International Journal of Education, Psychology and Counseling
EISSN : 0128-164X
IJEPC

**Volume 10 Issue 59 (September 2025) PP. 1002-1008**
**DOI 10.35631/IJEPC.1059072**

International Journal of Education, Psychology and Counseling (IJEPC)

**INTERNATIONAL JOURNAL OF EDUCATION, PSYCHOLOGY AND COUNSELLING (IJEPC)**
www.ijepc.com

GLOBAL ACADEMIC EXCELLENCE

# KNOWLEDGE, ATTITUDE, AND PASSWORD PRACTICES: DETERMINANTS OF CYBERSECURITY AWARENESS AMONG STUDENTS IN MALAYSIAN PUBLIC UNIVERSITIES

Rayyan Cheong Tian Ming[1]*, Nur Haffiza Rahaman[2], Liley Afzani Saidi[3], Wan Su Emi Yusnita Wan Yusof [4], Siti Nurhafizah Saleeza Ramlee[5]

[1] Department of Management, National Defence University of Malaysia
Email: rayyanming@upnm.edu.my
[2] Department of Management, National Defence University of Malaysia
Email: nurhaffiza@upnm.edu.my
[3] Department of Management, National Defence University of Malaysia
Email: liley.afzani@upnm.edu.my
[4] Department of Management, National Defence University of Malaysia
Email: wansuemi@upnm.edu.my
[5] Department of Management, National Defence University of Malaysia
Email: saleeza@upnm.edu.my
* Corresponding Author

**Article Info:**

**Article history:**
Received date: 25.06.2025
Revised date: 23.07.2025
Accepted date: 18.08.2025
Published date: 22.09.2025

**To cite this document:**

Cheong, T. M. R., Rahaman, N. H., Saidi, L. A., Wan Yusof, W. S. E. Y., & Ramlee, S. N. S. (2025). Knowledge, Attitude, and Password Practices: Determinants of Cybersecurity Awareness Among Students in Malaysian Public Universities. *International Journal of Education, Psychology and Counseling, 10* (59), 1002-1008.

**Abstract:**

This conceptual paper explores the determinants of cybersecurity awareness among students at the National Defence University of Malaysia (NDUM), with a focus on three key constructs: cybersecurity knowledge, attitude, and password practices. Cybersecurity threats are increasingly targeting educational institutions, making awareness and secure behavior critical, especially in defense oriented universities. The problem lies in the inconsistent awareness levels across student groups and the lack of a unified approach to address knowledge, behavioral, and attitudinal gaps. This study adopts Protection Motivation Theory (PMT) as the theoretical foundation, integrating threat and coping appraisals to explain students' motivation for protective behavior. A conceptual model is proposed to examine the relationships among the constructs and their collective influence on cybersecurity awareness. The discussion highlights the theoretical contribution of linking cognitive, affective, and behavioral domains under PMT, and the practical implications for policy and curriculum development at NDUM. The paper concludes by recommending future empirical studies to validate and extend the model for broader application in higher education cybersecurity strategies.

**DOI:** 10.35631/IJEPC.1059072

**Keywords:**

Cybersecurity Awareness, Knowledge, Attitude, Password Practices, Public University

## Introduction

Cybersecurity awareness has become a critical concern in modern higher education, particularly within military-affiliated institutions such as the National Defence University of Malaysia (NDUM), where the protection of digital assets holds both academic and national security implications. As students increasingly engage in digital platforms for learning, communication, and data storage, they become potential targets for various cyber threats, including phishing, malware, and identity theft. At NDUM, where cadets and civilian students coexist in a highly structured learning environment, ensuring a strong cybersecurity culture is essential not only to safeguard personal and institutional information but also to uphold operational discipline and national interests. As such, examining the factors that influence cybersecurity awareness, specifically knowledge, attitude, and password practices, is vital for supporting cyber resilient behavior among NDUM students.

