ANTECEDENTS OF CYBER SECURITY BEHAVIOR: THE ROLES OF COPING APPRAISAL, THREAT APPRAISAL AND RESPONSIBILITY NORMS AMONG GOVERNMENT EMPLOYEES

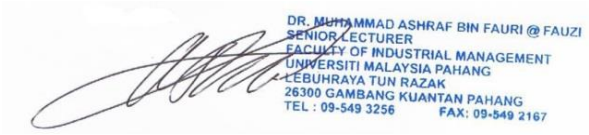
NOOR SUHANI BINTI SULAIMAN

DOCTOR OF PHILOSOPHY

UNIVERSITI MALAYSIA PAHANG

SUPERVISOR'S DECLARATION

We hereby declare that we have checked this thesis and in our opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Doctor of Philosophy.



_____

(Supervisor's Signature)

Full Name : Dr. Muhammad Ashraf Fauri @Fauzi

Position : Senior Lecturer

Date : 17 April 2023

_____

(Co-supervisor's Signature)

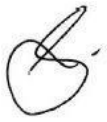
Full Name : Dr. Suhaidah Hussain

Position : Senior Lecturer

Date : 17 April 2023

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.



_____

(Student's Signature)

Full Name : NOOR SUHANI BINTI SULAIMAN

ID Number : PPB19007

Date : 17 April 2023

ANTECEDENTS OF CYBER SECURITY BEHAVIOR: THE ROLES OF COPING APPRAISAL, THREAT APPRAISAL AND RESPONSIBILITY NORMS AMONG GOVERNMENT EMPLOYEES

NOOR SUHANI BINTI SULAIMAN

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Doctor of Philosophy

Faculty of Industrial Management

UNIVERSITI MALAYSIA PAHANG

APRIL 2023

ACKNOWLEDGEMENTS

Assalamualaikum WBT.

Praise to Allah the Almighty for giving me health and strength to complete this PhD journey.

Firstly, I am grateful to my supervisor Dr. Muhammad Ashraf Fauri @ Fauzi and my co-supervisor Dr. Suhaidah Hussain, for their encouragement during this journey. I am constantly amazed at their knowledge and willingness to share their time and expertise. Dr. Ashraf has assisted and supported me in every possible way throughout this journey. I owe him more than I can adequately express, and I offer him my warmest appreciation and deepest thanks. I learn a lot from you, Dr. Ashraf.

I would like to express my gratitude to Mak Norihan Abu Bakar, Abah Sulaiman Ramly, Mek Zainun Abdullah, Ayah Ab. Razak Jusoh, Along Dr. Noor Suhana, and Adik Noor Suhaida for their support and understanding through every phase of my PhD journey. To my beloved husband, Mohd Sulaiman Ab. Razak, for the unrelenting support and always being there for me through thick and thin. To my adorable daughters, Nur Safiya Humaira and Nur Afina Humaira, both of you have constantly reminded me of what matters most in life. Not to forget my lovely family members and friends for their support, motivation and encouragement. All of you have been the motivational force for me to get through this journey. Thank you, and I love you all very much.

Moreover, in completing the thesis, I would like to thank all reviewers for all the comments and guidelines, which provided various valuable inputs, guidance and involvement. Special dedication also goes to UMP for providing financial support (Doctoral Research Scheme) for my study, and special thanks goes to all respondents who have participated in the study. Thank you very much.

