AN EXTENDED PROTECTION MOTIVATION THEORY FOR CYBER FRAUD PREVENTION

NORHASYIMATUL NAQUIAH BINTI GHAZALI

DOCTOR OF PHILOSOPHY
UNIVERSITI UTARA MALAYSIA
2025

Awang Had Salleh
Graduate School
of Arts And Sciences

Universiti Utara Malaysia

PERAKUAN KERJA TESIS / DISERTASI
(Certification of thesis / dissertation)

Kami, yang bertandatangan, memperakukan bahawa
(We, the undersigned, certify that)

NORHASYIMATUL NAQUIAH GHAZALI

calon untuk Ijazah
(candidate for the degree of) **PhD**

telah mengemukakan tesis / disertasi yang bertajuk:
(has presented his/her thesis / dissertation of the following title):

"AN EXTENDED PROTECTION MOTIVATION THEORY FOR CYBER FRAUD PREVENTION"

seperti yang tercatat di muka surat tajuk dan kulit tesis / disertasi.
(as it appears on the title page and front cover of the thesis / dissertation).

Bahawa tesis/disertasi tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan, sebagaimana yang ditunjukkan oleh calon dalam ujian lisan yang diadakan pada : **21 Oktober 2024.**
That the said thesis/dissertation is acceptable in form and content and displays a satisfactory knowledge of the field of study as demonstrated by the candidate through an oral examination held on: ***21 October 2024.***

Pengerusi Viva: *(Chairman for VIVA)*	**Assoc. Prof. Dr. Nur Haryani Zakaria**	Tandatangan *(Signature)*
Pemeriksa Luar: *(External Examiner)*	**Assoc. Prof. Dr. Yazrina Yahya**	Tandatangan *(Signature)*
Pemeriksa Dalam: *(Internal Examiner)*	**Assoc. Prof. Dr. Zahurin Mat Aji @ Alon**	Tandatangan *(Signature)*
Nama Penyelia/Penyelia-penyelia: *(Name of Supervisor/Supervisors)*	**Dr. Syahida Hassan**	Tandatangan *(Signature)*
Nama Penyelia/Penyelia-penyelia: *(Name of Supervisor/Supervisors)*	**Assoc. Prof. Dr. Rahayu Ahmad**	Tandatangan *(Signature)*

Tarikh:
(Date) ***21 October 2024***

Permission to Use

In presenting this thesis in fulfilment of the requirements for postgraduate degree from Universiti Utara Malaysia, I agree that the university library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence, by the Dean of Awang Had Salleh Graduate School of Art and Sciences. It is understood that any copying publication or use of this thesis or parts thereof for financial gain shall not be allowed without any written permission. It is also understood that due recognition shall be given to me and Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Request for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Awang Had Salleh Graduate School of Art and Sciences
UUM College of Art and Sciences
Universiti Utara Malaysia
06010 UUM Sintok

Abstrak

Kebimbangan mengenai keselamatan siber, terutamanya berkaitan dengan penipuan siber, semakin mendapat perhatian, khususnya dalam bidang e-Perkhidmatan. Walaupun sistem keselamatan yang lebih canggih telah dilaksanakan, e-Perkhidmatan masih terdedah kepada ancaman, menyebabkan kerugian bernilai berbilion dolar kepada ekonomi digital. Walaupun penting untuk mempercayai rangkaian dan sistem, individu atau pengguna harus belajar dan menerapkan tingkah laku perlindungan untuk diri mereka sendiri. Oleh itu, kajian ini memberi fokus kepada pembangunan model tingkah laku perlindungan penipuan siber menggunakan Teori Motivasi Perlindungan (PMT). Sebanyak 560 responden telah dipilih menggunakan teknik persampelan bertujuan, yang lazim digunakan dalam penyelidikan dalam talian kerana ketiadaan rangka persampelan yang stabil dan kumpulan responden yang sering berubah. Pautan kepada borang soal selidik telah diedarkan melalui beberapa pelantar media sosial yang popular, seperti Facebook, WhatsApp, dan Telegram. Data telah dianalisis menggunakan teknik "partial least squares structural equation modelling technique" (PLS-SEM). Hasil kajian ini mendapati bahawa persepsi terhadap seriusnya ancaman siber, norma subjektif, keberkesanan tindak balas, kemahiran kecekapan keselamatan siber, serta pengetahuan kecekapan keselamatan siber secara signifikan dapat meningkatkan niat pengguna untuk terlibat dalam tingkah laku perlindungan. Selain itu, faktor seperti kepentingan melindungi data peribadi dalam e-Perkhidmatan secara langsung mempengaruhi persepsi pengguna e-Perkhidmatan terhadap seriusnya ancaman siber, sementara itu, kredibiliti sesuatu sumber telah menunjukkan keputusan sebaliknya. Kajian ini turut memberikan pandangan tentang pelbagai kaedah yang berpotensi digunakan oleh pengguna untuk melindungi diri daripada menjadi mangsa penipuan siber. Secara keseluruhan, kajian ini menyediakan panduan kepada pembuat dasar dan pengamal dalam bidang keselamatan siber, terutamanya dalam merangka strategi untuk meningkatkan perlindungan pengguna e-Perkhidmatan daripada penipuan siber. Ini seterusnya mengukuhkan daya tahan platform digital dan menyokong pertumbuhan ekonomi mampan dalam ekonomi digital Malaysia.

Katakunci: Teori Motivasi Perlindungan (PMT), Keselamatan siber, Penipuan siber, e-Perkhidmatan, Tingkah laku dalam talian

Abstract

Cybersecurity concerns particularly around cyber fraud have come under increased scrutiny, especially in the area of e-Services. Despite implementing enhanced security systems, e- Services remain vulnerable, leading to billions of dollars in losses for the digital economy. While trust in networks and systems is essential, individuals must take proactive steps to learn and adopt protective behaviours to safeguard themselves. Therefore, this study focuses on developing a cyber fraud protection behaviour model using the Protection Motivation Theory (PMT). A total of 560 respondents were selected using the purposive sampling technique, which is widely employed in online research because there is no fixed list of respondents and the group keeps changing. The questionnaire link has been distributed on several popular social media platforms, such as Facebook, WhatsApp, and Telegram. The data were analysed using the partial least squares structural equation modelling technique (PLS-SEM). The finding revealed that perceived threat severity, subjective norm, response efficacy, cybersecurity efficacy skills, and cybersecurity efficacy knowledge significantly increases users' intention to engage in protective behaviour. Additionally, antecedent factors, such as the perceived value of data, directly influence the perceived threat severity of e-Services users, while source credibility indicates contradictory results. Furthermore, this study identifies that wishful thinking among e-Services users significantly strengthens maladaptive rewards, which influence the intention of users to engage in protective behaviour. The original model was extended, and a comprehensive research framework was developed through this research. It also provides insights into various potential methods users can use to protect themselves from becoming victims of cyber fraud. Ultimately, this dissertation provides valuable insights for policymakers and practitioners in the field of cybersecurity, particularly in formulating strategies to enhance the protection of e-Services users against cyber fraud, thereby strengthening resilience on digital platforms and supporting sustainable economic growth in Malaysia's digital economy.

Keywords: Protection motivation theory (PMT), Cybersecurity, Cyber fraud, e-Services, Online behaviour

Acknowledgement

In the name of Allah, the Most Gracious and the Most Merciful.

Alhamdulillah, I am deeply grateful to Allah SWT for providing me the strength, and knowledge and granting me the opportunity to pursue my PhD as well as make this journey possible. My deepest appreciation goes to my main supervisor, Dr. Syahida Hassan who has been very helpful and supportive throughout the process of doing the research. Thank you to her for her time, effort and patience in reviewing the countless revisions of my write-up. Not forgotten, my appreciation and gratitude to my second supervisor, Assoc Prof. Dr. Rahayu Ahmad who had been guiding me from the point when she was appointed as a co-supervisor. I have learned a lot and am totally indebted to both of them.

My appreciation also goes to my parents, Mr. Ghazali Ismail and Mrs. Saodah Ibrahim and my siblings. They are the reason why I want to pursue my studies this far. They have been there for me throughout all my life, through thick and thin, both morally and financially. I would also like to thank my close friends who have been supporting me throughout this journey, Nurul Ain Sallehuddin Haqe, Dr. Nur Rosdiatul Husna Ahmad Fauzi, and Siti Naquiah Md Fauzi. Not to be forgotten, my colleagues, Dr. Norbaizura Ramzi, Dr. Ani Asmaa Asli, Nurfarahiyah Mohd Najib, and Farah Sofiya Ilyana Ruzzaman who have been very supportive since the day I registered as a PhD candidate. Thank you so much for the unwavering support, prayers and motivation that kept me going even during challenging times. Last but not least, I wish to thank all wonderful people for their valuable contributions and spontaneous support.

My PhD journey has taught me many valuable lessons including the importance of trusting in Allah SWT. It has been an unforgettable experience that has transformed me into a better version of myself and for that, I am truly thankful.

Table of Contents

List of Tables

List of Figures

CHAPTER ONE

INTRODUCTION

1.1 Background of Studies

The internet has certainly enabled individuals, communities, and organisations to effect beneficial changes such as empowering people, improving and spreading democratic values, encouraging technology, and boosting the economy over the years. One of the most transformative aspects of the internet is its ability to drive innovation and improve access to services across various domains, fostering greater convenience and efficiency in everyday life. e-Services that have been widely used, such as e-commerce, e-government, e-learning and e-banking (Goundar, 2021; Saleemi et al., 2017) have allowed for efficient services and boosted productivity among netizens. This has led to an escalating volume of data being stored, processed, and managed within digital platforms (Khando et al., 2021).

However, the digital transition comes with two effects, offering massive opportunities and creating substantial risks to communities, economies, and national security. These substantial risks will worsen if left unchecked since the field is still in its infancy stage. Nevertheless, as the field continues progressing rapidly, more academic efforts are required to understand the field and remain up to date with the current trends (Dawson & Thomson, 2018). Among the substantial risks posed by the digital transition, cybercrime stands out as a pressing concern due to its pervasive and evolving nature (Payne & Hadzhidimova, 2018). As digital platforms become more integral to everyday life, the potential for malicious actors to exploit vulnerabilities for personal gain has grown significantly, particularly in the form of cyber fraud.

REFERENCES

Abdul Hameed, M., & Gamagedara Arachchilage, N. A. (2021). The role of self-efficacy on the adoption of information systems security innovations: A meta-analysis assessment. *Personal and Ubiquitous Computing*, *25*(5), 911–925. https://doi.org/10.1007/s00779-021-01560-1

Abu-Taieh, E. M. O. (2017). Cyber security body of knowledge. *2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2)*, 104–111. https://doi.org/10.1109/SC2.2017.23

Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2016). A consideration of the social impact of cybercrime: Examples from hacking, piracy, and child abuse material online. *Contemporary Social Science*, *11*(4), 373–391. https://doi.org/10.1080/21582041.2015.1117648

Ajzen, I. (1991). The Theory of Planned Behaviour. *Organizational Behaviour and Human Decision Process*, *50*, 179–211.

Ajzen, I. (2002). Residual effects of past on later behaviour: Habituation and reasoned action perspectives. *Personality and Social Psychology Review*, *6*(2), 107–122.

Ajzen, I., Brown, T. C., & Carvajal, F. (2004). Explaining the discrepancy between intentions and actions: The case of hypothetical bias in contingent valuation. *Personality and Social Psychology Bulletin*, *30*(9), 1108–1121. https://doi.org/10.1177/0146167204264079

Ajzen, I., Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention, and behaviour: An introduction to theory and research. In *Computers in Human Behaviour*.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2023). The assessment of the impact of cyberfraud in the South African banking industry. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-10-2022-0260

Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-Centric Computing and Information Sciences*. https://doi.org/10.1186/s13673-018-0128-7

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2). https://doi.org/10.3390/bdcc5020023

Alhussein, N. (2020). *Investigation of the variables that govern user behaviours related to e-crime attacks* [Luleå University of Technology]. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1437463&dswid=-1270

Ali Memon, M., Ting, H., Cheah, J.-H., Thurasamy, R., Chuah, F., & Huei Cham, T. (2020). Sample size for survey research: Review and recommendations. *Journal of Applied Structural Equation Modeling*, *4*(2), 2590–4221.