Previous research has emphasized that cybersecurity knowledge alone is insufficient to ensure safe digital conduct. Studies across different contexts have shown that awareness must be supported by proactive attitudes and consistent security behaviors. For instance, Alotaibi & Almagwashi (2022) discovered that while students are aware of basic cybersecurity threats, their actual practices, especially related to password hygiene, remain poor. Ismail et al. (2023) similarly noted that Malaysian students often demonstrate weak password habits despite general familiarity with cybersecurity concepts. At NDUM, where a military culture emphasizes discipline and structured routines, it is important to understand whether these institutional values are reflected in cybersecurity behavior across different academic backgrounds. However, most existing research tends to focus on civilian universities or ICT specific student populations, leaving a opportunity to further understand how cybersecurity awareness manifests in a defence university setting.

This study aims to fill that gap by examining the determinants of cybersecurity awareness among NDUM students, taking into account the unique academic-military environment. Although NDUM maintains a robust digital infrastructure, the diversity of student backgrounds ranging from technical to non-technical disciplines poses challenges in ensuring uniform cybersecurity awareness. Password practices, often overlooked despite their significance, deserve particular attention due to their role in identity protection and system access control (Madzlan et al., 2022). As cyber threats targeting educational institutions grow more complex and persistent (ENISA, 2023), it becomes increasingly important to develop empirical, context specific strategies that consider how knowledge, attitude, and password behaviors influence student readiness and resilience in cyber environments. This research will contribute to improved institutional policy and awareness programs tailored to the strategic needs of NDUM.

## Problem Statement

Ideally, students at the National Defence University of Malaysia (NDUM) should demonstrate a high level of cybersecurity awareness that aligns with the university's role as both an academic institution and a contributor to national defense. This includes the ability to recognize cyber threats, maintain secure online behavior, and apply good digital hygiene practices such as creating strong passwords and avoiding risky online interactions. NDUM's structured and disciplined learning environment is expected to promote responsible digital conduct, where both cadet officers and civilian students are equally trained to navigate cybersecurity risks with competence and accountability (Cheng et al., 2021). When knowledge, attitude, and practices are well aligned, the university community becomes better protected against unauthorized access and information breaches.

In reality, the level of cybersecurity awareness among NDUM students is not yet uniformly developed across different cohorts and academic streams. Research has shown that while many students are aware of common cybersecurity concepts, their actual behaviors do not always align with safe digital practices (Ismail et al., 2023). Password reuse, over-reliance on simple passwords, and low engagement in two-factor authentication are still widely reported, even in structured institutions (Madzlan et al., 2022). Furthermore, some students may display indifferent or passive attitudes towards cybersecurity, particularly those in non-technical faculties. Although NDUM promotes discipline, cybersecurity training is not yet systematically integrated across all academic programs. The focus remains more prominent in ICT and technical modules, leaving gaps in cybersecurity literacy among other students (Ramli et al., 2020).

Therefore, the inconsistency between knowledge, attitude, and secure practices places NDUM at risk of internal cyber vulnerabilities that could compromise both academic operations and sensitive data related to military training and research. This disconnect can weaken institutional resilience and undermine efforts to build a strong cybersecurity culture among future leaders in national defense. Without a comprehensive understanding of what shapes cybersecurity awareness at NDUM, institutional interventions may fail to address the root causes of unsafe behavior. Moreover, generic awareness campaigns may not resonate with the unique demands and structure of a defense university. Therefore, this study seeks to identify the specific roles that knowledge, attitude, and password practices play in influencing cybersecurity awareness at NDUM, ultimately contributing to more effective, targeted, and defense aligned cybersecurity strategies.

## Literature Review

Cybersecurity awareness among university students is shaped by a combination of knowledge, attitudes, and behavioral practices, particularly regarding password management. Studies in Malaysian higher learning institutions highlight that awareness is multidimensional, encompassing knowledge of threats, attitudes towards security, and actual practices such as password usage and social media behavior(Ramakrishnan et al., 2022; Raju et al., 2022; Kamalulail et al., 2022). Research consistently finds that knowledge especially about password security is a significant determinant of overall cybersecurity awareness. For example, password security knowledge has been shown to significantly influence students' awareness and ability to protect themselves online, with statistical analyses confirming its predictive value (Alqahtani, 2022; ; Kamalulail et al., 2022). However, while students may possess basic knowledge of cybersecurity, gaps remain in their understanding of cyber ethics and the practical application of secure behaviors, indicating a need for more comprehensive educational interventions (Raju et al., 2022).

