FACTORS AFFECTING CYBERSECURITY RISK BEHAVIOUR AMONG MALAYSIAN PAYTECH USERS: THE MODERATING ROLE OF TRUST

NOORHIDAYAH BINTI SALEHHUDIN [1*], AMIRAH BINTI AHMAD SUKI [2], FATIN HUSNA BINTI SUIB [3], ZULKULY BINTI RAMLY [4]

[123]Department of Business Administration,International Islamic University Malaysia, Kuala Lumpur, Malaysia
[4]Department of Finance, International Islamic University Malaysia, Kuala Lumpur, Malaysia

**Corresponding author: cphidayah@gmail.com*

ABSTRACT: The increased uptake of financial technology (FinTech) and digital payment platforms has heightened the importance of investigating the cybersecurity risk behaviour of users. The research focuses on analysing the role of essential constructs from the Unified Theory of Acceptance and Use of Technology (UTAUT) in eliciting cybersecurity risk behaviour among PayTech users in Malaysia, with an emphasis on the moderator of trust. A structured, self-administered survey was employed as a quantitative research design, targeting online payment system users aged 18 to 65 years who actively use this system. Hypothesized relationships were tested using Structural Equation Modeling (SEM). Results show that performance expectancy and effort expectancy have a significant effect on cybersecurity behaviour, but social influence and facilitating conditions are minor predictors of that behaviour. Trust was identified as mediating between several relationships, highlighting its importance in influencing user behaviour. The results provide empirical evidence on the determinants of secure online transaction behavior and will guide policymakers, developers, and financial institutions in improving system usability, user trust building, and the adoption of safer digital financial services.

KEY WORDS: *Paytech, Fintech, Cybersecurity, Behaviour, Risk*

1. INTRODUCTION

In the rapidly evolving digital landscape, financial technology (fintech) has arisen as a revolutionary entity, altering how individuals and enterprises oversee their financial matters. As a center of innovation and economic development, Malaysia has experienced a notable increase in the use and integration of financial technology within its financial ecosystem (Haridan et al., 2020; Shaikh et al., 2020). As “FinTech” refers to using technology platforms and mobile devices to facilitate financial transactions, access banking information, and leverage innovative financing modes such as e-financing and mobile banking (Shaikh et al., 2020). The fintech industry in Malaysia has become the center of the world financial ecosystem, with more than 549 Islamic fintech companies now contributing to a significant portion of the national economy (Santosdiaz, 2024). Meanwhile, mobile banking,

digital wallets, and blockchain are rapidly being adopted, which is why it have become a new wave of payment technology (PayTech) under financial technology, which now serves as a driving force behind financial inclusion (Shaikh et al., 2020; Napis and Daud, 2023). Nevertheless, even the innovations that increase the access present new security dilemmas. The cybercrime issue, such as phishing and malware, as well as the breach of data, has spread to a new level, and an overwhelming majority of cases of cybercrime in the future are likely to be associated with fraud (MyCERT, 2024). The governance measures have been unable to check these tendencies, implying that the scourge is more entrenched in the user behaviours and not necessarily in policy.

Studies indicate that there are a variety of behavioural factors that drive vulnerability: lack of understanding of cybersecurity and overconfidence in technology, peer pressure, and blind use of online resources (Kamalulail et al., 2022; Goddard et al., 2014; Kim et al., 2018). It has been empirically proved that users with limited security literacy or overconfidence are targeted by the cyber threats disproportionately (Parsons et al., 2017; Hadlington, 2018). Since PayTech is experiencing unprecedented growth and the related increase in cyber threats, it is urgent to unravel the factors of risky cybersecurity behaviour and to study the effects of trust on mitigating these relationships. This study can play a vital role in creating targeted recommendations to enhance user awareness, mitigate vulnerabilities, and enhance the integrity of Malaysia's digital financial ecosystem.

This study seeks to:

1. To examine the effect of performance expectancy, effort expectancy, social influence, facilitating conditions, and perceived risk on cybersecurity risk behaviour among Malaysian PayTech users.
2. To examine the direct effect of trust on cybersecurity risk behaviour.
3. To examine the moderating role of trust on the relationships between performance expectancy, effort expectancy, social influence, facilitating conditions, and perceived risk on cybersecurity risk behaviour.