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behaviour and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. In *Applied Sciences (Switzerland)* (Vol. 11, Issue 8). MDPI AG. https://doi.org/10.3390/app11083383

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behaviour: A systematic review of studies and theories. *Applied Sciences* , *13*(9), 1–17. https://doi.org/10.3390/app13095700

Alnifie, K. M., & Kim, C. (2023). Appraising the manifestation of optimism bias and its impact on human perception of cyber security: A meta analysis. *Journal of Information Security*, *14*(02), 93–110. https://doi.org/10.4236/jis.2023.142007

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. In *International Journal of Human Computer Studies* (Vol. 82). Elsevier. https://doi.org/10.1016/j.ijhcs.2015.05.005

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioural intentions. *MIS Quarterly: Management Information Systems*. https://doi.org/10.2307/25750694

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In *The Economics of Information Security and Privacy* (pp. 265–300). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39498-0_12

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviours. *Computers in Human Behaviour*, *69*, 437–443. https://doi.org/https://doi.org/10.1016/j.chb.2016.12.040

Appelman, A., & Sundar, S. S. (2015). Measuring message credibility: Construction and validation of an exclusive scale. *Http://Dx.Doi.Org/10.1177/1077699015606057*, *93*(1), 59–79. https://doi.org/10.1177/1077699015606057

Armstrong, C. L., & Nelson, M. R. (2005). How newspaper sources trigger gender stereotypes. *Journalism & Mass Communication Quarterly*, *82*(4), 820–837.

Arpaci, I., & Aslan, O. (2023). Development of a scale to measure cybercrime-awareness on social media. *Journal of Computer Information Systems*, *63*(3), 695–705. https://doi.org/10.1080/08874417.2022.2101160

Augustine, M. C., Wilcox, P., Ousey, G. C., & Clayton, R. R. (2002). Opportunity Theory and Adolescent School-Based Victimization. *Violence and Victims*, *17*(2), 233–253.

Aurigemma, S., & Mattson, T. (2018). Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. *Computers and Security*, *73*, 219–234. https://doi.org/10.1016/j.cose.2017.11.001

Aurigemma, S., Mattson, T., & Leonard, L. (2019). Evaluating the core and full protection motivation theory nomologies for the voluntary adoption of password manager applications. *AIS Transactions on Replication Research*, *5*, 1–21. https://doi.org/10.17705/1atrr.00035

Bandura, A., & Wessels, S. (1997). *Self-efficacy* (Vol. 4). Cambridge University Press. https://happyheartfamilies.citymax.com/f/Self_Efficacy.pdf

Barrett, E., Dresner, D., & Buil-Gil, D. (2020). *Why victims of cyber crime deserve "Cyber CPR."* Manchester Policy Articles . https://blog.policy.manchester.ac.uk/posts/2020/11/why-victims-of-cyber-crime-deserve-cyber-cpr/

Bastardi, A., Uhlmann, E. L., & Ross, L. (2011). Wishful thinking: Belief, desire, and the motivated evaluation of scientific evidence. In *Psychological Science*. https://doi.org/10.1177/0956797611406447

Bavel, R. van, Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behaviour. *International Journal of Human Computer Studies*. https://doi.org/10.1016/j.ijhcs.2018.11.003

Bax, S., McGill, T., & Hobbs, V. (2021). Maladaptive behaviour in response to email phishing threats: The roles of rewards and response costs. *Computers and Security*, *106*, 102278. https://doi.org/10.1016/j.cose.2021.102278

Bekkers, L., Susanne, V. H. de G., Ellen, M. ter H., Ynze, V. H., Remco, S., & Eric Rutger, L. (2023). Protecting your business against ransomware attacks? explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model. *Computers and Security*, *127*. https://doi.org/10.1016/j.cose.2023.103099

Berg, N. (2005). Non-response bias. In *Encyclopedia of Social Measurement* (Vol. 2, pp. 865-873.). Academic Press.

Bergmann, M. C., Dreißigacker, A., Von Skarczinski, B., & Wollinger, G. R. (2018). Cyber-dependent crime victimization: The same risk for everyone? *Cyberpsychology, Behaviour, and Social Networking*, *21*(2), 84–90. https://doi.org/10.1089/cyber.2016.0727

Berland, E. (2017). *Identity theft survey results: Consumers need more education and help*. Experian. www.experianplc.com

Berlo, D. K., Lemert, J. B., & Mertz, R. J. (1969). Dimensions for evaluating the acceptability of message sources. *Public Opinion Quarterly*, *33*(4), 563–576.

Bernama. (2020). *More than 90 pct jump in cyber crime complaints during MCO*. https://www.malaysia.gov.my

Bernama Infographic. (2020). *Online scams since MCO was enforced on 18 March, 2020*.

Bobbitt, Z. (2020). *What is an antecedent variable? (explanation & example)*. Statology.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behaviour: Insights from panel data.

Communication Research, *48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Bong, X. L. (2023). *A study of awareness of cyber scams and cybersecurity among university students in Malaysia*. Universiti Tunku Abdul Rahman.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviours. *MIS Quarterly: Management Information Systems*. https://doi.org/10.25300/MISQ/2015/39.4.5

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400–420.

Bottoms, A., & Tonry, M. (2002). *Ideology, crime and criminal justice*. Willan Publishing.

Bougie, R., & Sekaran, U. (2020). *Research methods for business: A skill building approach* (8th ed.). John Wiley & Sons. Inc.

Boulet, G. (2015). The difference between knowledge and skills: Knowing does not make you skilled. *ELearning Industry. Com. Retrieved from Https://Elearningindustry. Com/Difference-between-Knowledge-and-Skills-Knowingnot-Make-Skilled*.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.2307/25750690

Burgoon, J. K., Buller, D. B., Hale, J. L., & de Turck, M. A. (1984). Relational messages associated with nonverbal behaviours. *Human Communication Research*, *10*(3), 351–378.

Burns, S., & Roberts, L. (2013). Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety*, *15*(1), 48–64. https://doi.org/10.1057/cpcs.2012.13

Button, M., Nicholls, C. M. N., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian and New Zealand Journal of Criminology*, *47*(3), 391–408. https://doi.org/10.1177/0004865814521224

Cambridge Dictionary. (2020). *Cyberfraud*. Cambridge University Press & Assessment; Cambridge University Press & Assessment . https://dictionary.cambridge.org/dictionary/english/cyberfraud

Camoens, A. (2023). *On top of the scams list*. Star Media Group Berhad.

Caneppele, S., & Aebi, M. F. (2019). Crime drop or police recording flop? on the relationship between the decrease of offline crime and the increase of online and hybrid crimes. *Policing (Oxford)*, *13*(1), 66–79. https://doi.org/10.1093/police/pax055

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication*. https://doi.org/10.1109/TPC.2009.2017985

Chawla, M., & Chouhan, S. S. (2014). A survey of phishing attack techniques. *International Journal of Computer Applications*, *93*(3), 32–35. https://doi.org/10.5120/16197-5460

Chen, D. Q., & Liang, H. (2019). Wishful thinking and IT threat avoidance: An extension to the technology threat avoidance theory. *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2018.2835461

Chen, S., Yuan, Y., (Robert) Luo, X., Jian, J., & Wang, Y. (2021). Discovering group-based transnational cyber fraud actives: A polymethodological view. *Computers and Security*, *104*. https://doi.org/10.1016/j.cose.2021.102217

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS*. https://doi.org/10.1109/HICSS.2009.74

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *SA Journal of Information Management*, *23*(1). https://doi.org/10.4102/sajim.v23i1.1277

Chin, W. W. (1998). *Modern methods for business research: The partial least squares approach to structural equation modeling* (2nd ed., Vol. 2). Lawrence Elrbaum Associates. http://www.researchgate.net/publication/232569511

Choi, J., Kruis, N. E., & Choo, K. S. (2021). Explaining fear of identity theft victimization using a routine activity approach. *Journal of Contemporary Criminal Justice*, *37*(3), 406–426. https://doi.org/10.1177/10439862211001627

Choi, K.-S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, *2*(1), 308–333. https://www.researchgate.net/publication/238621672

Clarke, R. V, & Felson, M. (2017). The origins of the routine activity approach and situational crime prevention. In *The origins of American criminology* (pp. 245–260). Routledge.

Clough, J. (2015). Computer related fraud. In *Research Handbook on International Financial Crime* (pp. 366–378). Edward Elgar Publishing.

Clubb, A. C., & Hinkle, J. C. (2015). Protection motivation theory as a theoretical framework for understanding the use of protective measures. *Criminal Justice Studies*, *28*(3), 336–355. https://doi.org/10.1080/1478601X.2015.1050590

Cohen, J. (1988). *Statistical power analysis for the behavioural sciences*. Lawrence Erlbaum Associates.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588. https://doi.org/10.2307/2094589

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. In *Review* (Vol. 46, Issue 5).

Collins Dictionary. (2023). *Definition of "efficacy."* Collins Dictionary. https://www.collinsdictionary.com/us/dictionary/english/efficacy

Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behaviour*, *28*(5), 1849–1858. https://doi.org/10.1016/j.chb.2012.05.003

Creswell, J. W., & Creswell, J. D. (2022). *Research design: Qualitative, quantitative, and mixed methods approaches* (6th ed.). Sage Publication Inc.

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviours. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*. https://doi.org/10.1145/2691517.2691521

Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10. https://doi.org/10.1109/HICSS.2010.311

CyberSecurity Malaysia. (2019). *Keep yourself safe from online identity theft*. CyberSecurity Malaysia.

CyberSecurity Malaysia. (2021). *Experian and cybersecurity Malaysia: growth in digital transactions increases risk of identity theft*. CyberSecurity Malaysia. https://www.cybersecurity.my/data/content_files/44/2216.pdf

CyberSecurity Malaysia. (2022). *Mycert-incident-statistics 2022*.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers and Security*, *48*, 281–297. https://doi.org/10.1016/j.cose.2014.11.002

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. In *Frontiers in Psychology*. https://doi.org/10.3389/fpsyg.2018.00744

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behaviour*, *108*(May 2019), 106310. https://doi.org/10.1016/j.chb.2020.106310

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context.

Behaviour and Information Technology, *0*(0), 1–13. https://doi.org/10.1080/0144929X.2021.1905066

De Smidt, G., & Botzen, W. (2018). Perceptions of corporate cyber risks and insurance decision-making. *Geneva Papers on Risk and Insurance: Issues and Practice*, *43*(2), 239–274. https://doi.org/10.1057/s41288-018-0082-7

DeLiema, M., Li, Y., & Mottola, G. (2023). Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type. *International Journal of Consumer Studies*, *47*(3), 1042–1059. https://doi.org/10.1111/ijcs.12886

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioural intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7), 386–408. https://doi.org/10.17705/1jais.00133

Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviours. *Information Communication and Society*. https://doi.org/10.1080/1369118X.2018.1428652

Doty, P. (2015). U.S. homeland security and risk assessment. *Government Information Quarterly*, *32*(3), 342–352. https://doi.org/10.1016/j.giq.2015.04.008

Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research*, *19*(6), 537–549. https://doi.org/10.1080/15614263.2018.1507890

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity approach. *Crime Prevention Studies*, *16*, 7–40.

Edgerly, S. (2017). Seeking out and avoiding the news media: Young adults' proposed strategies for obtaining current events information. *Mass Communication and Society*, *20*(3), 358–377. https://doi.org/10.1080/15205436.2016.1262424

Edgerly, S., Mourão, R. R., Thorson, E., & Tham, S. M. (2020). When do audiences verify? how perceptions about message and source influence audience verification of news headlines. *Journalism and Mass Communication Quarterly*, *97*(1), 52–71. https://doi.org/10.1177/1077699019864680

Experian. (2020). *Only 32 percent of businesses have made operational adjustments to meet new consumer demands for digital banking, payment and retail transactions*. Experian Information Solutions, Inc. https://www.experianplc.com/newsroom/press-releases/2020/only-32-percent-of-businesses-have-made-operational-adjustments-to-meet-new-consumer-demands-for-digital-banking-payment-and-retail-transactions

Fagan, M., & Mohammad Maifi, H. K. (2016). Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016).*, 59–75.

Fansher, A. K., & Randa, R. (2019). Risky social media behaviours and the potential for victimization: A descriptive look at college students victimized by someone met online. *Violence and Gender*, *6*(2), 115–123. https://doi.org/10.1089/vio.2017.0073

Finance Ministry of Slovak Republic. (2006). *Metodicky pokyn na pouzitie odbornych vyrazov pre oblasť informatizacie spolocnosti*. http://www.informatizacia.sk/terminologia/3480s.

Fleming, P., Bayliss, A. P., Gareth Edwards, S., & Seger, C. R. (2021). The role of personal data value, culture and self-construal in online privacy behaviour. *PLoS ONE*, *16*(7 July). https://doi.org/10.1371/journal.pone.0253568

Fletcher, E. (2019). *Government imposter scams top the list of reported frauds*. Federal Trade Commission, Protecting America's Consumers.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Focus Malaysia. (2023). *Online scams cost M'sians RM52 mil in 3 months*. Focus Malaysia. https://focusmalaysia.my/author/focusm/

Folkman, S., Lazarus, R. S., Dunkel-Schetter, C., DeLongis, A., & Gruen, R. J. (1986). Dynamics of a stressful encounter: Cognitive appraisal, coping, and encounter outcomes. *Journal of Personality and Social Psychology*. https://doi.org/10.1037/0022-3514.50.5.992

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50.