ABSTRAK

Nilai kesedaran keselamatan siber dalam kalangan pekerja merupakan peranan penting bagi organisasi dalam melindungi aset. Keselamatan siber telah menjadi isu kritikal dalam masyarakat kerana penggunaan Internet yang semakin meningkat. Pelbagai sikap terhadap amalan keselamatan siber untuk pekerja dalam organisasi adalah punca utama perkara ini. Kajian terdahulu telah mendedahkan di rantau Asia Tenggara, Malaysia dilaporkan negara paling terdedah dengan 46% responden mengaku menjadi mangsa penipuan. Sama pentingnya, menurut tinjauan pengguna Internet pada 2020 yang dijalankan oleh Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) sejak 6 bulan lalu, 53.1% pengguna pernah mengalami jenayah siber. Sebaliknya, 9.4% pengguna telah mengalami jenayah siber dalam tempoh lebih 3 tahun, 7.6% pengguna dalam 2 tahun lepas dan 27.7% pengguna Internet telah mengalami jenayah siber dalam tempoh 12 bulan terakhir pada tahun 2020. Untuk mempelbagaikan tahap penilaian ancaman (kelemahan yang dirasakan, keterukan yang dirasakan), penilaian daya tindak (halangan yang dirasakan, keberkesanan tindak balas keselamatan, keberkesanan kendiri tindak balas) dan juga untuk menilai tahap impak norma tanggungjawab (tanggungjawab peribadi, tanggungjawab pihak ketiga) terhadap tingkah laku keselamatan siber pengguna. Norma tanggungjawab disepadukan ke dalam model sebagai cara untuk menilai tingkah laku pekerja terhadap keselamatan siber. Kajian ini juga menangani jurang dalam literatur dengan menyiasat sejauh mana hubungan antara kelemahan yang dirasakan, keterukan yang dirasakan, halangan yang dirasakan, keberkesanan tindak balas keselamatan, keberkesanan kendiri tindak balas, tanggungjawab peribadi dan tanggungjawab pihak ketiga wujud. Reka bentuk kajian kuantitatif telah digunakan dalam kajian ini. Kajian rintis digunakan untuk menguji model yang direka menggunakan pemodelan persamaan struktur untuk menganalisis hubungan antara pembolehubah. 446 responden daripada agensi kerajaan di Malaysia mengambil bahagian dan dianalisis menggunakan pemodelan persamaan struktur kuasa dua separa (PLS-SEM). Salah satu penemuan yang paling ketara dalam kajian ini ialah tingkah laku keselamatan siber memberi kesan yang besar kepada kakitangan kerajaan Malaysia. Penemuan ini merupakan salah satu penemuan paling kritikal daripada kajian ini. Keterukan yang dirasakan, halangan yang dirasakan, keberkesanan kendiri tindak balas, keberkesanan tindak balas keselamatan, tanggungjawab peribadi dan tanggungjawab pihak ketiga secara positif mempengaruhi tingkah laku keselamatan siber. Sebaliknya, hanya kelemahan yang dirasakan mempunyai kesan negatif terhadap tingkah laku keselamatan siber kakitangan kerajaan di Malaysia. Oleh itu, ia menyimpulkan bahawa penilaian daya tindak dan norma tanggungjawab yang dikaitkan dengan PMT mempunyai pengaruh yang ketara terhadap tingkah laku keselamatan siber kakitangan kerajaan Malaysia berbanding penilaian ancaman. Hasil kajian ini menunjukkan penemuan sebenar yang mungkin boleh diambil tindakan dengan berkesan untuk mengurangkan kesan serangan siber terhadap kakitangan kerajaan di Malaysia. Kajian ini juga telah menemui potensi untuk menyumbang kepada keselamatan agensi kerajaan di Malaysia daripada serangan siber yang dilancarkan oleh pelaku di alam siber.

ABSTRACT

The value of cyber security awareness among employees plays an important role for organizations in the protection of assets. Cyber security has become a critical issue in society due to growing internet use. Various attitudes towards cyber security practices for employees in organizations are a major cause. Previous research has revealed that in the South East Asia region, Malaysia is reportedly the most vulnerable country, with 46% of respondents admitting to being victims of scams. Equally important, according to an Internet user survey in 2020 conducted by the Malaysian Communication and Multimedia Commission (MCMC), over the last six months, 53.1% of users have experienced cybercrime. On the other hand, 9.4% of users have experienced cybercrime in more than three years, 7.6% of users in the last two years and 27.7% of Internet users have experienced cybercrime in the previous 12 months in 2020. This study verify the extent of threat appraisal (perceived vulnerability, perceived severity), coping appraisal (perceived barrier, security response efficacy, response self-efficacy) and also to evaluate the impact level of responsibility norm (personal responsibility, third-party responsibility) on user's cyber security behaviour. Responsibility norms are integrated into the model as a means to assess employees' behaviors toward cybersecurity. This study also addresses a gap in the literature by investigating the extent to which the relationships between perceived vulnerability, perceived severity, perceived barrier, security response efficacy, response self-efficacy, personal responsibility, and third-party responsibility exist. A quantitative research design was used in this study. The designed model was tested in two stages of pre-test using structural equation modelling to analyze relationships between variables. 446 respondents from government agencies in Malaysia took part and were analysed using partial least-squares structural equation modelling (PLS-SEM). One of the most notable findings of this study is that cyber security behaviour has a significant impact on Malaysian government employees. These findings are one of the most critical findings from this study. The perceived severity, perceived barrier, response self-efficacy, personal responsibility, and third-party responsibility positively influenced cybersecurity behaviour. In contrast, the perceived vulnerability and security response efficacy have a negative impact on the government employee's cybersecurity behaviour in Malaysia. Thus, it concluded that the coping appraisal and responsibility norm associated with PMT has a significantly strong influence on the cyber security behaviour of Malaysian government employees than threat appraisal does. The outcomes of this study will demonstrate the actual findings that may be brought into effective action to decrease the impact of cyber-attacks on government employees in Malaysia. This study also has discovered the potential to contribute to the security of government agencies in Malaysia from cyber-attacks launched by perpetrators in cyberspace.