2. PROBLEM STATEMENT

The fintech industry is pivotal in the Malaysian economy, contributing to sustainable economic growth and financial innovation. Despite several steps by the government to address cybercrime issues, the number of cybersecurity incidents in Malaysia keeps increasing due to the revolution that keeps changing (Rahim et al., 2024). Based on the increase in the number of incidents reported in figure 2, it has shown that government strategies and policies cannot efficiently solve the issues.

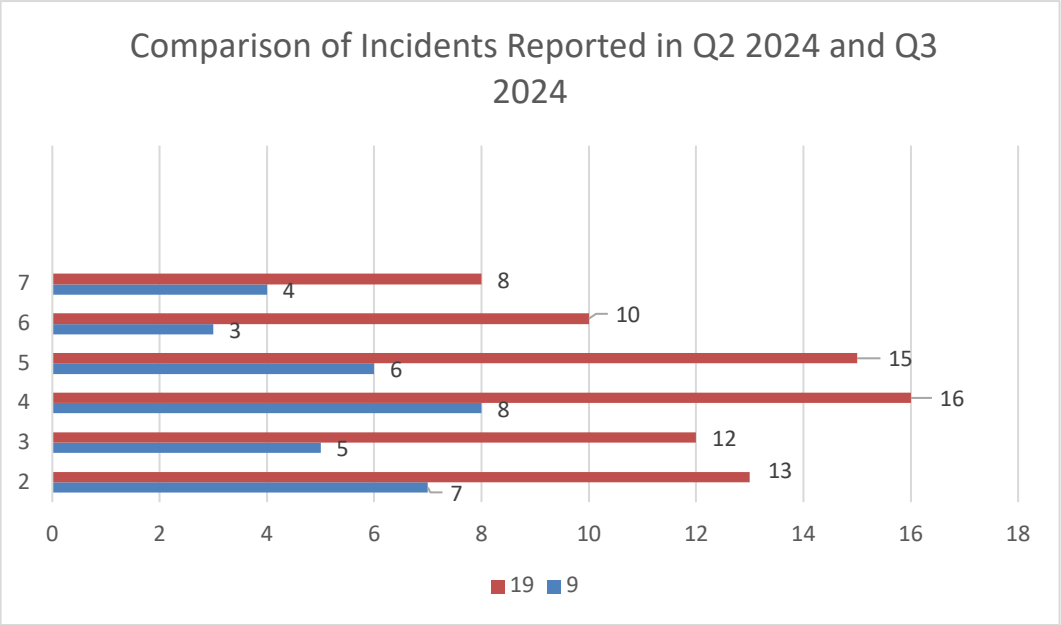

Fig. 1. Cybersecurity Malaysia's comparison of Incidents Reported in Q2 and Q3 2024.

Whereby, according to Figure 1, four categories of events (Denial of Service, Intrusion, Intrusion Attempts, and Spam) were reported to have risen in Q2 2024 relative to Q1 2024, while another four categories (Vulnerabilities et al.) have declined. In the second quarter of 2024, fraud constituted the predominant incident, accounting for 63.94% of all recorded incidents. Subsequently, there are malicious software (11.01%) and data breaches (7.90%). According to prevailing patterns, fraudulent activities will increase in Malaysia in 2024. Simultaneously, for fraud incidents excluding phishing URLs, innovative strategies and methodologies in online scams that amalgamate social engineering and malicious code may persistently proliferate in Malaysian cyberspace (mycert, 2024). Diyana and Shazwani (2018) on phishing threats, provided a real case in Malaysia.

In November 2017, a young woman was scammed by a phisher that forged an e-mail from the Inland Revenue Board of Malaysia (IRBM) asking for her CIMB bank account password, username, and Transaction Authorization Code (TAC), which led to an unauthorised money withdrawal from her account. Phishing is a form of fraud that is used to trick victims into giving their personal information, which includes sensitive passwords and usernames of their accounts. Diyana and Shazwani (2018) revealed that about 97% of users around the globe are unable to identify phishing attacks. Therefore, , the problem statement underscores the need to investigate the various elements influencing cybersecurity risk behaviour, particularly among Malaysian PayTech users, with a specific focus on the mediating role of security knowledge and the moderating impact of trust. This analysis is crucial for developing targeted tactics that enhance user awareness and promote safer cybersecurity practices within the growing PayTech sector.