Frydenberg, M., & Lorenz, B. (2020). Lizards in the street! introducing cybersecurity awareness in a digital literacy context. In *Information Systems Education Journal (ISEDJ)* (Vol. 18, Issue 4). https://isedj.org/;http://iscap.info

Garofalo, J. (1987). Reassessing the lifestyle model of criminal victimization. *Positive Criminology*, 23–42.

Gibbs, S., Moore, K., Steel, G., & McKinnon, A. (2017). The dunning-kruger effect in a workplace computing setting. *Computers in Human Behaviour*, *72*, 589–595. https://doi.org/10.1016/j.chb.2016.12.084

Goundar, S. (2021). Introductory chapter: Introduction to e-Services. In *e-Services*. IntechOpen. https://doi.org/10.5772/intechopen.99605

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behaviour intentions. *Computers and Security*, *73*, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Grimes, M., & Marquardson, J. (2019). Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions. *Decision Support Systems*, *119*(February), 23–34. https://doi.org/10.1016/j.dss.2019.02.010

Gruber, S. (2020). Personal trust and system trust in the sharing economy: A comparison of community- and platform-based models. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.581299

Guedes, I., Martins, M., & Cardoso, C. S. (2023). Exploring the determinants of victimization and fear of online identity theft: An empirical study. *Security Journal*, *36*(3), 472–497. https://doi.org/10.1057/s41284-022-00350-5

Guerra, C., & Ingram, J. R. (2022). Assessing the relationship between lifestyle routine activities theory and online victimization using panel data. *Deviant Behaviour*, *43*(1), 44–60. https://doi.org/10.1080/01639625.2020.1774707

Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: An empirical investigation. In *Information Management and Computer Security*. https://doi.org/10.1108/09685220910978112

Haag, S., Siponen, M., & Liu, F. (2021). Protection motivation theory in information systems security research: A review of the past and a road map for the future. *Data Base for Advances in Information Systems*, *52*(2), 25–67. https://doi.org/10.1145/3462766.3462770

Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behaviour. *International Conference on Information Systems*, 1–16. https://aisel.aisnet.org/icis2013/proceedings/SecurityOfIS/9

Hair, J., Anderson, R., Babin, B., & Black, W. (2019). Multivariate data analysis. In *Australia : Cengage* (8th ed.). Pearson Prentice Hall.

Hair, J. F. , Hult, G. T., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM) second edition* (2nd ed.). Sage.

Hair, J. F., Hult, G. T. M. , Ringle, C. M. , & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). Sage. https://www.smartpls.com/documentation/getting-started/pls-sem-book/

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24.

Hanus, B., & Wu, Y. "Andy." (2016). Impact of users' security awareness on desktop security behaviour: A protection motivation theory perspective. *Information Systems Management*. https://doi.org/10.1080/10580530.2015.1117842

Haque, A., Karim, W., Md, S., Kabir, H., & Kumar Tarofder, A. (2020). Understanding social distancing intention among university students during Covid-19 outbreak: An application of protection motivation theory. *Test Engineering and Management*, *83*(May-June 2020), 16360–16377. https://www.researchgate.net/publication/342047665

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*, *40*(2), 265–281. https://doi.org/10.1108/OIR-04-2015-0106

Hassandoust, F., Singh, H., & Williams, J. (2023). The role of contextualization in users' vulnerability to phishing attempts. *Australasian Journal of Information Systems*, *24*, 1–32.

Hassandoust, F., & Techatassanasoontorn, A. A. (2019). Understanding users' information security awareness and intentions: A full nomology of protection motivation theory. In *Cyber Influence and Cognitive Threats* (pp. 129–143). Elsevier. https://doi.org/10.1016/B978-0-12-819204-7.00007-5

Hatem, G., Zeidan, J., Goossens, M., & Moreira, C. (2022). Normality testing methods and the importance of skewness and kurtosis in statistical analysis. *BAU Journal - Science and Technology*, *3*(2). https://doi.org/10.54729/ktpe9512

Henseler, J., Ringle, C. M., & Sarstedt, M. (2016). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing*, *20*(January), 277–319. https://doi.org/10.1108/S1474-7979(2009)0000020014

Henson, B., Wilcox, P., Reyns, B. W., & Cullen, F. T. (2010). Gender, adolescent lifestyles, and violent victimization: Implications for routine activity theory. *Victims and Offenders*, *5*(4), 303–328. https://doi.org/10.1080/15564886.2010.509651

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*. https://doi.org/10.1057/ejis.2009.6

Hewitt, B., & White, G. L. (2022). Optimistic bias and exposure affect security incidents on home computer. *Journal of Computer Information Systems*, *62*(1), 50–60. https://doi.org/10.1080/08874417.2019.1697860

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. In *Expert Systems with Applications* (Vol. 193). Elsevier Ltd. https://doi.org/10.1016/j.eswa.2021.116429

Hindelang, M. J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*.

Holt, T. J., van Wilsem, J., van de Weijer, S., & Leukfeldt, R. (2020). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review*, *38*(2), 187–206. https://doi.org/10.1177/0894439318805067

Hong, Y., & Furnell, S. (2019). Organizational formalization and employee information security behavioural intentions based on an extended TPB model. *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1–4. https://doi.org/10.1109/CyberSecPODS.2019.8885405

Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). *Communication and persuasion*.

Hunton, P. (2009). The growing phenomenon of crime and the internet: A cybercrime execution and analysis model. *Computer Law and Security Review*, *25*(6), 528–535. https://doi.org/10.1016/j.clsr.2009.09.005

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Computers and Security*. https://doi.org/10.1016/j.cose.2011.10.007

Ikart, E. M. (2019). Survey questionnaire survey pretesting method: An evaluation of survey questionnaire via expert reviews technique. *Asian Journal of Social Science Studies*, *4*(2), 1. https://doi.org/10.20849/ajsss.v4i2.565

Interpol. (2021). *ASEAN Cyberthreat Assessment 2021*. https://www.interpol.int/en/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf

Jansen, J., & Van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security*. https://doi.org/10.1108/ICS-03-2017-0018

Jansen, J., & van Schaik, P. (2018a). Persuading end users to act cautiously online: A fear appeals study on phishing. *Information and Computer Security*, *26*(3), 264–276. https://doi.org/10.1108/ICS-03-2018-0038

Jansen, J., & van Schaik, P. (2018b). Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behaviour*, *87*, 371–383. https://doi.org/10.1016/j.chb.2018.05.010

Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, *123*, 40–55. https://doi.org/10.1016/j.ijhcs.2018.10.004

Jensen, G. F., & Brownfield, D. (1986). Gender, lifestyles, and victimization: Beyond routine activity. In *Violence and Victims* (Vol. 1, Issue 2).

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviours: An empirical study. *MIS Quarterly: Management Information Systems*, *34*(SPEC. ISSUE 3), 549–566. https://doi.org/10.2307/25750691

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly: Management Information Systems*, *39*(1), 113–134. https://doi.org/10.25300/MISQ/2015/39.1.06

Joseph, D. L., & Newman, D. A. (2010). Emotional intelligence: An integrative meta-analysis and cascading model. *Journal of Applied Psychology*, *95*(1), 54.

Jun, Y., Craig, A., Shafik, W., & Sharif, L. (2021). Artificial intelligence application in cybersecurity and cyberdefense. *Wireless Communications and Mobile Computing*, 1–10. https://doi.org/10.1155/2021/3329581

Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults. *Cyberpsychology, Behaviour, and Social Networking*, *21*(2), 129–137. https://doi.org/10.1089/cyber.2016.0728

Kasinathan, S. (2023). Bank Negara clarifies cyber threat alert after warning on pro-Israeli hacker targeting Malaysian organisations spreads. *MalayMail*. https://www.malaymail.com/news/malaysia/2023/10/27/bank-negara-clarifies-cyber-threat-alert-after-warning-on-pro-israeli-hacker-targeting-malaysian-organisations-spreads/98657

Kaspersky. (2020). *What is cyber security?* Kaspersky. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kemp, S. (2023). Exploring public cybercrime prevention campaigns and victimization of businesses: A bayesian model averaging approach. *Computers & Security*, *127*, 103089. https://doi.org/https://doi.org/10.1016/j.cose.2022.103089

Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The dark figure and the cyber fraud rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*, *26*(3), 293–312. https://doi.org/10.1007/s10610-020-09439-2

Kerr, D. S., Loveland, K. A., Smith, K. T., & Smith, L. M. (2023). Cryptocurrency risks, fraud cases, and financial performance. *Risks*, *11*(3). https://doi.org/10.3390/risks11030051

Khan, I. (2012). An introduction to computer viruses: Problems and solutions. *Library Hi Tech News*, *29*(7), 8–12. https://doi.org/10.1108/07419051211280036

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on kirkpatrick's model. *Computers & Security*, *125*, 103049.

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267. https://doi.org/10.1016/J.COSE.2021.102267

Kirwan, G. H., Fullwood, C., & Rooney, B. (2018). Risk factors for social networking site scam victimization among Malaysian students. *Cyberpsychology, Behaviour, and Social Networking*, *21*(2), 123–128. https://doi.org/10.1089/cyber.2016.0714

Knapova, L., Kruzikova, A., Dedkova, L., & Smahel, D. (2021). Who is smart with their smartphones? determinants of smartphone security behaviour. *Cyberpsychology, Behaviour, and Social Networking*, *24*(9), 584–592.

Kock, N. (2021). *WarpPLS user manual: Version 7.0* (pp. 1–142). ScriptWarp Systems. www.scriptwarp.com

Kock, N., & Lynn, G. S. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. In *Journal of the Association for Information Systems* (Vol. 13, Issue 7).

Kont, K. R. (2023). Cyber literacy skills of Estonians: Activities and policies for encouraging knowledge-based cyber security attitudes. *Information and Media*, *96*, 80–94. https://doi.org/10.15388/Im.2023.96.67

Kumar, S., & Agarwal, D. (2018). Hacking attacks, methods, techniques and their protection measures. *International Journal of Advance Research in Computer Science and Management*, *4*, 2253–2257. www.ijsart.com

Kumara, S. (2022). Orang Melayu paling ramai jadi mangsa scammer. *MalaysiaGazette*, 1–3. https://malaysiagazette.com/2022/06/22/orang-melayu-paling-ramai-jadi-mangsa-scammer/

Kvasnicova, T., Kremenova, I., & Fabus, J. (2016). From an analysis of e-services definitions and classifications to the proposal of new e-service classification. *Procedia Economics and Finance*, *39*, 192–196. https://doi.org/10.1016/s2212-5671(16)30282-9

Lankton, N. K., McKnight, D. H., & Thatcher, J. B. (2012). The moderating effects of privacy restrictiveness and experience on trusting beliefs and habit: An empirical test of intention to continue using a social networking website. *IEEE Transactions on Engineering Management*, *59*(4), 654–665. https://doi.org/10.1109/TEM.2011.2179048

Larasati Irawan, R., & Hurriyati, R. (2021). *The effects of subjective norm on the intention to use of the online shopping customers in Bandung*. https://www.statista.com/statistics/276623/number-

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(9), 1–10. http://www.crimesciencejournal.com/content/3/1/9

Latan, H., & Noonan, R. (2017). Partial least squares path modeling: Basic concepts, methodological issues and applications. In *Partial Least Squares Path Modeling: Basic Concepts, Methodological Issues and Applications*. Springer International Publishing. https://doi.org/10.1007/978-3-319-64069-3

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behaviour and Information Technology*, *27*(5), 445–454. https://doi.org/10.1080/01449290600879344

Lesjak, B., & Čretnik, M. (2021). How individuals care for personal data protection when using online services. *International Journal of Management, Knowledge and Learning*, *10*, 139–148. https://doi.org/10.53615/2232-5697.10.139-148

Leuprecht, C., Skillicorn, D. B., & Tait, V. E. (2016). Beyond the castle model of cyber-risk and cyber-security. *Government Information Quarterly*, *33*(2), 250–257. https://doi.org/10.1016/j.giq.2016.01.012

Lewis, B. R., Templeton, G. F., & Byrd, T. A. (2005). A methodology for construct development in MIS research. *European Journal of Information Systems*, *14*(4), 388–400. https://doi.org/10.1057/palgrave.ejis.3000552

Li, R., & Suh, A. (2015). Factors influencing information credibility on social media platforms: Evidence from facebook pages. *Procedia Computer Science*, *72*, 314–328. https://doi.org/10.1016/j.procs.2015.12.146

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Liang, H., & Xue, Y. (2010). Understanding security behaviours in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*. https://doi.org/10.17705/1jais.00232