Attitudes towards cybersecurity and the translation of knowledge into practice are critical for effective cyber risk mitigation. Attitudinal factors, such as the perceived importance of cybersecurity and personal responsibility, interact with knowledge to shape behaviors like password management and safe browsing (Ramakrishnan et al., 2022; Kamalulail et al., 2022). Some studies report that while students recognize the importance of cybersecurity, their actual practices such as creating strong passwords or avoiding risky online behaviors do not always align with their knowledge or attitudes (Raju et al., 2022). Gender, age, and environmental factors appear to have limited influence, with knowledge emerging as the primary differentiator in cybersecurity awareness among Malaysian university students (Kamalulail et al., 2022). Furthermore, the lack of standardized cybersecurity policies and structured support systems in higher education institutions may contribute to inconsistent practices and awareness levels (Ramakrishnan et al., 2022; Khoo et al., 2025).

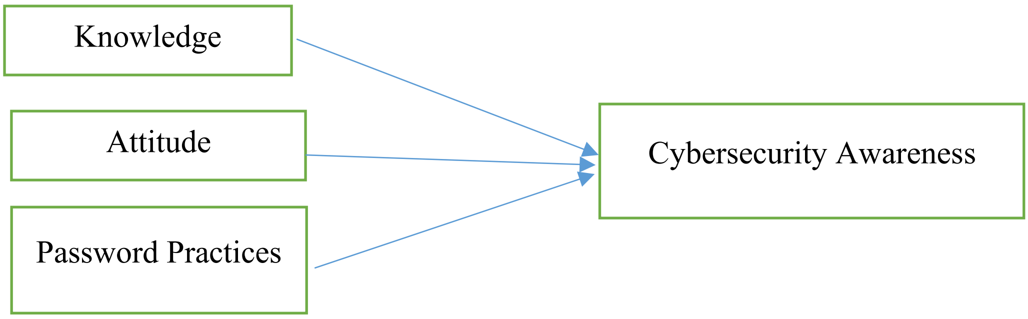
## Theoretical Frameworks: Protection Motivation Theory (PMT)

This study applies Protection Motivation Theory (PMT) as the underlying theoretical framework to explain how students at NDUM assess cyber threats and decide whether to engage in protective behaviors. PMT, developed by Rogers (1975) and later refined for health and digital behavior contexts, posits that individuals form protective intentions based on two cognitive appraisals: *threat appraisal* and *coping appraisal* (Rogers & Prentice-Dunn, 1997). PMT provides a useful lens for understanding how knowledge, attitudes, and practices interact to influence cybersecurity awareness. PMT posits that individuals' motivation to protect themselves is driven by their appraisal of threats (perceived severity and vulnerability) and their belief in the efficacy of protective behaviors (response efficacy and self-efficacy). In the context of Malaysian public universities, students' knowledge of password security and cyber threats increases their perceived vulnerability and severity, while positive attitudes and confidence in their ability to implement secure practices (such as using strong passwords) enhance their motivation to adopt protective behaviors(Alqahtani, 2022; Ramakrishnan et al., 2022; , Xiang & Hasbullah, 2023; Adeshola & Oluwajana, 2024). Empirical findings support the relevance of PMT, as educational interventions that target both knowledge and attitudes while fostering practical skills are shown to improve cybersecurity awareness and reduce risky behaviors among students (Xiang & Hasbullah, 2023; Adeshola & Oluwajana, 2024). Ongoing education, advocacy, and the integration of cybersecurity into university curricula are recommended to sustain and enhance awareness levels (Ramakrishnan et al., 2022; Xiang &Hasbullah,2023; Raju et al., 2022; Kamalulail et al., 2022).

## Proposed Model

Based on the conceptual background and the Protection Motivation Theory (PMT), this study proposes a model that links cybersecurity knowledge, attitude, and password practices to cybersecurity awareness among university students. The model assumes that knowledge and attitude influence the motivation to adopt cybersecurity behaviors, which are reflected in password practices. These three variables together are proposed to determine the level of cybersecurity awareness among students at NDUM.