3. LITERATURE REVIEW

The Unified Technology Acceptance and Use Theory (UTAUT) which were built on the earlier models like the Technology Acceptance Model (Davis, 1989) and later enhanced to UTAUT 2 (Venkatesh et al., 2012), is one of the fundamental theories explaining the process through which people adopt and use technology. As the digital landscape continues to evolve, thorough knowledge of the determinants of cybersecurity risk behaviour has taken on great importance, given that behaviour encapsulates the actions and attitudes of users towards protecting their digital assets. Anchored in the Unified Theory of Acceptance and Use of Technology (UTAUT), a collection of antecedent studies leads to the conclusion that performance expectancy, effort expectancy, social influence, facilitating conditions, perceived risk, and trust interact in a synergistic manner to influence cybersecurity-related decision-making. Performance expectancy is one of the main determinants, as people will show an increased tendency to use cybersecurity measures when they perceive the technological tools to be effective in enhancing performance and protecting information, a phenomenon that has been well-documented in the context of digital finance and new technology areas (Venkatesh et al., 2016; Kaur et al., 2025).The influence of performance expectancy is also enhanced by effort expectancy; the ease by which cybersecurity tools are perceived to be easy to use enhances adoption intentions, thereby reducing psychological and practical obstacles to protective behaviour (Wang et al., 2008; Kumar et al., 2020).

Social influence, in turn, strengthens these relationships, as users often adjust their cybersecurity practices based on the expectations and behaviour of salient others, consequently normalising and promoting secure digital behaviour within socio-professional networks (Alalwan et al., 2017; Chen & Barnes, 2007).Notwithstanding these antecedents, the translation of intention into concrete cybersecurity behaviour is nevertheless highly contingent upon the facilitation of conditions such as adequate technical infrastructure, organisational endorsement, and access to relevant resources that collectively empower users to engage productively with security technologies (Abd-Allawari et al., 2020; Kaur et al., 2025). Despite the existence of enabling conditions, perceived risk remains a key and potentially inhibiting factor, in which high levels of concern about privacy and security breaches and potential losses can undermine the willingness of users to adopt digital solutions.

In this context, trust takes on a pivotal moderating function by reducing the harmful effects of perceived risk by reducing uncertainty and strengthening the confidence of users in cybersecurity technologies. Trust, with its informational elements of reliability, security, and reputation has been shown to empirically foster more favourable attitudes and behavioural intentions in a variety of situations, such as online banking, e-commerce, and telehealth (Casalo et al., 2007; Kumar et al., 2020; AlMojaibel, 2025). Importantly, empirical findings suggest that trust is a crucial bridging agent that helps users reach a position of reconciling their risk perceptions with anticipated benefits from their technology utilisation (Choudhury et al., 2025).