Lošonczi, P. (2018). Importance of dealing with cybersecurity challenges and cybercrime in the senior population. *Security Dimensions*, *26*(26), 173–186. https://doi.org/10.5604/01.3001.0012.7249

Luo, X., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the heuristic-systematic model: A theoretical framework and an exploration. *Computers and Security*, *38*, 28–38. https://doi.org/10.1016/j.cose.2012.12.003

Lwin, M. O., Li, B., & Ang, R. P. (2012). Stop bugging me: An examination of adolescents' protection behaviour against online harassment. *Journal of Adolescence*, *35*(1), 31–41. https://doi.org/10.1016/j.adolescence.2011.06.007

Ma, X. (2022). IS professionals' information security behaviours in Chinese IT organizations for information security protection. *Information Processing & Management*, *59*(1), 102744. https://doi.org/10.1016/j.ipm.2021.102744

Machuletz, D., Sendt, H., Laube, S., & B□hme, R. (2017). Users protect their privacy if they can: Determinants of webcam covering behaviour. *Proceedings of the European Workshop on Usable Security at the Privacy Enhaning Technologies Symposium* , 1–11. https://doi.org/10.14722/eurousec.2016.23014

Madanchian, M., & Taherdoost, H. (2016). Evaluation of electronic services' usage in Malaysia. In *International Journal of Engineering Issues* (Vol. 2016, Issue 2). https://www.researchgate.net/publication/305323671

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*. https://doi.org/10.1016/0022-1031(83)90023-9

Mahmud, I., Ramayah, T., Nayeem, Md. M. H., Islam, S. M. M. M., & Gan, P. L. (2016). Modelling cyber-crime protection behaviour among computer users in the context of Bangladesh. In *Design Solutions for User-Centric Information Systems*. https://doi.org/10.4018/978-1-7998-2466-4.ch021

Majlis Keselamatan Negara. (2022). *Awas! scam sindiket TAC*. https://www.mkn.gov.my/web/ms/2022/03/23/awas-scam-sindiket-tac/

Malay Mail. (2019). *TAC scams: What are they and how to avoid falling prey*. 1–11. https://www.malaymail.com/news/money/2019/01/28/tac-scams-what-are-they-and-how-to-avoid-falling-prey/1717198

Malay Mail. (2023a). Bank Negara clarifies cyber threat alert after warning on pro-Israeli hacker targeting Malaysian organisations spreads. *Malay Mail*.

Malay Mail. (2023b). Malaysians suffer RM302m losses in online scams from 2021 to June 2023, says deputy minister. *Malay Mail*, 1–5.

Malay Mail. (2024). With Malaysians losing billions of ringgit to online scams, Guan Eng moots IGP lead special task force in war against fraudsters. *Malay Mail*. https://www.malaymail.com/news/malaysia/2024/06/04/with-malaysians-losing-billions-of-ringgit-to-online-scams-guan-eng-moots-igp-lead-special-task-force-in-war-against-fraudsters/138035

Malaysiakini. (2020). Scam Alert: Don't give banking password to "LHDN." *Malaysiakini*.

Marett, K., Vedadi, A., & Durcikova, A. (2019). A quantitative textual analysis of three types of threat communication and subsequent maladaptive responses. *Computers & Security*, *80*, 25–35. https://doi.org/https://doi.org/10.1016/j.cose.2018.09.004

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behaviour*, *92*(May 2018), 139–150. https://doi.org/10.1016/j.chb.2018.11.002

Maurya, S., & Jain, A. (2020). Deep learning to combat phishing. *Journal of Statistics and Management Systems*, *23*(6), 945–957.

McCombie, S., & Pieprzyk, J. (2010). Winning the phishing war: A strategy for Australia. *2010 Second Cybercrime and Trustworthy Computing Workshop*, 79–86.

McCroskey, J. C., Richmond, V. P., Sallinen, A., Fayer, J. M., & Barraclough, R. A. (1995). A cross-cultural and multi-behavioural analysis of the relationship between nonverbal immediacy and teacher evaluation. *Communication Education*, *44*(4), 281–291.

McGill, T., & Thompson, N. (2018). *Gender differences in information security perceptions and behaviour*. https://doi.org/10.5130/acis2018.co

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Methmali, S. (2016). Perception of internet usage and its impact on cyber-crime in Sri Lanka. *International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016 : IEEE Conference Proceedings*, 674–690.

Metzger, M. J., Flanagin, A. J., Eyal, K., Lemus, D. R., & McCann, R. M. (2003). Credibility for the 21st century: Integrating perspectives on source, message, and media credibility in the contemporary media environment. *Annals of the International Communication Association*, *27*(1), 293–335.

Milani, R., Caneppele, S., & Burkhardt, C. (2022). Exposure to cyber victimization: Results from a Swiss survey. *Deviant Behaviour*, *43*(2), 228–240. https://doi.org/10.1080/01639625.2020.1806453

Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology*. https://doi.org/10.1348/135910702169420

M'manga, A., Faily, S., Mcalaney, J., & Williams, C. (2017). System design considerations for risk perception. *Proceedings - International Conference on Research Challenges in Information Science*, 322–327.

Mokhsin, M., Aziz, A. A., Zainol, A. S., Humaidi, N., & Zaini, N. A. A. (2019). Probability model: Malaysian consumer online shopping behaviour towards online shopping scam. *International Journal of Academic Research in Business and Social Sciences*, *9*(1), 1529–1538. https://doi.org/10.6007/ijarbss/v9-i1/5478

Morrison, B., Coventry, L., & Briggs, P. (2021). How do older adults feel about engaging with cyber-security? *Human Behaviour and Emerging Technologies*, *3*(5), 1033–1049. https://doi.org/10.1002/hbe2.291

mStar. (2022). *Labur sedikit, dipaksa tukar pakej mahal... ada yang sampai tangguh kahwin! Ramai miskin selepas "bantu" scammer jadi kaya*. https://www.mstar.com.my/lokal/viral/2022/09/30/labur-sedikit-dipaksa-tukar-pakej-mahal-ada-yang-sampai-tangguh-kahwin-ramai-miskin-selepas-bantu-scammer-jadi-kaya

Muhamad Saiful Bahri, Y. (2019). ABC of content validation and content validity index calculation. *Education in Medicine Journal*, *11*(2), 49–54. https://doi.org/10.21315/eimj2019.11.2.6

Muhammad Ikhsan, Asrizal, Muhammad Fithriani, Ali Habibi, M Ridwan, Ibnu Rusydi, A. Sipahutar, A., & Suhardi, B. (2021). Digital literacy in the post-truth era: Employing fact-checking applications in adult EFL reading classes. *KnE Social Sciences*, 468–481. https://doi.org/10.18502/kss.v5i4.8704

Mustaine, E. E., & Tewksbury, R. (1998). Predicting risks of larceny theft victimization: A routine activity analysis using refined lifestyle measures. *Criminology*, *36*, 829–858.

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. In *Computers and Security* (Vol. 132). Elsevier Ltd. https://doi.org/10.1016/j.cose.2023.103387

Nazura Abdul Manap, Anita Abdul Rahim, & Hossein Taji. (2015). Cyberspace identity theft: The conceptual framework. *Mediterranean Journal of Social Sciences*, *6*(4S3), 595–605. https://doi.org/10.5901/mjss.2015.v6n4s3p595

New Straits Times. (2020). Cybercrime in Penang shoots up 441.7 per cent since MCO. *New Straits Times*. http://biztrust.ssm.com.my

New Straits Times. (2023). Malaysia faces increasing cybersecurity threats. *New Straits Times*.

Newman, G. R., & Clarke, R. V. (2013). *Superhighway robbery* (1st ed.). Willan. https://doi.org/doi.org/10.4324/9781843924876

Ngo, F., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*.

Ngo, F. T., Piquero, A. R., LaPrade, J., & Duong, B. (2020). Victimization in cyberspace: Is it how long we spend online, what we do online, or what we post online? *Criminal Justice Review*, *45*(4), 430–451. https://doi.org/10.1177/0734016820934175

Nobanee, H., Alodat, A., Bajodah, R., Al-Ali, M., & Al Darmaki, A. (2023). Bibliometric analysis of cybercrime and cybersecurity risks literature. *Journal of Financial Crime*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/JFC-11-2022-0287

Noe, R. A., Hollenbeck, J. R., Gerhart, B., & Wright, P. M. (2020). *Fundamentals of human resource management*. McGraw-Hill.

Nordin, R. (2020). *Cops record 20% increase in phone scams during MCO period*. https://www.thestar.com.my/news/nation/2020/05/19/cops-record-20-increase-in-phone-scams-during-mco-period

Nur Farhana, M. Z., & Mazurina, M. A. (2021). Phishing as cyber fraud: The implications and governance. *Journal of Social Sciences*, *57*, 119–133. www.malaysiaairlines.com,

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Guidelines for usable cybersecurity: past and present. *2011 Third International Workshop on Cyberspace Safety and Security (CSS)*, 21–26.

Nurulatiq Ahmad, B. (2019). Ancaman jenayah scam. *SinarHarian*, 1–5. https://m.sinarharian.com.my/mobile-article?articleid=71853

Ogbanufe, O. (2023). Securing online accounts and assets: An examination of personal investments and protection motivation. *International Journal of Information Management*, *68*. https://doi.org/10.1016/j.ijinfomgt.2022.102590

Ogbanufe, O., & Pavur, R. (2022). Going through the emotions of regret and fear: Revisiting protection motivation for identity theft protection. *International Journal of Information Management*, *62*(August 2021), 102432. https://doi.org/10.1016/j.ijinfomgt.2021.102432

Ophoff, J., & Lakay, M. (2019). Mitigating the ransomware threat: A protection motivation theory approach. *Communications in Computer and Information Science*. https://doi.org/10.1007/978-3-030-11407-7_12

Oseni, K. O., Dingley, K., & Hart, P. (2015). Barriers facing e-service technology in developing countries: A structured literature review with Nigeria as a case study. *International Conference on Information Society (i-Society)*. 10.1109/i-Society.2015.7366867

Ousey, G. C., Wilcox, P., & Brummel, S. (2008). Déjà vu all over again: Investigating temporal continuity of adolescent victimization. *Journal of Quantitative Criminology*, *24*(3), 307–335. https://doi.org/10.1007/s10940-008-9046-6

Pallant, J. (2020). *SPSS survival manual: A step by step guide to data analysis using IBM SPSS* (7th ed.). McGraw-Hill Education. www.allenandunwin.com/spss

Partin, R. D., Meldrum, R. C., Lehmann, P. S., Back, S., & Trucco, E. M. (2022). Low self-control and cybercrime victimization: An examination of indirect effects through risky online behaviour. *Crime & Delinquency*, *68*(13–14), 2476–2502.

Payne, B. K., & Hadzhidimova, L. (2018). Cyber security and criminal justice programs in the United States: Exploring the intersections. *International Journal of Criminal Justice Sciences*, *13*(2), 385–404.

Pedrosa, A. L., Bitencourt, L., Fróes, A. C. F., Cazumbá, M. L. B., Campos, R. G. B., de Brito, S. B. C. S., & Simões e Silva, A. C. (2020). Emotional, behavioural, and psychological impact of the COVID-19 pandemic. In *Frontiers in Psychology* (Vol. 11). Frontiers Media S.A. https://doi.org/10.3389/fpsyg.2020.566212

Phua, C., Lee, V., Smith, K., & Gayler. Ross. (2010). A comprehensive survey of data mining-based fraud detection research. *ArXiv Preprint ArXiv:1009.6119.*, 1–14.

Pleger, L. E., Guirguis, K., & Mertes, A. (2021). Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security. *Computers in Human Behaviour*, *122*. https://doi.org/10.1016/j.chb.2021.106830

Polit, D. F., Beck, C. T., & Owen, S. V. (2007). Is the CVI an acceptable indicator of content validity? appraisal and recommendations. *Research in Nursing & Health*, *30*(4), 459–467. https://doi.org/10.1002/NUR.20199

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267–296. https://doi.org/10.1177/0022427810365903

Qabajeh, I., Thabtah, F., & Chiclana, F. (2018). A recent review of conventional versus automated cybersecurity anti-phishing techniques. *Computer Science Review*, *29*, 44–55. https://doi.org/10.1016/j.cosrev.2018.05.003

Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. *International Journal of Economics & Management Sciences*, *06*(02). https://doi.org/10.4172/2162-6359.1000403

Ramayah, T., Cheah, J., Chuah, F., Ting, H., & Memon, M. A. (2018). Partial least squares structural equation modeling (PLS-SEM) using smartPLS 3.0. *An Updated Guide and Practical Guide to Statistical Analysis*.