TABLE OF CONTENT

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour and Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Abdallah, N., Abdalla, O., Alkhazaleh, H., & Ibrahim, A. (2020). Information security awareness behavior among higher education students: Case study. *Journal of Theoretical and Applied Information Technology*, *8*(10), 3825–3836.

Abdallah, N., & Abdullah, O. (2019). Computer security behavior and awareness: an empirical case study. *International Journal on Perceptive and Cognitive Computing*, *5*(1), 8-14.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of economic Literature*, *54*(2), 442-492.

Adhikari, K., & Panda, R. K. (2018). Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. *Journal of Global Marketing*, *31*(2), 96–110. https://doi.org/10.1080/08911762.2017.1412552

Agarwal, R., Sambamurthy, V., & Stair, R. M. (2000). The evolving relationship between general and specific computer self-efficacy—An empirical assessment. *Information systems research*, *11*(4), 418-430.

Ahmad, M. O., Markkula, J., & Oivo, M. (2013). Factors affecting e-government adoption in Pakistan: a citizen's perspective. *Transforming Government: People, Process and Policy*.

Aibinu, A. A., & Al-Lawati, A. M. (2010). Using PLS-SEM technique to model construction organizations' willingness to participate in e-bidding. *Automation in construction*, *19*(6), 714-724.

Akman, I., Yazici, A., Mishra, A., & Arifoglu, A. (2005). E-Government: A global view and an empirical evaluation of some attributes of citizens. *Government Information Quarterly*, *22*(2), 239-257.

Akter, S., D'ambra, J., & Ray, P. (2011). An evaluation of PLS based complex models: the roles of power analysis, predictive relevance and GoF index.

Alavi, R., Islam, S., & Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. *Information & Computer Security*, *24*(2), 205-227.

Aldossary, A. A., & Zeki, A. M. (2015). Web user'knowledge and their behavior towards security threats and vulnerabilities. In *2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT)* (pp. 256-260). IEEE.

Allred, S. B., & Ross-Davis, A. (2011). The drop-off and pick-up method: An approach to reduce nonresponse bias in natural resource surveys. *Small-Scale Forestry*, *10*(3), 305-318.

Alghamdi, M. I. (2021). Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. *Materials Today: Proceedings*.

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of advances in information technology*, *3*(3), 176-183.

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1), e06016.

Ameen, N., Tarhini, A., Hussain Shah, M., & Madichie, N. O. (2020). Employees' behavioural intention to smartphone security: A gender-based, cross-national study. *Computers in Human Behavior*, *104*(May 2019), 106184. https://doi.org/10.1016/j.chb.2019.106184

Anderson, B. C. L. (2016). *Qiarterly*. *34*(3), 613–643.

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

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS quarterly*, 613-643.

Andreassen, C. S., Torsheim, T., & Pallesen, S. (2014). Use of online social network sites for personal purposes at work: does it impair self-reported performance?. *Comprehensive psychology*, *3*, 01-21.

Angelin Yeoh & Christina Chin. (2019, October 18). Universiti Malaya E-Pay portal is down after being defaced. Retrieved from https://www.thestar.com.my/tech/tech-news/2019/10/18/universiti-malaya-e-pay-portal-is-down-after-being-defaced

Anthopoulos, L., Reddick, C. G., Giannakidou, I., & Mavridis, N. (2016). Why e-government projects fail? An analysis of the Healthcare.gov website. *Government Information Quarterly*, *33*(1), 161–173. https://doi.org/10.1016/j.giq.2015.07.003

Antonucci, T. C., Ajrouch, K. J., & Manalel, J. A. (2017). Social Relations and Technology: Continuity, Context, and Change. *Innovation in Aging*, *1*(3), 1–9.

https://doi.org/10.1093/geroni/igx029

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

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

Arlitsch, K., & Edelman, A. (2014). Staying Safe: Cyber Security for People and Organizations. *Journal of Library Administration*, *54*(1), 46–56. https://doi.org/10.1080/01930826.2014.893116

Armstrong, J., and T. Overton. (1977). Estimating nonresponse bias in mail surveys. *Journal of Marketing Research* 14: 396-402.