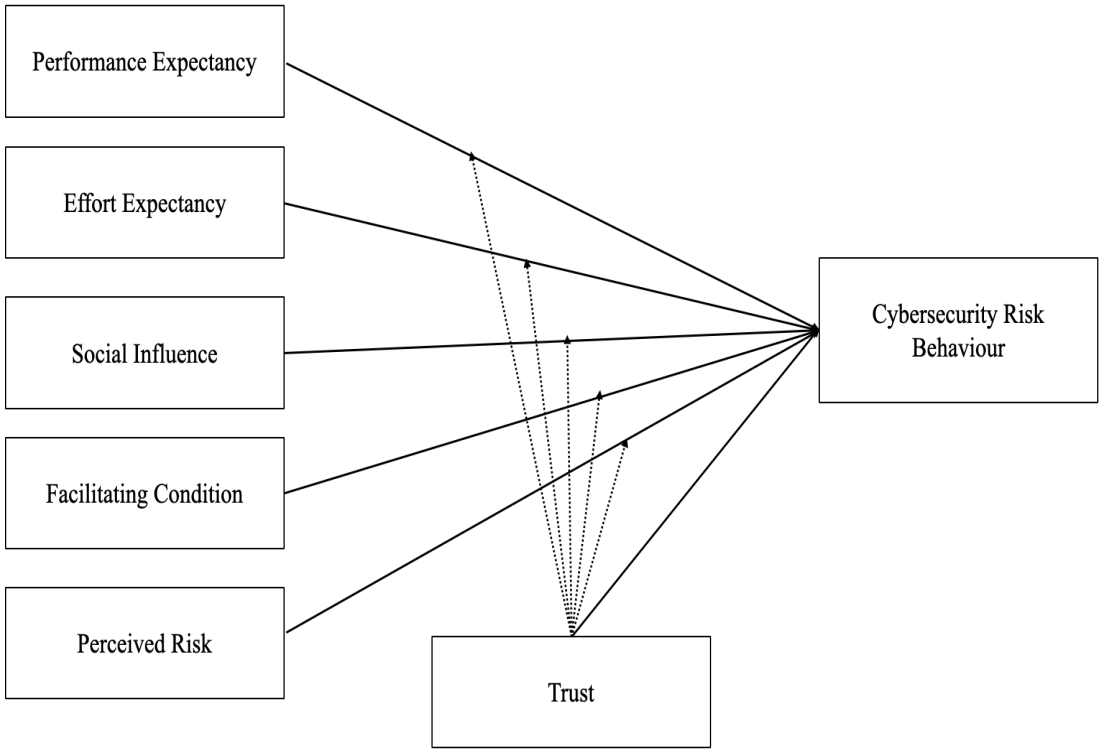

Fig. 2. Theoretical Framework

4. METHODOLOGY

4.1. Research Design

Research design is a comprehensive methodological system by which a study is more or less guided. It specifies the process of data gathering and the methods of analyzing information used to present and prove hypotheses or answer research questions. The strongly designed design is essential in providing the validity and reliability of the empirical studies. This type of design allows studying phenomena in a systematic way, creates critical mental activity, and provides substantive conclusions by using statistical models and analytical procedures to achieve pre-established goals (N. Salkind et al., 2019). A survey instrument to measure self-reported cybersecurity behaviours was created by Kennison and Chan-Tin (2020) and its relationship with personality traits and other personal characteristics was investigated. Similarly, Antunes et al. (2021) have also used two questionnaires to assess cybersecurity risky attitudes and behavior in high-school students. More recently, Tempestini et al. (2023) developed the Cybersecurity Awareness Inventory (CAIN) to measure the cybersecurity knowledge of the users and its relationship with behavioral practices. The current research thus takes a quantitative design, which was considered to be important to examine the determinants of cybersecurity risk behavior among Malaysian PayTech users (Guba & Lincoln, 1994; Sekaran and Bougie, 2016). The cross-sectional design is used in which self-administered questionnaires are used to gather standardized data at one point in time. This model allows studying the correlation between important constructs (Sekaran, 2010; Salkind et al., 2019).

4.2. Population of the study

According to Bryman and Bell (2007), population is the unit over which the samples are taken. It is made up of all the elements that constitute a sample that can be social groupings, organisations, communities, schools, students, states or any other common feature. The target group in the current research is residents of Malaysia who use PayTech, which is a general concept used to define various digital payment tools, including peer-to-peer (P2P) networks, mobile wallets, and other fintech solutions.

Whereas, according to Sekaran (2003), population is defined as a set of all conceivable individuals, objects or measurements of interest of concern. Bank Negara Malaysia (BNM) has indicated that the age at which one may open bank account and online banking account is usually 18 years, in accordance with legal definition of adulthood in Malaysia. As a result, the study focuses on people aged 18-65 that use different FinTech services, which include mobile banking, e-wallets, online investment services and PayTech. According to the statistics provided by the Department of Statistics Malaysia (2023), the number of residents in this age group is estimated at between 23 and 23 million people. Moreover, according to Amanda (2024), there were more than 17 million mobile wallets users in Malaysia in 2022, which is almost one and a half more than in 2021 and a sign that cashless payment technologies are becoming popular in the country.

4.3. Sample size

G*Power was used to calculate the sample size of 103 based on linear regression model with six predictors and an alpha of 0.05 and a statistical power of 0.80 (Erdfelder, Faul, & Buchner, 1996). Data collected using structured questionnaires was used to obtain data of the study variables by ensuring the reliability of data measuremeht, to facilitate testing of the hypothesis.