Randa, R., & Reyns, B. W. (2020). The physical and emotional toll of identity theft victimization: A situational and demographic analysis of the national crime victimization survey. *Deviant Behaviour*, *41*(10), 1290–1304. https://doi.org/10.1080/01639625.2019.1612980

Rao, R. S., & Ali, S. T. (2015). A computer vision technique to detect phishing attacks. *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*. https://doi.org/10.1109/CSNT.2015.68

Rath, D. K., & Kumar, A. (2021). Information privacy concern at individual, group, organization and societal level: A literature review. *Vilakshan - XIMB Journal of Management*, *18*(2), 171–186. https://doi.org/10.1108/xjm-08-2020-0096

Raz, J. (2017). *Intention and motivation*. *556*. https://scholarship.law.columbia.edu/faculty_scholarship/2044

Redmiles, E. M., Malone, A. R., & Mazurek, M. L. (2016). I think they're trying to tell me something: Advice sources and selection for digital security. *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, 272–288. https://doi.org/10.1109/SP.2016.24

Reid, R., & Van Niekerk, J. (2016). Decoding audience interpretations of awareness campaign messages. *Information and Computer Security*, *24*(2), 177–193. https://doi.org/10.1108/ICS-01-2016-0003

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216–238. https://doi.org/10.1177/0022427811425539

Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian general social survey. *Journal of Financial Crime*, *22*(4), 396–411. https://doi.org/10.1108/JFC-06-2014-0030

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none. In *International Journal of Offender Therapy and Comparative*

Criminology (Vol. 60, Issue 10, pp. 1119–1139). SAGE Publications Inc. https://doi.org/10.1177/0306624X15572861

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behaviour*, *38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Reyns, B. W., Randa, R., & Henson, B. (2016). Preventing crime online: Identifying determinants of online preventive behaviours using structural equation modeling and canonical correlation analysis. *Crime Prevention and Community Safety*, *18*(1), 38–59. https://doi.org/10.1057/cpcs.2015.21

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In *Handbook of health behaviour research 1: Personal and social determinants* (pp. 113–132). https://doi.org/10.4135/9781483332222.n225

Rogers, W. R. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*.

Sacco, V., & Kennedy, L. W. (2002). *The criminal event: Perspectives in space and time*. Cengage Learning.

Saeed, S. (2023). Education, online presence and cybersecurity implications: A study of information security practices of computing students in Saudi Arabia. *Sustainability (Switzerland)*, *15*(12). https://doi.org/10.3390/su15129426

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78. https://doi.org/10.1016/J.COSE.2015.05.012

Sahney, S. (2017). *Module 6: Consumer behaviour* (pp. 1–16).

Saleemi, M., Anjum, M., & Rehman, M. (2017). E-services classification, trends, and analysis: A systematic mapping study. In *IEEE Access* (Vol. 5, pp. 26104–26123). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2017.2766287

Salina Daud, Nurazariah Abidin, Noraina Mazuin Sapuan, & Jegatheesan Rajadurai. (2012). Efficient human resource deployment technique in higher education: A

standpoint from Malaysia. *African Journal of Business Management*, *6*(25). https://doi.org/10.5897/ajbm11.558

Sameen, M., Han, K., & Hwang, S. O. (2020). PhishHaven - An efficient real-time AI phishing URLs detection system. *IEEE Access*, *8*, 83425–83443. https://doi.org/10.1109/ACCESS.2020.2991403

San Miguel, C., Morales, K., & Antonius Ynalvez, M. (2020). Online victimization, social media utilization, and cyber crime prevention measures. In *Asia-Pacific Social Science Review* (Vol. 20).

Sandywell, B. (2010). *On the globalisation of crime: The Internet and new criminality* (pp. 38–66). Willan Publishing.

Sarstedt, M., & Mooi, E. (2019). *A concise guide to market research: The process, data, and methods using IBM SPSS statistics* (3rd ed.). Springer, Heidelberg.

Sarstedt, M., Ringle, C. M., & Hair, J. F. (2017). Partial least squares structural equation modeling. In *Handbook of Market Research* (pp. 1–40). Springer International Publishing. https://doi.org/10.1007/978-3-319-05542-8_15-1

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2020). *Research methods for business students* (8th ed.). Pearson. www.pearson.com/uk

ScamWatch. (2020). *Scam statistics*. https://www.scamwatch.gov.au/research-and-resources/scam-statistics

Schreck, C. J., Miller, J. M., & Gibson, C. L. (2003). Trouble in the school yard: A study of the risk factors of victimization at school. *Crime & Delinquency*, *49*(3), 460–484. https://doi.org/10.1177/0011128703252275

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2021). Employees' behaviour in phishing attacks: What individual, organizational, and technological factors matter? *Journal of Computer Information Systems*, *61*(6), 539–550. https://doi.org/10.1080/08874417.2020.1812134

Shaheera, A. S. (2019). 63% of fraudulent cases in Malaysia occurred online. *The Malaysian Reserve*, 1–2. https://themalaysianreserve.com/2019/10/29/63-of-fraudulent-cases-in-malaysia-occurred-online/

Shao, J., Zhang, Q., Ren, Y., Li, X., & Lin, T. (2019). Why are older adults victims of fraud? current knowledge and prospects regarding older adults' vulnerability to fraud. *Journal of Elder Abuse and Neglect*, *31*(3), 225–243. https://doi.org/10.1080/08946566.2019.1625842

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). *Online safety begins with you and me: Convincing Internet users to protect themselves*. https://doi.org/10.1016/j.chb.2015.01.046

Shmueli, G., & Koppius, O. (2011). Predictive analytics in information systems research. *Economics of Networks EJournal.*, *35*(3), 553–572. https://doi.org/10.2139/ssrn.1606674

Shmueli, G., Ray, S., Velasquez Estrada, J. M., & Chatla, S. B. (2017). The elephant in the room: Predictive performance of PLS models. *Journal of Business Research*, *69*(10), 4552–4564. https://doi.org/10.1016/j.jbusres.2016.03.049

Shmueli, G., Sarstedt, M., Hair, J. F., Cheah, J. H., Ting, H., Vaithilingam, S., & Ringle, C. M. (2019). Predictive model assessment in PLS-SEM: Guidelines for using PLSpredict. *European Journal of Marketing*, *53*(11), 2322–2347. https://doi.org/10.1108/EJM-02-2019-0189

Shubham, Kumar, R., Aditya, A., & Shivahare, B. D. (2023). Cyber crime prevention and techniques: A comprehensive survey. *2023 3rd International Conference on Innovative Sustainable Computational Technologies (CISCT)*, 1–4. https://doi.org/10.1109/CISCT57197.2023.10351225

Siddique, M. A. M. (2012). Explaining the role of perceived risk, knowledge, price, and cost in dry fish consumption within the theory of planned behaviour. *Journal of Global Marketing*, *25*(4), 181–201. https://doi.org/10.1080/08911762.2012.743203

Sitti Syamsiar Muharram, Mohd Zuhairizan, S., & Marcus, M. (2022). Cybercrimes in Malaysia. *Journal of Education and Social Sciences*, *22*(1), 34–38.

Siyed, Z. (2023). A new cyber risk: How teens expose corporations in WFH era. *Journal of Information Security*, *14*(04), 396–421. https://doi.org/10.4236/jis.2023.144022

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy*. https://doi.org/10.4018/IJISP.2015010102

Srisawang, S., Thongmak, M., & Ngarmyarn, A. (2015). Factors affecting computer crime protection behaviour. *Pacific Asia Conference on Information Systems, PACIS 2015 - Proceedings*.

Stewart, G. L., Courtright, S. H., & Barrick, M. R. (2012). Peer-based control in self-managing teams: Linking rational and normative influence with individual and group performance. *Journal of Applied Psychology*, *97*(2), 435.

Stouffer, C. (2022). *Online scams: An overview + 20 internet scams to avoid in 2024*. Gen Digital Inc.

Szumski, O. (2018). Cybersecurity best practices among Polish students. *Procedia Computer Science*, *126*, 1271–1280. https://doi.org/10.1016/j.procS.2018.08.070

Tăbușcă, A., Garais, G., & Enăceanu, A. (2022). Cybersecurity education: The new literacy. *Journal of Information Systems & Operations Management*, *16*. https://www.rferl.org/

Taherdoost, H. (2017). Understanding of e-service security dimensions and its effect on quality and intention to use. *Information & Computer Security*, *25*(5), 535–559. https://doi.org/10.1108/ICS-09-2016-0074

Taherdoost, H., Sahibuddin, S., & Jalaliyoon, N. (2015). A review paper on e-service: Technology concepts. *Procedia Technology*, *19*, 1067–1074. https://doi.org/10.1016/j.protcy.2015.02.152

Tang, Z., Miller, A. S., Zhou, Z., & Warkentin, M. (2021). Does government social media promote users' information security behaviour towards COVID-19 scams? Cultivation effects and protective motivations. *Government Information Quarterly*, *38*(2), 101572. https://doi.org/10.1016/j.giq.2021.101572

Telo, J. (2021). Privacy and cybersecurity concerns in smart governance systems in developing countries. *Tensorgate Journal of Sustainable Technology and Infrastructure for Developing Countries*, *4*(1), 1–13. https://orcid.org/0009-0004-5101-8064

The Star. (2024). RM3.2bil lost to online scams from 2020 to 2023, says Kulasegaran. *The Star*, 1–6. https://www.thestar.com.my/news/nation/2024/03/04/rm23bil-lost-to-online-scams-from-2020-to-2023-says-kulasegaran#:~:text=2bil%20has%20been%20lost%20to,government%20to%20tackle%20the%20issue.

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behaviour. *Computers and Security*, *70*(September), 376–391. https://doi.org/10.1016/j.cose.2017.07.003

Tillyer, M. S., Gialopsos, B. M., & Wilcox, P. (2016). The short-term repeat sexual victimization of adolescents in school. *Crime and Delinquency*, *62*(1), 81–106. https://doi.org/10.1177/0011128713501026

Tillyer, M. S., Wilcox, P., & Fissel, E. R. (2018). Violence in schools. *Source: Journal of Quantitative Criminology*, *34*(2), 609–632. https://doi.org/10.2307/48701203

Tsai, H. Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviours: A protection motivation theory perspective. *Computers and Security*, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft. *Information and Management*, *52*(4), 506–517. https://doi.org/10.1016/J.IM.2015.03.002

Turanovic, J. J., Pratt, T. C., & Piquero, A. R. (2018). Structural constraints, risky lifestyles, and repeat victimization. *Source: Journal of Quantitative Criminology*, *34*(1), 251–274. https://doi.org/10.2307/48701149

Tyugu, E. (2011). Artificial intelligence in cyber defense. *In 2011 3rd International Conference on Cyber Conflict* , 1–12.

Vafaei-Zadeh, A., Thurasamy, R., & Hanifah, H. (2019). Modeling anti-malware use intention of university students in a developing country using the theory of planned behaviour. *Kybernetes*, *48*(8), 1565–1585. https://doi.org/10.1108/K-05-2018-0226

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse

victimization. *Http://Dx.Doi.Org/10.1177/1043986215621379*, *32*(2), 169–188. https://doi.org/10.1177/1043986215621379

Van Laar, E., van Deursen, A. J. A. M., van Dijk, J. A. G. M., & de Haan, J. (2017). The relation between 21st-century skills and digital skills: A systematic literature review. *Computers in Human Behaviour*, *72*, 577–588. https://doi.org /10.1016/j.chb.2017.03.010

Van Laar, E., van Deursen, A. J. A. M., van Dijk, J. A. G. M., & de Haan, J. (2020). Determinants of 21st-century skills and 21st-century digital skills for workers: A systematic literature review. *SAGE Open*, *10*(1). https://doi.org/ 10.1177/2158244019900176

van Schaik, P., Renaud, K., Wilson, C., Jansen, J., & Onibokun, J. (2020). Risk as affect: The affect heuristic in cybersecurity. *Computers and Security*, *90*. https://doi.org/10.1016/j.cose.2019.101651

Van Wilsem, J. (2011). Worlds tied together? online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, *8*(2), 115–127. https://doi.org/10.1177 /1477370810393156

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information and Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Vanhee, A. J., & McNealey, R. (2023). Individual residence and identity theft: How residential characteristics shape exposure and risk of offline and online identity theft victimization. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-03-2023-0045

Verkijika, S. F. (2018). Understanding smartphone security behaviours: An extension of the protection motivation theory with anticipated regret. *Computers and Security*, *77*, 860–870. https://doi.org/10.1016/j.cose.2018.03.008

Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behaviour*, *101*(January), 286–296. https://doi.org/10.1016/ j.chb.2019.07.034

VinciWorks Group. (2018). *What is cyber fraud?*

Vitak, J., Liao, Y., Subramaniam, M., & Kumar, P. (2018). "I knew it was too good to be true": The challenges economically disadvantaged users face in assessing trustworthiness, avoiding scams, and developing self-efficacy online. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW). https://doi.org/10.1145/3274445

Vogt, W. P. (2007). Quantitative research methods for professionals. In *(No Title)*. Pearson Education.