The model integrates threat appraisal (linked to cybersecurity knowledge) and coping appraisal (linked to attitude and behavior). PMT suggests that individuals who perceive a high level of threat and believe in their ability to cope effectively are more likely to engage in protective behavior. Therefore, knowledge provides students with the understanding necessary to recognize risks (threat appraisal), while attitude shapes their belief in the benefits and feasibility of taking action (coping appraisal). Password practices, as observable behavior, are used as a measure of coping action and indicate the practical application of both cognitive and attitudinal factors.



## Discussion and Implications

The proposed conceptual model, grounded in Protection Motivation Theory (PMT), offers important insights into how cybersecurity awareness can be understood and strengthened among students at the National Defence University of Malaysia (NDUM). As a unique institution that blends military discipline with academic education, NDUM presents a distinct environment where cybersecurity readiness is not only an academic requirement but also a national defense priority. The integration of knowledge, attitude, and password practices in this framework reflects a comprehensive approach that aligns well with the university's structured and high responsibility learning culture.

From a theoretical perspective, this model addresses key gaps in the literature by examining the interaction between cognitive (knowledge), affective (attitude), and behavioral (password practices) factors. Existing studies have often treated these elements in isolation or focused narrowly on knowledge alone. By aligning them under PMT, this study emphasizes that cybersecurity awareness does not emerge from knowledge in isolation but requires the motivation to act, shaped by how individuals perceive threats and their confidence in managing those threats (Rogers & Prentice-Dunn, 1997; Cheng et al., 2021). For NDUM students, this is particularly relevant, as discipline, accountability, and operational security are values embedded in their training.

Practically, the findings and propositions of this conceptual model can inform curriculum design, cybersecurity policy, and student training at NDUM. For example, cybersecurity awareness programs should not only deliver technical content but also shape positive attitudes through real-life scenarios, simulations, and case studies that demonstrate consequences of poor digital practices. Furthermore, password hygiene, a commonly neglected behavior should be emphasized with practical guidelines and monitoring tools. By embedding cybersecurity principles across all academic faculties, rather than limiting them to ICT-related courses, NDUM can foster an inclusive and campus-wide cybersecurity culture.

In addition, this model provides a foundation for future empirical research. Quantitative studies can be conducted to test the strength of the proposed relationships across different student groups (e.g., cadets vs. civilian students, technical vs. non-technical disciplines). Qualitative methods such as focus group discussions may also help explore deeper perceptions and cultural attitudes that influence behavior in this hybrid military-academic environment. By validating and refining the model through further research, NDUM and other military universities can adopt a more evidence-based and contextually relevant approach to developing cyber-resilient graduates.

## Conclusion

This conceptual paper proposes a structured model to examine how cybersecurity knowledge, attitude, and password practices influence cybersecurity awareness among students at the National Defence University of Malaysia (NDUM). By adopting Protection Motivation Theory (PMT) as the theoretical foundation, the study highlights the importance of both threat appraisal and coping appraisal in shaping students' motivation to engage in safe digital behavior. In the context of NDUM, where students are trained for leadership roles in both military and civilian sectors, understanding these determinants is essential to building a proactive and resilient cybersecurity culture.

The model contributes to the literature by integrating three commonly discussed but often separately analyzed constructs, knowledge, attitude, and behavior, into a unified framework. It emphasizes that awareness is not merely the outcome of technical knowledge but also depends on psychological and behavioral readiness to act upon that knowledge. Furthermore, the emphasis on password practices as a key behavioral outcome adds practical value to the model, particularly for institutions where secure access to sensitive systems is critical.

This paper offers significant implications for education and policy. At NDUM, cybersecurity training should be expanded beyond ICT programs to ensure inclusivity and wider impact. Attitudinal change, hands on behavioral training, and context-specific awareness strategies are recommended to enhance the effectiveness of current initiatives. Future empirical studies may validate the proposed model using a combination of quantitative and qualitative methods, helping to refine theory and inform practice across other defense and higher learning institutions in Malaysia and beyond.