4.4. Data Collection

This research study involved the use of a structured self-administered questionnaire to gather the data. The questionnaire approach method has been chosen by the researchers to determine necessary information and to define parameters of measurement of the variables of interest as outlined by Sekaran (2010). The strengths associated with the questionnaire method involve ease of establishment of a rapport with the respondents and a sense of a motivational factor to fill in the instrument. In addition, use of questionnaires allows the researcher to interact with the respondents and to clarify any remaining ambiguities concerning the survey questions. This study has embraced a primary data method. Primary data refers to data that is collected at the point of origin in relation to the variable of interest in the case of the particular research (Sekaran, 2010). In this regard, such data are obtained with the help of the questionnaire. The survey will be distributed to the relevant PayTech users in Malaysia.

4.5. Data Analysis

Smart-PLS 4.0 was employed to analyse the collected data using Partial Least Squares Structural Equation Modeling (PLS-SEM), a robust statistical technique suitable for examining complex relationships among multiple variables, including latent constructs measured through observed indicators. Prior to analysis, the survey data were edited, coded, and classified, and descriptive analyses were conducted using IBM SPSS version 30. PLS-SEM was then applied to assess the predictive power of the structural model and the relationships between constructs, as it enables simultaneous evaluation of the measurement and structural models. Consistent with Anderson and Gerbing (1988), integrating both models provides a comprehensive and confirmatory assessment of construct validity and theoretical relationships. Previous studies have demonstrated the effectiveness of SEM and PLS-SEM in examining construct validity and interrelationships among variables (Moon et al., 2011; Jyoti & Dev, 2015), while Sarstedt et al. (2017) highlighted its ability to model structural relationships among latent variables. Additionally, PLS-SEM was deemed appropriate due to its flexibility and suitability for studies with relatively small sample sizes (Amri et al., 2020).

5. FINDING

In this section, the evaluation of the measurement model focuses on assessing both the convergent validity and internal consistency reliability of the study's constructs, ensuring that the measurement instruments are both accurate and dependable. The analysis was based on data collected from 318 successful respondents to the questionnaire. Convergent validity examines the extent to which items intended to measure the same construct are highly correlated, and it is typically assessed using the Average Variance Extracted (AVE), with a value greater than 0.50 considered indicative of satisfactory convergent validity (Hair et al., 2019). Internal consistency reliability, on the other hand, evaluates the degree to which the items within a construct consistently measure the same underlying concept, which is commonly assessed using both Composite Reliability (CR) and Cronbach's Alpha, with values of 0.70 or higher reflecting acceptable reliability (Nunnally, 1994). By examining both convergent validity and internal consistency reliability together, the study ensures that the constructs are not only conceptually coherent but also empirically robust, providing a solid foundation for subsequent structural model analysis.

Table 1: Reflective Measurement Models

Constructs	**Convergent Validity**	**Internal Consistency Reliability**	
	AVE	Composite Reliability	Cronbach's Alpha
	>0.5	>0.70	>0.70
Performance Expectancy	0.603	0.901	0.867
Effort Expectancy	0.603	0.901	0.871
Social Influence	0.703	0.922	0.896

Facilitating Conditions	0.649	0.879	0.837
Perceived Risk	0.731	0.731	0.837
Trust	0.751	0.938	0.917
Cybersecurity Risk Behaviour	0.565	0.833	0.734

These findings suggest that all constructs attained sufficient convergent validity, with the AVE yielding values between 0.565 and 0.751, which is significantly larger than the suggested threshold of 0.50. The threat of internal consistency also proved to be satisfactory, with consistency ranging from 0.833 to 0.938 and Cronbach's Alpha ranging from 0.734 to 0.917, indicating the reliability of the measurement items. Trust (AVE = 0.751; CR = 0.938; α = 0.917) and cybersecurity risk behaviour (AVE = 0.565; CR = 0.833; α = 0.734) demonstrated the greatest validity and reliability, indicating that these constructs could be subjected to structural analysis in the future.