Vousinas, G. L. (2019). Advancing theory of fraud: the S.C.O.R.E. model. *Journal of Financial Crime*, *26*(1), 372–381. https://doi.org/10.1108/JFC-12-2017-0128

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behaviour: A longitudinal study. *Decision Support Systems*, *92*(May 2018), 25–35. https://doi.org/10.1016/j.dss.2016.09.013

Warkentin, M., & Willison, R. (2009). Behavioural and policy issues in information systems security: The insider threat. In *European Journal of Information Systems*. https://doi.org/10.1057/ejis.2009.12

Warshaw, P. R., & Davis, F. D. (1985). The accuracy of behavioural intention versus behavioural expectation for predicting behavioural goals. *The Journal of Psychology*, *119*(6), 599–602.

Weeks, B. E., & Garrett, R. K. (2014). Electoral consequences of political rumors: Motivated reasoning, candidate rumors, and vote choice during the 2008 U.S. presidential election. *International Journal of Public Opinion Research*, *26*(4), 401–422. https://doi.org/10.1093/ijpor/edu005

Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal*. https://doi.org/10.1057/sj.2012.57

Whitty, M. T. (2018). Do you love me? psychological characteristics of romance scam victims. *Cyberpsychology, Behaviour, and Social Networking*. https://doi.org/10.1089/cyber.2016.0729

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/JFC-10-2017-0095

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behaviour, and Social Networking*. https://doi.org/10.1089/cyber.2011.0352

Whitty, M. T., & Buchanan, T. (2015). The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Http://Dx.Doi.Org/10.1177/1748895815603773*, *16*(2), 176–194. https://doi.org/10.1177/1748895815603773

Wilcox, P., & Cullen, F. T. (2018). Situational opportunity theories of crime. *Annual Review of Criminology*, *1*, 123–148. https://doi.org/10.1146/annurev-criminol

Wilcox, P., & Gialopsos, B. M. (2015). Crime-event criminology: An overview. *Journal of Contemporary Criminal Justice*, *31*(1), 4–11. https://doi.org/10.1177/1043986214552601

Williams, A. S., Maharaj, M. S., & Ojo, A. I. (2019). Employee behavioural factors and information security standard compliance in Nigeria banks. *International Journal of Computing and Digital Systems*, *8*(4). https://doi.org/10.12785/ijcds/080407

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human Computer Studies*, *120*(June), 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004

Wilson, T. D. (2002). The nonsense of "knowledge management." *Information Research*, *8*(1), 1–33. http://informationr.net/ir/8-1/paper144.html

Wineburg, S., & McGrew, S. (2019). Lateral reading and the nature of expertise: Reading less and learning more when evaluating digital information. *Teachers College Record*, *121*(11), 1–40. https://doi.org/10.1177/016146811912101102

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, *59*(4), 329–349. https://doi.org/10.1080/03637759209376276

Witten, I. H., Frank, E., Hall, M. A., & Pal, C. J. (2016). Data mining fourth edition: Practical machine learning tools and techniques. *San Francisco: Morgan Kaufmann Publishers Inc;*

Ye, S., & Ho, K. K. W. (2019). Would you feel happier if you have more protection behaviour? a panel survey of university students in Japan. *Behaviour and Information Technology*, *38*(4), 422–434. https://doi.org/10.1080/0144929X.2018.1544275

Yeoh, A. (2020). LHDN warns of SMS scam targeting Bantuan Prihatin Nasional recipients. *The Star*.

Yesuf, A. S., & Probst, C. W. (2018). Estimating the risk of fraud against e-services. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-030-03638-6_19

Yoon, C., Hwang, J. W., Kim, R., Cheolho Yoon1, carlyoon@empal. com, Jae-Won Hwang2, hjw504@Kunsan. ac. kr, & Kim rhkim@ucr.edu, R. (2012). Exploring factors that influence students' behaviours in information security. *Journal of Information Systems Education*, *23*(4), 407–415. https://proxy.library.mcgill.ca/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eft&AN=89084300&site=ehost-live&scope=site

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviours among young adolescents. *Journal of Consumer Affairs*. https://doi.org/10.1111/j.1745-6606.2009.01146.x

Zaabi, K. Al, & Tubaishat, A. (2015). Security awareness program for customers using online banking. *GSTF Journal on Computing (JoC) 2014 4:3*, *4*(3), 1–10. https://doi.org/10.7603/S40601-014-0019-3

Zahari, A. I., Bilu, R., & Said, J. (2019). *The role of familiarity, trust and awareness towards online fraud*. *6*(9), 2470–2480. https://doi.org/10.15520/jro.v6i9.

Zhang, L., & McDowell, W. C. (2009). Am i really at risk? determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, *8*(3–4), 180–197. https://doi.org/10.1080/15332860903467508

Zhu, Z., Liu, Y., Kapucu, N., & Peng, Z. (2020). Online media and trust in government during crisis: The moderating role of sense of security. *International Journal of Disaster Risk Reduction*, *50*. https://doi.org/10.1016/j.ijdrr.2020.101717

Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2013). *Business research methods*. Cengage Learning. https://books.google.com.my/books?id=veM4gQPnWHgC

Zou, Y., Roundy, K., Tamersoy, A., Shintre, S., Roturier, J., & Schaub, F. (2020, April 21). Examining the adoption and abandonment of security, privacy, and identity theft protection practices. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3313831.3376570

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behaviour: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

APPENDICES

Questionnaire feedback

Constructs	Questionnaire Items	Scale	Your Assessment			Comment	F
			Perfect Match (maintain item as it is)	Moderate Match (maintain item but needs some refining)	Poor Match (remove item)		
Source credibility	I believe emails from Malaysian government domain (.gov) are credible. *Saya percaya e-mel dari domain kerajaan Malaysia (.gov) boleh dipercayai. .adalah sahih.* *e-Services (.gov.my/.edu.my.)*	7-point of scale	E1: / E2: / E3: E4: /	E1: E2: E3: / E4:	E1: E2: E3: E4:	E1: - E2: - E3: Semak (.gov) atau Malaysian goverment (. gov.my) E4: Yes, I agree with this item. However, I have a different understanding on the word credible which to me it not translated to "boleh dipercayai". It is more towards sesuatu sumber yang sahih. Boleh dipercayai lebih merujuk kepada "trusted".	

	I believe emails from Malaysian government domain (.gov) tend to be free from grammatical errors. *Saya percaya e-mel dari domain kerajaan Malaysia (.gov) kebiasaannya bebas daripada kesalahan tatabahasa.*		E1: / E2: / E3: E4:	E1: E2: E3: / E4: /	E1: E2: E3: E4:	E1: - E2: - E3: Juga adakah semua responden menggunakan e-Services dan domain gov.my sahaja? E4: I do not have strong preference for this item as I think it does not really reflect directly with the source of credibility. Maybe you consider to use the term "trusted" here instead. "I believe emails from Malaysia government domain (.gov) can be trusted." If you introduce this, perhaps you can retain item no 1.	
	I believe emails from Malaysian government domain (.gov) tend to have a sense of urgency. *Saya percaya e-mel dari domain kerajaan Malaysia (.gov) kebiasaannya mendesak pengguna bertindak dengan segera.*		E1: / E2: / E3: E4: /	E1: E2: E3:/ E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Acceptable	
Perceived value data	I perceive the importance of regarding the security protection of my data in e-Services. *Saya merasakan pentingnya melindungi data saya dalam e-Perkhidmatan*.	7-point of scale	E1: / E2: E3: / E4: /	E1: E2: / E3: E4:	E1: E2: E3: E4:	E1: E2: I perceive the importance of security protection of my data in e-Services. E3: Semak e-Services/e-gov services or define e-Services. *answering below* E4: Suggestion:	R

						I would reword the English version to: "I perceived the importance of security protection towards my data in e-Services.	
	I am aware of the potential risk of monetary loss if there are breaches to my personal data. *Saya menyedari saya berkemungkinan menghadapi risiko kerugian wang sekiranya terdapat kejadian akses tanpa izin terhadap data peribadi saya.*		E1: / E2: E3: / E4: /	E1: E2: / E3: E4:	E1: E2: E3: E4:	E1: E2: Saya menyedari kemungkinan menghadapi risiko kerugian wang sekiranya terdapat kejadian akses tanpa izin terhadap data peribadi saya. E3: Dicadangkan lebih ringkas tetapi sekiranya maksud tidak sampai kekalkan. Contoh: I am aware of monetary loss if there are breaches to my personal data E4: I would reword the Malay version to; "Saya sedar akan kemungkinan menghadapi risiko kerugian wang sekiranya brlaku akses tanpa izin terhadap data peribadi saya".	R

	I perceived the e-Services high guarantee confidential of my personal data. *Saya merasakan e-Perkhidmatan dapat memberikan jaminan yang tinggi dalam merahsiakan data peribadi saya*		E1: / E2: E3: / E4: /	E1: E2: / E3: E4:	E1: E2: E3: E4:	E1: E2: I perceived the e-Services provide a high guarantee confidential of my personal data. E3: E4: Suggestion: I would reword both version to: "I perceived the e-Services can fully guarantee the confidentiality of my personal data. "Saya merasakan e-Perkhidmatan dapat memberikan sepenuh jaminan dalam merahsiakan data peribadi saya"	R E4
Subjective norm	Most people who are important to me think it is a good idea to logout after using e-Services account. *Kebanyakan kenalan rapat saya berpendapat adalah idea yang baik untuk log keluar setelah menggunakan akaun e-perkhidmatan.*	7-point of scale	E1: / E2: E3: / E4: /	E1: E2: / E3: E4:	E1: E2: E3: E4:	E1: E2: Kebanyakan kenalan rapat saya berpendapat adalah penting untuk log keluar setelah menggunakan akaun e-perkhidmatan. E3: Semak alih bahasa E4: This is an important construct-however, the question appears to be incomplete as it only stated what others think about the behaviour. How about whether one should perform it or not?	R

						I would suggest to revise the question as follows: “Most people who are close to me think it is important to logout after using e-Services account, hence it is important to me to do so.” “Kebanyakan kenalan rapat saya berpendapat bahawa ianya penting untuk log keluar setelah menggunakan akaun e-Perkhidmatan, maka dengan itu ianya penting untuk saya berbuat demikian”	
	Most people who are important to me think it is a good idea to not save password automatically when using e-Services account. *Kebanyakan kenalan rapat saya berpendapat bahawa adalah idea yang baik untuk tidak menyimpan kata laluan secara automatik apabila menggunakan akaun e-perkhidmatan.*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: Semak alih bahasa E4: I think maybe for this item you can try to reword accordingly as suggested above.	R

	Most people who are important to me think it is a good idea to more cautious when using e-Services. *Kebanyakan kenalan rapat saya berpendapat adalah idea yang baik untuk lebih berhati-hati apabila menggunakan e-perkhidmatan*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: Semak alih bahasa E4: Same here-please try to reword it to make it consistent with the above.	R
Wishful thinking	I wish I could use e-Services without increasing my security protection. *Saya harap saya dapat menggunakan e-Perkhidmatan tanpa meningkatkan perlindungan keselamatan saya.*	7-point of scale	E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Acceptable	
	I wish that the threat would go away or somehow not affected me. *Saya berharap bahawa ancaman siber akan hilang dan tidak akan memberi kesan kepada saya.*		E1: E2: / E3: / E4: /	E1: / E2: E3: E4:	E1: E2: E3: E4:	E1: When you use word OR, there is a possibility of the item to be double barrelled. I would suggest the items to be separated into two items, to be safe E2: E3: Semak “double barrel” E4: Acceptable	? split 2
	I hope I will not encounter any cyber threat situation.		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Acceptable	

	Saya harap saya tidak akan menghadapi sebarang situasi ancaman siber.						
Perceived threat severity	I believe that being a victim of cyber fraud in e-Services is a serious problem for me. *Saya percaya bahawa menjadi mangsa penipuan siber dalam e-Perkhidmatan adalah masalah serius bagi saya.*	7-point of scale	E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: It is better to simplify the sentence E2: E3: E4:	
	I believe that the time/masa loss to recover the damages (e.g., money loss, data loss) after being a victim of cyber fraud is a serious problem. *Saya percaya bahawa kerugian masa untuk memulih kerosakan selepas menjadi mangsa penipuan siber adalah masalah yang serius.*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: This sentence also needs to be simplified E2: E3: E4: I would like to suggest for item 2& 3 of this construct to be combined: Suggestion: I believe that the time and productivity loss to recover the damages (e.g.: money or data loss) after being a victim cyber fraud is a serious problem for me. *The reason for combining -time & productivity is view as related to one another- can maintain consistency of having 3 item per construct.	