Asarch, A., Chiu, A., Kimball, A. B., & Dellavalle, R. P. (2009). Survey research in dermatology: guidelines for success. *Dermatologic clinics*, *27*(2), 121-131.

Aurigemma, S., & Mattson, T. (2017). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers and Security*, *66*, 218–234. https://doi.org/10.1016/j.cose.2017.02.006

Awang, Z., Afthanorhan, A., & Mamat, M. (2016). The Likert scale analysis using parametric based Structural Equation Modeling (SEM). *Computational Methods in Social Sciences*, *4*(1), 13.

Azura Abas. (2017, November 28). Almost 10,000 online incidents reported to CyberSecurity Malaysia each year. Retrieved from https://www.nst.com.my/news/nation/2017/11/308374/almost-10000-online-incidents-reported-cybersecurity-malaysia-each-year.

Bajpai, N. (2011). *Business research methods*. Pearson Education India.

Bakker, T. C. M., Mazzi, D., & Zala, S. (1997). Parasite-induced changes in behavior and color make Gammarus pulex more prone to fish predation. *Ecology*, *78*(4), 1098–1104. https://doi.org/10.1890/0012-9658(1997)078[1098:piciba]2.0.co;2

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review*, *84*(2), 191.

Bandura, A. (1986). The explanatory and predictive scope of self-efficacy theory. Journal of social and clinical psychology, 4(3), 359.

Bandura, A., Freeman, W. H., & Lightsey, R. (1999). Self-efficacy: The exercise of control.

Bandura, A. (2006). Guide for constructing self-efficacy scales. *Self-efficacy beliefs of adolescents*, *5*(1), 307-337.

Bandura, A., & Locke, E. A. (2003). Negative self-efficacy and goal effects revisited. *Journal of applied psychology*, *88*(1), 87.

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and informatics*, *34*(7), 1038-1058.

Barnes, S. J., & Böhringer, M. (2011). Modeling use continuance behavior in microblogging services: the case of Twitter. *Journal of Computer Information Systems*, *51*(4), 1-10.

Beam, H. D., & Mueller, T. G. (2017). What do educators know, do, and think about behavior? An analysis of special and general educators' knowledge of evidence-based behavioral interventions. *Preventing School Failure: Alternative Education for Children and Youth*, *61*(1), 1-13.

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*. *54*, 887-901. doi:10.1016/j.im.2017.01.003

Belisario, J. S. M., Jamsek, J., Huckvale, K., O'Donoghue, J., Morrison, C. P., & Car, J. (2015). Comparison of self-administered survey questionnaire responses collected using mobile apps versus other methods. *Cochrane database of systematic reviews*, (7).

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, *87*(August 2017), 87–97. https://doi.org/10.1016/j.chb.2018.05.023

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour and Information Technology*, *34*(10), 1022–1035. https://doi.org/10.1080/0144929X.2015.1028448

Boone, H. N., & Boone, D. A. (2012). Analyzing likert data. *Journal of extension*, *50*(2), 1-5.

Bonsón, E., Torres, L., Royo, S., & Flores, F. (2012). Local e-government 2.0: Social media and corporate transparency in municipalities. *Government Information Quarterly*, *29*(2), 123–132. https://doi.org/10.1016/j.giq.2011.10.001

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 behaviors. *MIS Quarterly: Management Information Systems*, *39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Bryman, A. (2016). Social Research Methods - Alan Bryman - Oxford University Press. In *Oxford University Press*.

Buchanan, J., Gjerstad, S., & Porter, D. (2016). Information effects in uniform price multi-unit dutch auctions. *Southern Economic Journal*, *83*(1), 126–145. https://doi.org/10.1002/soej.12145

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548.

Burton, D. (2000). Research training for social scientists. *Research Training for Social Scientists*, 1-528.

Burns, A. J., Posey, C., Roberts, T. L., & Benjamin Lowry, P. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190–209. https://doi.org/10.1016/j.chb.2016.11.018

Byrne, Z. S., Peters, J. M., & Weston, J. W. (2016). The struggle with employee engagement: Measures and construct clarification using five samples. *Journal of Applied Psychology*, *101*(9), 1201.