Table 2: Structural Model Assessment

Relationship	Path Coefficients(β)	Standard Error	t-value	p-values	Decision
PE => CRB	0.337	0.052	6.418	0	Supported
EE => CRB	0.199	0.067	2.979	0.001	Supported
SI => CRB	-0.171	0.071	2.402	0.008	Not Supported
FC => CRB	0.065	0.063	1.034	0.151	Not Supported
PR=> CRB	0.125	0.067	1.859	0.032	Supported
TR => CRB	0.234	0.054	4.315	0.000	Supported
TR x PE -> CRB	-0.142	0.052	2.736	0.003	Supported
TR x EE -> CRB	-0.037	0.056	0.667	0.252	Not Supported
TR x SI -> CRB	0.284	0.066	4.319	0	Supported
TR x FC -> CRB	-0.221	0.056	3.923	0	Supported
TR x PR-> CRB	0.021	0.062	0.336	0.368	Not Supported

The results of the structural model illustrate how UTAUT constructs affect Cybersecurity Risk Behaviour (CRB) of PayTech users. The positive influence of Performance Expectancy (PE) on CRB is strong and significant ($b = 0.337$, $p < 0.001$), as users who view digital payment systems as useful are more likely to develop secure behaviours. Another positive influence is exerted by Effort Expectancy (EE) ($b = 0.199$, $p = 0.001$), which suggests that more convenient system use will encourage safer cybersecurity-related behaviours. Social Influence (SI) and Facilitating Conditions (FC) did not prove to be significant, which implies that peer pressure and support do not significantly affect the cybersecurity behaviour of users. The moderation analysis indicates that trust strengthens the relationship between PE, SI, and FC with CRB, which makes sense given that the UTAUT constructs contribute to either strengthening or weakening these relationships. In general, these results indicate that the perception of usefulness and ease of use are the dominant motivations for cybersecurity behaviour among PayTech users, whereas social and facilitating conditions do not significantly influence perceptions.

The results show that the important drivers of cybersecurity risk behaviour (CRB) among PayTech users are performance expectancy and effort expectancy. When it comes to securing behaviours, users who perceive digital payment systems as convenient will have a greater likelihood of engaging in secure behaviours (Venkatesh et al., 2003; Davis, 1989). The influence of social influence and facilitating conditions on CRB was negligible, which agrees with past researchers who suggest that external factors are not necessarily of great influence on user behaviour in digital environments (Venkatesh et al., 2003; Venkatesh and Bala, 2008). The moderating role of trust is also important in facilitating interactions between performance expectancy, social influence, and facilitating conditions to CRB (McKnight et al., 2002). In general, the research demonstrates the relevance of the perceived usefulness, ease of use, and trust element in developing secure cybersecurity environments in PayTech systems, which is consistent with the results obtained by previous studies on the power of trust in technology acceptance (Gefen, 2000; Lee, 2009).

6. CONCLUSION

The results of the current study provide substantive knowledge on the major determinants of cybersecurity risk behaviour by PayTech users. By defining the most important drivers that shape the security-related behavior of users, this research adds to the academic knowledge of how users cogently perceive and cope with cyber-risk in digital payment ecosystems. Specifically, the results highlight the overriding importance of trust, alongside technological and behavioural variables, when determining users' propensity to adopt secure practices when using PayTech platforms. Notwithstanding these contributions, the study lays out a number of prospective research trajectories. Longitudinal studies are needed to examine long-term impacts of user trust and frequency of system updates on cybersecurity behaviors, since trust will vary and potentially change as users gain experience with PayTech services or are exposed to security events. Looking into the effect of continuous system improvements, security patches, and platform transparency on sustainable secure behaviour could provide meaningful insights for PayTech providers and policy makers.

Future inquiry should also include the appraisal of the efficacy of cybersecurity education and awareness initiatives in modulating user behaviour. Determining if structured training, digital literacy programmes, or focused awareness programmes lead to demonstrable improvement in cybersecurity practices would be helpful to determine the most efficacious strategies for mitigating user-related security risks in the PayTech ecosystem. Moreover, an exploration of emotional and psychological variables, such as fear, confidence, anxiety, or perceived control, may further enrich extant models of cybersecurity behaviour. These affective dimensions have a powerful influence on the way users value security threats and their response to security measures to protect themselves, but they are underexplored in the PayTech context. Integrating emotional constructs into later research could provide a more holistic understanding of user decision-making processes. Ultimately, by broadening the scope of investigation to include longitudinal effects, educational interventions, and emotional determinants, future research may build on the current research to create more comprehensive

frameworks to understand and improve cybersecurity behaviour amongst PayTech users. Such scholarly endeavors would promote the advancement of both theoretical knowledge and the praxis of the design of efficacious security strategies, user-centric systems, and policy measures in the rapidly evolving digital payment landscape.