	I believe that my productivity/effort loss to recover the damages (e.g., money loss, data loss) from being a victim of cyber fraud is a serious problem. (relate more on kerja)* doble check. *Saya percaya bahawa kehilangan produktiviti (cth.: Kehilangan pendapatan) untuk memulihkan daripada penipuan siber adalah masalah yang serius.* *Saya percaya bahawa kerugian produktiviti untuk memulih kerosakan (kehilangan harta,) selepas menjadi mangsa penipuan siber adalah masalah yang serius.* **maksud kerugian produktiviti*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: It is better if you could simplify this sentence E2: E3: E4:	
	I believe that the data/information loss from being a victim of cyber fraud is a serious problem. *Saya percaya bahawa kehilangan data/maklumat daripada menjadi mangsa penipuan siber adalah masalah yang serius*.		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: Saya percaya bahawa kehilangan data/maklumat akibat menjadi mangsa penipuan siber adalah masalah yang serius. E2: E3: E4: Acceptable	R

Perceived threat vulnerability	I am exposed to the cyber fraud threats of e-Services. *Saya terdedah kepada ancaman penipuan siber e-Perkhidmatan.*	7-point of scale	E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: Macam mana responden boleh rasa dirinya terdedah kepada ancaman penipuan siber? E3: E4:	
	I am at risk for being victimized by cyber fraud attackers. *Saya berisiko menjadi mangsa penyerang penipuan siber*.		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Suggestion to reword: "I am at risk of being victimized by cyber fraud attacker"	R
	It is likely that I will become a victim of cyber fraud. *Saya mungkin akan menjadi mangsa penipuan siber.*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Suggestion to reword: "It is possible for me to become a victim of cyber fraud." *No need attacker	R
Maladaptive rewards / Preventive countermeasures (d4)	I can save my time if I'm not using any preventive countermeasures application (e.g.: antivirus, anti-malware). *Saya dapat jimatkan masa saya jika saya tidak menggunakan sebarang aplikasi langkah balas pencegahan (contohnya: antivirus, anti-malware).*	7-point of scale	E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Acceptable	

	I can save my money if I'm not using any preventive countermeasure applications. *Saya dapat jimatkan wang saya jika saya tidak menggunakan sebarang aplikasi langkah balas pencegahan.*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4:	
	I will be better informed of the security risk if I'm using any preventive countermeasure applications. *Saya akan dimaklumkan dengan lebih baik mengenai risiko keselamatan jika saya menggunakan aplikasi pencegahan.*		E1: / E2: / E3: / E4:	E1: E2: E3: E4: /	E1: E2: E3: E4:	E1: E2: E3: E4: This item is slightly contradict with the OD for this construct. If you purposely place it for reverse effect then it has to be reworded so that it will not contradict with its original definition. Suggestion: I think it is a waste of effort to spend more money on anti-virus software to increase the protection against cyber fraud. *Further discussion and improvement, more jelas*	R E4

	I will spend less effort if I do not perform the recommendations of the preventive countermeasure applications. *Saya tidaklah perlu bersusah-payah sangat sekiranya saya tidak melaksanakan saranan-saranan aplikasi tindak balas pencegahan.*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Acceptable	
	I will feel less stressful if I do not perform the recommendations of the preventive countermeasure applications. *Saya akan berasa kurang tertekan jika tidak melaksanakan saranan-saranan aplikasi langkah balas pencegahan.*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Acceptable	
Response efficacy	When using preventive countermeasures application, a computers data is more likely to be protected. *Semasa menggunakan aplikasi langkah balas pencegahan, data komputer lebih berkemungkinan dilindungi.*	7-point of scale	E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Acceptable	

	Performing any cybersecurity recommendations would reduce the chance of myself from becoming cyber fraud victims. *Melakukan sebarang saranan-saranan keselamatan siber akan mengurangkan risiko saya menjadi mangsa penipuan siber.*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Acceptable	
	Performing any of the provided recommendations make me feel safe from cyber fraud attack. *Melaksanakan sebarang saranan-saranan keselamatan yang diberikan membuat saya merasa selamat daripada serangan penipuan siber.*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Acceptable	
Cybersecurity efficacy skills (E2S)	I am competent in using web browsers. *Saya cekap menggunakan pelayar web.*	7-point of scale	E1: / E2: / E3: / E4:	E1: E2: E3: E4: /	E1: E2: E3: E4:	E1: E2: E3: E4: Item 1 & 2 does not reflect skills on countermeasures against cyber fraud-only reflect general IT skills. refer back to the OD of this construct- Cybersecurity Efficacy. Suggestion:	

						"I know how to construct a good strong password for my email account." *add soalan yg ni	
	I am competent to manage my email. *Saya cekap menguruskan e-mel saya.*		E1: / E2: / E3: / E4:	E1: E2: E3: E4: /	E1: E2: E3: E4:	E1: E2: E3: E4: "I can easily differentiate between legitimate and fake website by looking at its URL." *jwpn jd yes and no	
	I am competent to connect to a virtual private network (VPN) to access e-Services. *Saya cekap menyambung ke rangkaian persendirian maya (VPN) untuk mengakses e-perkhidmatan.*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4:	
	I am competent to install anti-malware software. *Saya cekap memasang perisian anti-malware.*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4:	
Cybersecurity efficacy knowledge (E2K)	I always update my software to the current version. *Saya selalu mengemaskini perisian saya kepada versi semasa.*	7-point of scale	E1: / E2: / E3: / E4:	E1: E2: E3: E4: /	E1: E2: E3: E4:	E1: E2: E3: E4: Choose the relevant item to represent the construct for E2b and E2c	

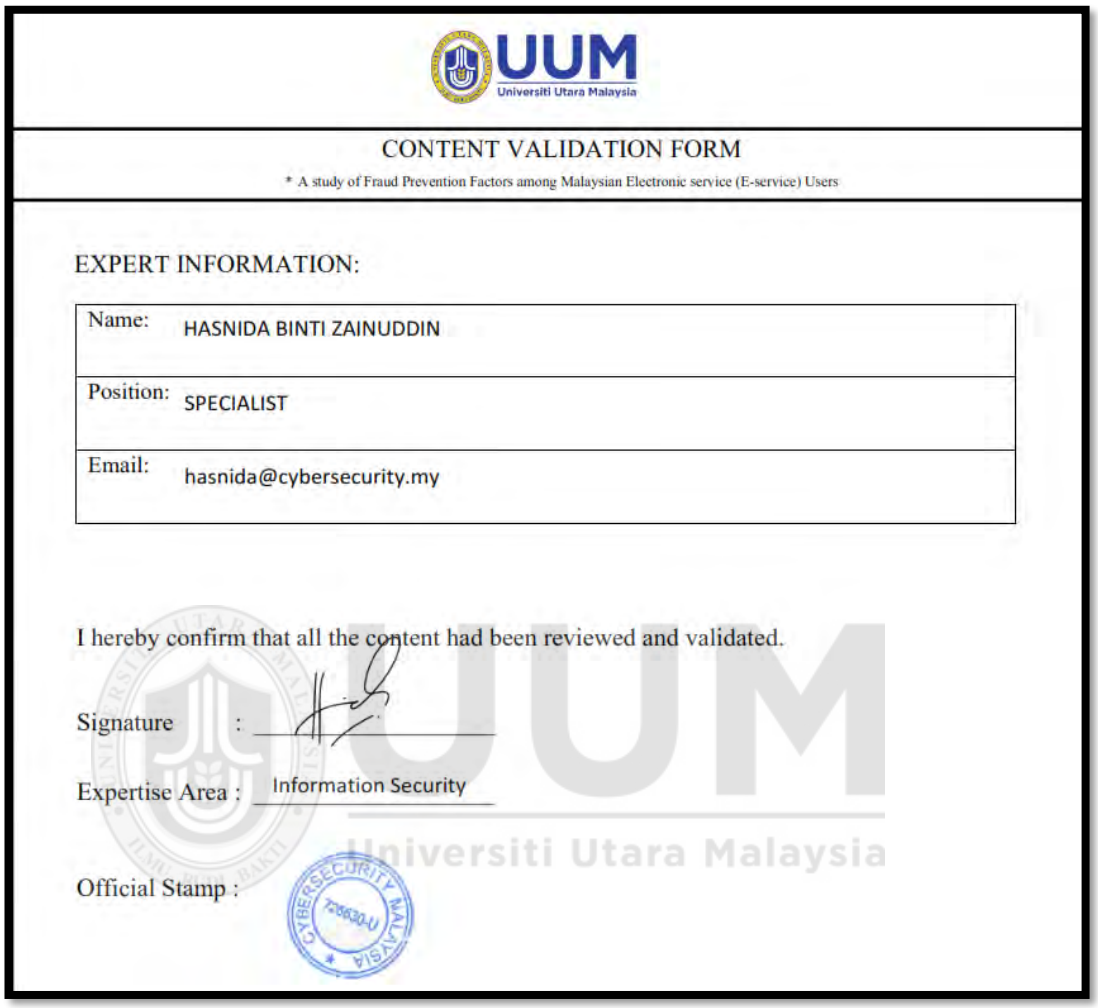
	I will update my details, like passwords, PINs, credit card information or account details via links in email or SMS. *Saya akan mengemaskini atau mengesahkan butiran saya, seperti kata laluan, PIN, maklumat kad kredit atau butiran akaun melalui pautan-pautan dalam e-mel atau SMS.*		E1: E2: / E3: / E4:	E1: / E2: E3: E4: /	E1: E2: E3: E4:	E1: E2: E3: Semak “double barrel” E4:	
	I do not notice the differences between http and https. *Saya tidak perhatikan perbezaan antara http dan https.*		E1: / E2: / E3: / E4:	E1: E2: E3: E4: /	E1: E2: E3: E4:	E1: E2: Saya tidak kisah perbezaan antara http dan https. E3: E4:	
	I share my password with my family members. *Saya berkongsi kata laluan saya dengan ahli-ahli keluarga saya.*	7-point of scale	E1: / E2: / E3: / E4:	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: Saya berkongsi kata laluan saya dengan ahli keluarga saya. E3: E4:	
	I share the e-Services Transaction Authorization Code (TAC) with others upon request. *Saya berkongsi Kod Keizinan Transaksi e-Perkhidmatan (TAC) dengan orang lain jika diminta.*		E1: / E2: / E3: / E4:	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4:	
	I will open attachments or click links from the email sent by the e-Services providers.		E1: / E2: / E3: / E4:	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4:	

	Saya akan membuka lampiran atau mengklik pautan-pautan daripada e-mel yang dihantar oleh pembekal e-Perkhidmatan.						
Protection behaviour intention	I will update my knowledge to use e-Services safely. *Saya akan meningkatkan ilmu pengetahuan saya untuk menggunakan e-Perkhidmatan dengan selamat.*	7-point of scale	E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Acceptable	
	I will likely engage in activities that protect my personal information from cyber fraud when I use e-Services. *Saya mungkin akan terlibat dalam aktiviti yang melindungi maklumat peribadi saya daripada penipuan siber semasa saya menggunakan e-Perkhidmatan.*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Acceptable	
	I intend to protect myself from cyber fraud when I use e-Services. *Saya berhasrat untuk melindungi diri daripada penipuan siber semasa menggunakan e-Perkhidmatan.*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Acceptable	

	I am willing to spend more in order to protect myself from cyber fraud when I use e-Services. *Saya bersedia membelanjakan lebih banyak wang untuk melindungi diri daripada penipuan siber semasa saya menggunakan e-Perkhidmatan.*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: "I am willing to spend more money in order to protect myself from cyber fraud when I use e-Services." Although it is understood when we say spend more usually refer to money but one can read it as spend more time/effort-so better consistent with the Malay version.	e4
	I will likely take precaution that protects my personal information from cyber fraud when I use e-Services. *Saya mungkin akan mengambil langkah berjaga-jaga untuk melindungi maklumat peribadi saya daripada penipuan siber semasa saya menggunakan e-Perkhidmatan.*		E1: / E2: / E3: / E4: /	E1: E2: E3: E4:	E1: E2: E3: E4:	E1: E2: E3: E4: Acceptable	

CONTENT VALIDITY (EXPERTS)

Expert 1



CONTENT VALIDATION FORM

* A study of Fraud Prevention Factors among Malaysian Electronic service (E-service) Users

EXPERT INFORMATION:

Name:	HASNIDA BINTI ZAINUDDIN
Position:	SPECIALIST
Email:	hasnida@cybersecurity.my

I hereby confirm that all the content had been reviewed and validated.