Cain, M. K., Zhang, Z., & Yuan, K. H. (2017). Univariate and multivariate skewness and kurtosis for measuring nonnormality: Prevalence, influence and estimation. *Behavior research methods*, *49*(5), 1716-1735.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Calderoni, L., & Maio, D. (2014). Cloning and tampering threats in e-Passports. *Expert Systems with Applications*, *41*(11), 5066–5070. https://doi.org/10.1016/j.eswa.2014.02.044

Caless, B. (2014). Yar M. CYBERCRIME AND SOCIETY. *Policing*, *8*(3), 285–286. https://doi.org/10.1093/police/pau024

Cheng, E. W. (2001). SEM being more effective than multiple regression in parsimonious model testing for management development research. *Journal of management development*, *20*(7), 650-667.

Cheng, L., Pei, J., & Danesi, M. (2019). A sociosemiotic interpretation of cybersecurity in U.S. legislative discourse. *Social Semiotics*, *29*(3), 286–302. https://doi.org/10.1080/10350330.2019.1587843

Chin, W. W. (1998). Issues and Opinion on Structural Equation Modeling. *MIS Quarterly*, *22*(March), vii–xvi. https://doi.org/Editorial

Churchill Gilbert A, J. (1979). Churchill, Gilbert A., Jr, A Paradigm for Developing Better Measures of Marketing Constructs , Journal of Marketing Research, 16:1 (1979:Feb.) p.64. *Journal of Marketing*, *1*(1), 64.

Choi, M., Levy, Y., & Hovav, A. (2013, December). The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. In *Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC–Workshop on Information Security and Privacy (WISP)*.

Chou, H. L., & Sun, J. C. Y. (2017). The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers. *Computers and Education*, *112*, 83–96. https://doi.org/10.1016/j.compedu.2017.05.003

Chyung, S. Y., Roberts, K., Swanson, I., & Hankinson, A. (2017). Evidence-based survey design: The use of a midpoint on the Likert scale. *Performance Improvement*, *56*(10), 15-23.

Cisco. (2017). Annual Cyber Security Report 2017. *Cisco*, 110. https://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf

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

Cobanoglu, C., Moreo, P. J., & Warde, B. (2001). A comparison of mail, fax and web-based survey methods. *International journal of market research*, *43*(4), 1-15.

Coffey, M., Hannigan, B., & Simpson, A. (2017). Care planning and coordination: Imperfect solutions in a complex world. *Journal of Psychiatric and Mental Health Nursing*, *24*(6), 333–334. https://doi.org/10.1111/jpm.12393

Cohen, J. (1988). Statistical power analysis for the behavioral sciences. *Statistical Power Analysis for the Behavioral Sciences*. https://doi.org/10.1234/12345678

Cohen, J., & Cohen, P. (1983). Applied multiple regression/correlation for the behavioral sciences. *Hillsdale, NJ: Lawrence Earlbaum*.

Compeau, D. R., & Higgins, C. A. (2017). ASTM E2368-10, Standard Practice for Strain Controlled Thermomechanical Fatigue Testing. *MIS Quarterly*, *19*(2), 189–211.

Conger, R. D., Schofield, T. J., & Neppl, T. K. (2012). Intergenerational Continuity and Discontinuity in Harsh Parenting. *Parenting*, *12*(2–3), 222–231. https://doi.org/10.1080/15295192.2012.683360

Cooper, D. R., & Schindler, P. S. (2014). *Business Research Methods*. *Business Research Methods*. The McGraw-Hill Companies, Inc.

https://doi.org/658.0072—dc23

Cordes, J. (2011). An Overview of the Economics of Cybersecurity and Cybersecurity Policy. *Developing Cyber Security Synergy*, 9.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview835

Crocker, L., Llabre, M., & Miller, M. D. (1988). The generalizability of content validity ratings. *Journal of Educational Measurement*, *25*(4), 287-299.

Cronk, L. (2017). Culture's influence on behavior: Steps toward a theory. *Evolutionary Behavioral Sciences*, *11*(1), 36–52. https://doi.org/10.1037/ebs0000069

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

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. Computers and Security, 32, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 45(4), 51-71.