ACKNOWLEDGEMENT

The authors would like to acknowledge all respondents for their valuable time and for sharing their perceptions in support of this study. This research did not receive any specific funding. The encouragement and constructive advice provided by peers and tutors throughout the research period are also deeply appreciated.

REFERENCES

Abd-Allawari, H. A., Al-Omari, A. A., & Abuhashesh, M. (2020). *The role of facilitating conditions in adoption of cybersecurity practices: A UTAUT2 perspective***.** International Journal of Security and Networks, 15(3), 135–148.

Alalwan, A. A., Dwivedi, Y. K., & Rana, N. P. (2017). Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. *International Journal of Information Management*, *37*(3), 99–110. https://doi.org/10.1016/j.ijinfomgt.2017.01.002

Amri, M., Ali, R., & Rahman, A. (2020). Application of PLS-SEM in small sample research: Advantages and limitations. *Journal of Statistics and Management Systems, 23*(4), 617–634. https://doi.org/10.1080/09720510.2020.1713176Jyoti, J., & Dev, N. (2015). Application of structural equation modeling in social sciences. *International Journal of Social Science and Interdisciplinary Research, 4*(2), 32–40.

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411–423. https://doi.org/10.1037/0033-2909.103.3.411

Antunes, D., Pacheco, C., & Antunes, M. (2021).Cybersecurity risky behaviors and attitudes among adolescents: An empirical study. *Computers & Security, 102*, 102151. https://doi.org/10.1016/j.cose.2020.102151

Bryman, A., & Bell, E. (2007). *Business research methods* (2nd ed.). Oxford University Press.

Casaló, L. V., Flavián, C., & Guinalíu, M. (2007). *The role of security, privacy, usability and reputation in the development of online banking*. Online Information Review, 31(5), 583-603.

Chen, Y. H., & Barnes, S. (2007). *Initial trust and online buyer behaviour*. Industrial Management & Data Systems, 107(1), 21–36. https://doi.org/10.1108/02635570710719034

Choudhury, A., Shahsavar, Y., & Shamszare, H. (2025). *User intent to use DeepSeek for healthcare purposes and their trust in the large language model: Multinational survey study*.

Davis, F. D. (1989). Perceived Usefulness, Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), 319–340. https://doi.org/10.2307/249008

Department of Statistics Malaysia. (2023). *Population and demographic statistics 2023*. https://www.dosm.gov.my

Diyana, Z.N.A.; and Shazwani, M.Z.N. (2018). Phishing threats. *eSecurity The First Line of Digital Defense Begins with Knowledge*, 45(2), 25-27.

Goddard, K., Roudsari, A., & Wyatt, J. C. (2014). Automation bias: Empirical results assessing influencing factors. *International Journal of Medical Informatics*, *83*(5), 368–375. https://doi.org/10.1016/j.ijmedinf.2014.01.001

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research*(pp. 105–117). Sage Publications.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2019). *Partial least squares structural equation modeling (PLS-SEM) using SmartPLS: A primer* (2nd ed.). Sage Publications.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2019). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). Sage.

Haridan, N M., Hassan, A F S., & Alahmadi, H A. (2020, June 29). *Financial Technology Inclusion in Islamic Banks: Implication on Shariah Compliance Assurance*. , 10(14). https://doi.org/10.6007/ijarbss/v10-i14/7361

Kamalulail, A., Razak, N. E. N. A., Omar, S. A., & Yusof, N. M. (2022). Awareness of Cybersecurity: A Case study in UITM Negeri Sembilan Branch, Seremban Campus. *e-Academia Journal*, *11*(1). https://doi.org/10.24191/e-aj.v11i1.18266