## Acknowledgements

The authors would like to acknowledge and extend special gratitude to the Department of Management, National Defence University of Malaysia.

## References

Adeshola, I., & Oluwajana, D. (2024). Assessing cybersecurity awareness among university students: Implications for educational interventions. *Journal of Computers in Education*.

Alam, M. A., Iqbal, R., & Islam, M. S. (2021). A cybersecurity awareness framework for university students in developing nations: A case study from Bangladesh. *Information, 12*(10), 417.

Alotaibi, M., & Almagwashi, H. (2022). Cybersecurity awareness among university students: Knowledge, attitude, and practices. *Journal of Cybersecurity and Information Management, 6*(2), 103–117.

Alqahtani, M. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*.

Asiyai, R. I., & Ugwu, R. (2021). University students' perception of cybersecurity practices and risks in digital learning environments. *Journal of Education and e-Learning Research, 8*(2), 203–210.

Aziz, A. A., & Hashim, H. (2023). Knowledge, attitude, and practices towards internet safety and security among Generation Z in Malaysia: A conceptual paper. *International Journal of Academic Research in Business and Social Sciences, 13*(1), 115–123.

Cheng, Y., Li, J., & Zhou, Z. (2021). Improving cybersecurity awareness among university students: A review of recent strategies and methods. *Education and Information Technologies, 26*(5), 5917–5936.

ENISA. (2023). *Cybersecurity threat landscape for education*. European Union Agency for Cybersecurity.

Ismail, R., Zakaria, R., & Hassan, S. (2023). Cybersecurity awareness and password management practices among university students in Malaysia. *Malaysian Journal of Computing, 8*(1), 88–99.

Kamalulail, A., Razak, N., Omar, S., & Yusof, N. (2022). Awareness of cybersecurity: A case study in UiTM Negeri Sembilan Branch, Seremban Campus. *e-Academia Journal*.

Khamkanya, T., & Woraphiphat, W. (2023). Bridging the gap: How knowledge, attitudes, and practices shape cybersecurity awareness in Thai education. *Educational Process: International Journal, 12*(2), 45–60.

Khan, M. A., Yu, Z., & Majeed, A. (2023). Investigating cybersecurity challenges and risk mitigation in higher education institutions. *Journal of Cybersecurity and Privacy, 3*(1), 112–130.

Khoo, L., Yatim, M., & Wong, Y. (2025). Research on Capture the Flag exercises for cybersecurity skill training among Malaysian undergraduates. *Journal of Human Centered Technology*.

Lim, R. J., & Rahman, R. A. (2023). A qualitative approach of KAP model against online scam in Malaysia. *Journal of Social Science Advancement, 4*(2), 55–67.

Madzlan, M. R., Hamzah, N., & Wahid, A. (2022). Assessment of password hygiene practices among Malaysian undergraduate students. *International Journal of Cyber Research and Education, 4*(2), 45–56.

Mohamed, A. A., & Musa, N. M. (2022). Cyber hygiene and password practices among Malaysian undergraduates: A case study of a public university. *Journal of Southeast Asian Studies, 27*(3), 241–254.

Raju, R., Hidayah, N., Rahman, A., & Ahmad, A. (2022). Cybersecurity awareness in using digital platforms among students in a higher learning institution. *Asian Journal of University Education*.

Ramakrishnan, K., Yasin, N., & Periasamy, J. (2022). Digital divide on cybersecurity awareness among the Malaysian higher learning institution students. In *The 5th Innovation and Analytics Conference & Exhibition (IACE 2021)*.

Ramli, M. F., Zolkepli, I. A., & Hassan, S. (2020). A study on cybersecurity awareness and behavior among students in Malaysian public universities. *Journal of Information Systems and Digital Technologies, 2*(1), 56–64.

Xiang, C. S., & Hasbullah, M. (2023). Cybersecurity awareness, cyber human values and cyberbullying among university students in Selangor, Malaysia. *International Journal of Advanced Research in Technology and Innovation, 5*(2), 1–11.