time using security technologies (eg, biometrics) while knowing almost nothing about backend vulnerabilities or data leakage risks. Because of years spent under-engaging with the aspects of digital safety that are not technical, such as behavior or privacy settings, male users may well underestimate threats.

Also, however, these gendered disparities are not due to ex-natural reasons but rather produced with the design of socio-technical influences, such as gender differences in digital literacy opportunities, societal stereotypes about tech-savviness, or gendered messaging in cybersecurity education. The more troubling implication of these findings, then, is that the current security awareness campaigns are just perpetuating (or further solidifying) such disparities by ignoring them by and large.

Ultimately, it is not just a matter of identifying and describing gendered distinctions in mobile security engagement; we need to deconstruct them and put them into question. In sum, security education and intervention strategies should not stop at the mere adjustment of surface-level behavior; they must address the more fundamental structural, cultural, and psychological mechanisms that can help shed light on why members exhibit behavioral patterns that are difficult to predict.

CONCLUSION

The study explored mobile security behaviors of Malaysian youth across eight targeted survey dimensions and found variations in update practices, app source, protective behaviors, and perceived security confidence. We found that users failed to align perceived security with actual protective behaviors when their prior experiences of security incidents were considered. Female users exhibited behavior associated with higher engagement of protective measures, gender-based patterns-notably-while they were also more likely to follow guidelines, their emotional response to security concerns seemed more fluctuating. On the other side of things, male users

had a slightly higher system update frequency but less engagement with multi-layered protection. These findings point to the necessity of more responsive educational approaches and call into question prevailing assumptions about young people's digital literacy.

Triangulating data from behavior frequency, security incident exposure, and self-reported confidence, the study affirms the need for structural as well as education-based interventions. This includes platform-level protections as well as sensitization campaigns that cater to more than just information gaps, but also how Consistency in behavior is key. The findings demonstrate preliminary evidence to support the development of context-sensitive mobile security education, risk-sensitive system design, and gender-informed policy frameworks. Future research is encouraged to expand the demographic and methodological scope to further refine these insights and translate them into sustainable youth safety programs.

Acknowledgement

The authors appreciate the many individuals who made a contribution to allowing this research to be completed successfully. Special thanks go to Balqis Sofea, Muhammad Syahmi, Mohamad Nur Hakeem, Khairul Aina Safia, and the voice of my life—my friend Nur Iman Maisara for their collaboration, commitment, and insightful thoughts, which heavily contributed to the research. We also thank the staff at Universiti Utara Malaysia for providing an environment conducive to working and resourcing this study. We thank all survey participants who took the time to answer and provide input; we could not have obtained the data for analysis without you

BIBLIOGRAPHY

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, 73, 102258. <https://doi.org/10.1016/j.techsoc.2023.102258>

Bwalya, D., & Phiri, J. (2023). Fraud Detection in Mobile Banking Based on Artificial Intelligence. In R. Silhavy & P. Silhavy (Eds.), *Artificial Intelligence Application in Networks and Systems* (pp. 537–554). Springer International Publishing. https://doi.org/10.1007/978-3-031-35314-7_48

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Education and Information Technologies*, 27(4), 4729–4752. <https://doi.org/10.1007/s10639-021-10806-7>

Debb, S. M., & McClellan, M. K. (2021). Perceived Vulnerability As a Determinant of Increased Risk for Cybersecurity Risk Behavior. *Cyberpsychology, Behavior, and Social Networking*, 24(9), 605–611. <https://doi.org/10.1089/cyber.2021.0043>

Hong, Y., & Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications*, 57, 102710. <https://doi.org/10.1016/j.jisa.2020.102710>

Hopcan, S., Türkmen, G., & Polat, E. (2024). Exploring the artificial intelligence anxiety and machine learning attitudes of teacher candidates. *Education and Information Technologies*,

29(6), 7281–7301. <https://doi.org/10.1007/s10639-023-12086-9>

Keyes, K. M., & Platt, J. M. (2024). Annual Research Review: Sex, gender, and internalizing conditions among adolescents in the 21st century – trends, causes, consequences. *Journal of Child Psychology and Psychiatry*, 65(4), 384–407. <https://doi.org/10.1111/jcpp.13864>

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & H. Breitner, M. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, 37(12), 1049–1092. <https://doi.org/10.1108/MRR-04-2013-0085>

Luo, Y., Wang, G., Li, Y., & Ye, Q. (2021). Examining Protection Motivation and Network Externality Perspective Regarding the Continued Intention to Use M-Health Apps. *International Journal of Environmental Research and Public Health*, 18(11), Article 11. <https://doi.org/10.3390/ijerph18115684>

Morán-Soto, G., & González-Peña, O. I. (2022). Mathematics Anxiety and Self-Efficacy of Mexican Engineering Students: Is There Gender Gap? *Education Sciences*, 12(6), Article 6. <https://doi.org/10.3390/educsci12060391>

Ogden, S. E. (n.d.). CYBERSECURITY: CREATING A CYBERSECURITY CULTURE.

Patel, S., & Doshi, N. (2022). Internet of Behavior in Cybersecurity: Opportunities and Challenges. In P. K. Singh, S. T. Wierzchoń, J. K. Chhabra, & S. Tanwar (Eds.), *Futuristic Trends in Networks and Computing Technologies* (pp. 219–227). Springer Nature. https://doi.org/10.1007/978-981-19-5037-7_14

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information*, 13(9), Article 9. <https://doi.org/10.3390/info13090413>

Yadav, C. S., Singh, J., Yadav, A., Pattanayak, H. S., Kumar, R., Khan, A. A., Haq, M. A., Alhussen, A., & Alharby, S. (2022). Malware Analysis in IoT & Android Systems with Defensive Mechanism. *Electronics*, 11(15), Article 15. <https://doi.org/10.3390/electronics11152354>

Yanti, A., Yani, M., Saputra, I., Zaman, N., & Maulana, T. (2024). An Analysis of Determinants Affecting the Utilization of Integrated Non-Communicable Disease Service Posts (Posbindu PTM) in the Ulee Kareng Public Health Center, Banda Aceh City: A Health Belief Model Approach. *Universal Publication Index E-Library*, 101–127.

Zhou, K. Z., Cao, J., Yuan, X., Weissglass, D. E., Kilhoffer, Z., Sanfilippo, M. R., & Tong, X. (2023). “I’m Not Confident in Debiasing AI Systems Since I Know Too Little”: Teaching AI Creators About Gender Bias Through Hands-on Tutorials (No. arXiv:2309.08121). *arXiv*. <https://doi.org/10.48550/arXiv.2309.08121>

Zou, Y., Le, K., Mayer, P., Acquisti, A., Aviv, A. J., & Schaub, F. (2024). Encouraging Users to Change Breached Passwords Using the Protection Motivation Theory. *ACM Transactions on Computer-Human Interaction*, 31(5), 1–45. <https://doi.org/10.1145/3689432>