Kaur, R., Klobučar, T., & Gabrijelčič, D. (2025). *Barriers and enablers for organisational cybersecurity behaviour: The role of infrastructure, leadership support, and access to resources*. IETE Technical Review, 42(2), 246–258. https://doi.org/10.1080/02564602.2025.2485910

Kaur, S. and Arora, S. (2020). Role of perceived risk in online banking and its impact on behavioural intention: trust as a moderator. *Journal of Asia Business Studies*, 15(1), 1-30. https://doi.org/10.1108/jabs-08-2019-0252

Kennison, S. M., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Frontiers in Psychology, 11*, 546546. https://doi.org/10.3389/fpsyg.2020.546546

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). *A trust-based consumer decision-making model in electronic commerce*. Decision Support Systems, 44(2), 544–564.

Kumar, A., Adlakaha, A., & Mukherjee, K. (2020). *The effect of perceived security and trust on mobile payment adoption: A study of emerging economy*. International Journal of Innovation and Technology Management, 17(04), 2050022. https://doi.org/10.1142/S021987702050022X

Kumar, A., Hosseini, A., Azarbayjani, A., & Heydarian, A. (2025). *Adoption of AI-assisted mobility technologies: The role of* perceived trust and safety function as key predictors of behavioural intention in adopting emerging technologies by enhancing confidence and alleviating uncertainty.

Moon, J., Choi, I., & Lee, S. (2011). The use of SEM in examining organizational behavior constructs. *Journal of Organizational Behavior Research, 16*(2), 45–59.

Napis, N M., & Daud, N. (2023, February 9). Factors Influencing Adoption of E-Wallet Among Malaysian Young. , 13(2). https://doi.org/10.6007/ijarbss/v13-i2/16363

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 51*, 345–356. https://doi.org/10.1016/j.cose.2017.01.007

Rahim, S. S. I., Huda, M. I. M., Sa'ad, S., & Moorthy, R. (2024). Cyber Security Crisis/Threat: Analysis of Malaysia National Security Council (NSC) involvement through the perceptions of government, private and people based on the 3P model. *Deleted Journal*, *21*(2). https://doi.org/10.17576/ebangi.2024.2102.17

Salkind, N. J. (2019).*Exploring research* (9th ed.). Pearson Education.

Santosdiaz, R. (2024, August 13). *Malaysia's Fintech Boom: A Growing Force in Southeast Asia*. The Fintech Times. https://thefintechtimes.com/fintech-landscape-of-malaysia/

Sarstedt, M., Ringle, C. M., & Hair, J. F. (2017). Partial least squares structural equation modeling. In C. Homburg, M. Klarmann, & A. Vomberg (Eds.), *Handbook of market research* (pp. 1–40). Springer. https://doi.org/10.1007/978-3-319-05542-8_23-1

Sekaran, U. (2010). *Research methods for business: A skill-building approach* (5th ed.). John Wiley & Sons.

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed.). John Wiley & Sons.

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed.). Chichester, UK: Wiley.

Shaikh, I. M., Qureshi, M. A., Noordin, K., Shaikh, J. M., Khan, A., & Shahbaz, M. S. (2020). Acceptance of islamic financial technology (fintech) banking services by malaysian users: an extension of technology acceptance model. *Foresight*, 22(3), 367-383. https://doi.org/10.1108/fs-12-2019-0105

Tempestini, A., Sani, L., Nisi, M., & Mancini, A. (2023). Measuring cybersecurity awareness: Development and validation of the Cybersecurity Awareness Inventory (CAIN). *Computers & Security, 124*, 102981. https://doi.org/10.1016/j.cose.2022.102981

Venkatesh, N., Thong, N., & Xu, N. (2012). Consumer Acceptance and use of Information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157. https://doi.org/10.2307/41410412

Venkatesh, V., Thong, J., & Xu, X. (2016). Unified Theory of Acceptance and Use of Technology: a Synthesis and the Road ahead. *Journal of the Association for Information Systems*, *17*(5), 328–376. https://doi.org/10.17705/1jais.00428

Wang et al. (2008) *Investigating the determinants and age and gender differences in the acceptance of mobile learning*. British Journal of Educational Technology, 40(1), 92–118. https://doi.org/10.1111/j.1467-8535.2007.00809.x