Signature :

Expertise Area : Information Security

Official Stamp :

Expert 2

UUM
Universiti Utara Malaysia

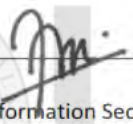
CONTENT VALIDATION FORM

* A study of Fraud Prevention Factors among Malaysian Electronic service (E-service) Users

EXPERT INFORMATION:

Name:	NAHZATULSHIMA BINTI ZAINUDDIN
Position:	SPECIALIST
Email:	nahzatul@cybersecurity.my

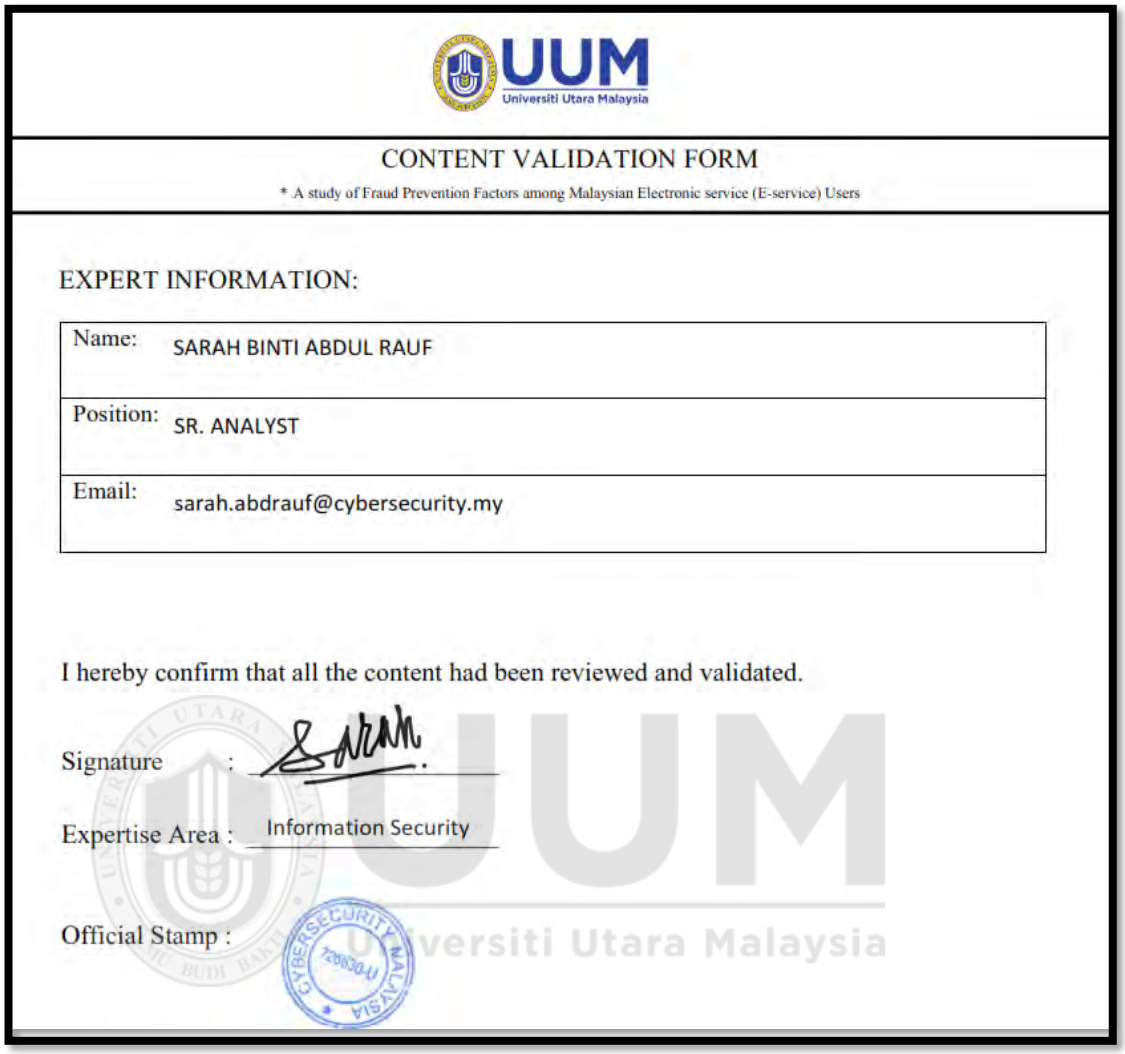
I hereby confirm that all the content had been reviewed and validated.

Signature : 

Expertise Area : Information Security

Official Stamp : 

Expert 3



CONTENT VALIDATION FORM

* A study of Fraud Prevention Factors among Malaysian Electronic service (E-service) Users

EXPERT INFORMATION:

Name:	SARAH BINTI ABDUL RAUF
Position:	SR. ANALYST
Email:	sarah.abdrauf@cybersecurity.my

I hereby confirm that all the content had been reviewed and validated.

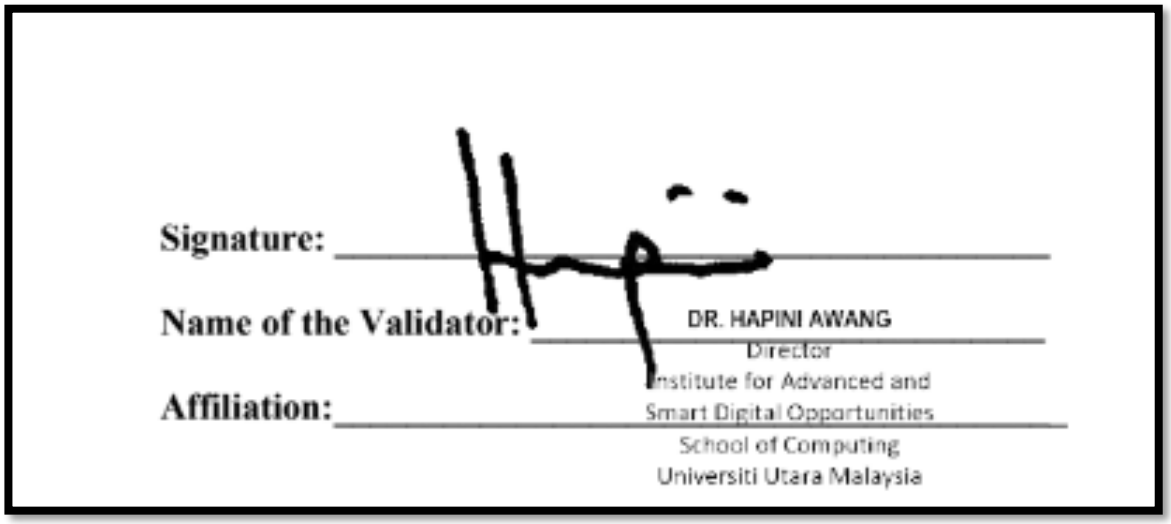
Signature : _____

Expertise Area : Information Security

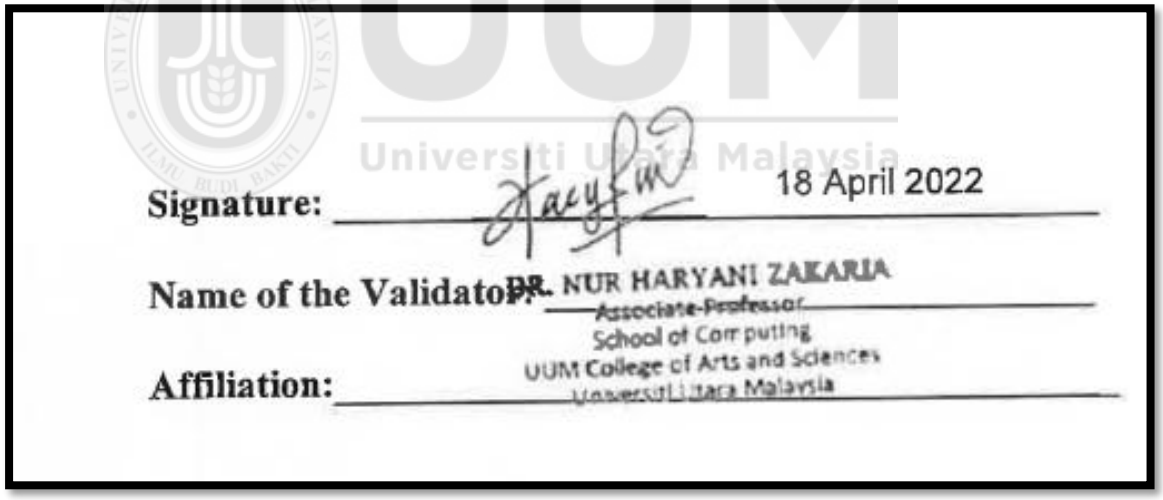
Official Stamp :

Content Validity (University Expert)

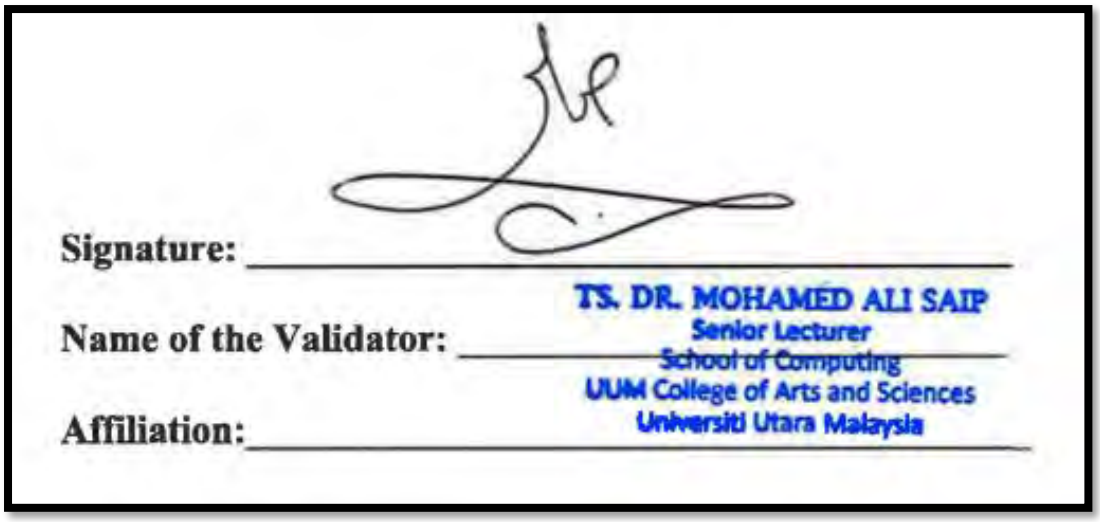
Expert 1



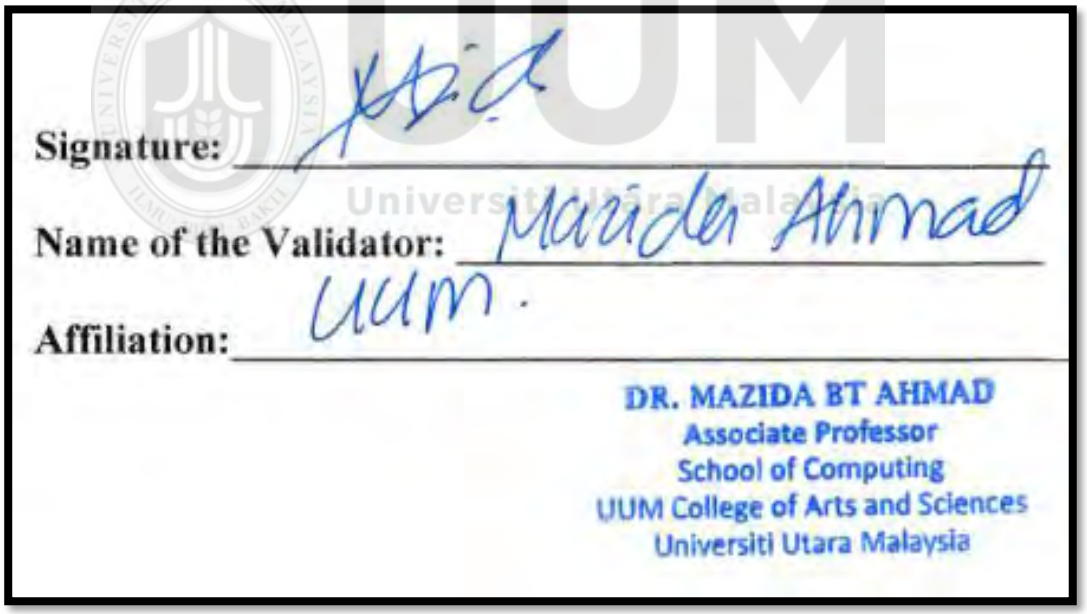
Expert 2



Expert 3



Expert 4



Questionnaire Distribution