Cyber Security Malaysia. (2019, November 19). Hacking Costs Malaysia MYR3.3 mln. Retrieved from https://www.cybersecurity.my/en/knowledge_bank/news/2012/main/detail/2249

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79–98. https://doi.org/10.1287/isre.1070.0160

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2014). Towards a complete understanding of information security misbehaviours: A proposal for future research with social network approach. Proceedings of the 25th Australasian Conference on Information Systems, ACIS 2014, December. https://doi.org/10.13140/2.1.4368.4165

Das, A., & Khan, H. U. (2016). Security behaviors of smartphone users. Information and Computer Security, 24(1), 116–134. https://doi.org/10.1108/ICS-04-2015-0018

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. Computers in human behavior, 26(6), 1739-

1747.

De Vries, H. (2016). Self-efficacy: skip the main factor paradigm! A comment on Williams and Rhodes (2016). Health Psychology Review, 10(2), 140–143. https://doi.org/10.1080/17437199.2016.1163234

Degaut, M. (2016). Spies and Policymakers: Intelligence in the Information Age. Intelligence and National Security, 31(4), 509–531. https://doi.org/10.1080/02684527.2015.1017931

Delgado-Rico, E., Carretero-Dios, H., & Ruch, W. (2012). Content validity evidences in test development: An applied perspective. International Journal of Clinical and Health Psychology España, 12(3), 449-460.

DeMaio, T. J., Rothgeb, J., & Hess, J. (1998). Improving survey quality through pretesting (pp. 50-58). Washington, DC: US Bureau of the Census.

Digi, 2016. Telenor: Top scams in Malaysia are Work from Home fraud, Internet Auction, Online Dating. (2016, March 11). Retrieved from https://www.malaysianwireless.com/2016/03/telenor-internet-scams-study-malaysia/.

Dimakopoulou, A., Nikitakos, N., Dagkinis, I., Lilas, T. E., Papachristos, D. A., & Papoutsidakis, M. (2019). The New Cyber Security Framework in Shipping Industy. *Journal of Multidisciplinary Engineering Science and Technology*, *6*(12), 11227–11233.

Djatsa, F. (2019). How Perceived Benefits and Barriers Affect Millennial Professionals' Online Security Behaviors. *Journal of Information Security, 10*(04), 278–301. https://doi.org/10.4236/jis.2019.104016

Doane, A. N., Boothe, L. G., Pearson, M. R., & Kelley, M. L. (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of Protection Motivation Theory. *Computers in Human Behavior*, *60*, 508–513. https://doi.org/10.1016/j.chb.2016.02.010

Dodel, M., & Mesch, G. (2019). An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. *Computers and Security*, *86*, 75–91. https://doi.org/10.1016/j.cose.2019.05.023

Doong, H. S., Wang, H. C., & Foxall, G. R. (2010). Psychological traits and loyalty intentions towards e-Government services. *International Journal of Information Management*, *30*(5), 457-464.

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter?. *Journal of Information Policy*, *9*(1), 280-306.

Dykema, J., Jones, N. R., Piché, T., & Stevenson, J. (2013). Surveying clinicians by

web: current issues in design and administration. *Evaluation & the health professions*, *36*(3), 352-381.

Egelman, S., Harbach, M., & Peer, E. (2016). Behavior ever follows intention?: A validation of the Security Behavior Intentions Scale (SeBIS). *Conference on Human Factors in Computing Systems - Proceedings*, 5257–5261. https://doi.org/10.1145/2858036.2858265

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, *272*(3), 1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021

Enocson, J., & Söderholm, L. (2018). Prevention of Cyber Security Incidents within the Public Sector. 46(0), 13–28.

Estay, S., & Alberto, D. (2018). CyberShip Project Cyber resilience for the shipping industry Work Package 3 & 4 Report. *Dtu*, *January 2019*.

Farahani, H. A., Rahiminezhad, A., & Same, L. (2010). A comparison of partial least squares (PLS) and ordinary least squares (OLS) regressions in predicting of couples mental health based on their communicational patterns. *Procedia-Social and Behavioral Sciences*, *5*, 1459-1463.

Fan, W., & Yan, Z. (2010). Factors affecting response rates of the web survey: A systematic review. *Computers in human behavior*, *26*(2), 132-139.

Feng, Z. (2012). The research and implementation of a unified identity authentication in e-government network. *Physics Procedia*, *24*, 2032–2038. https://doi.org/10.1016/j.phpro.2012.02.298

Fida, R., Tramontano, C., Paciello, M., Ghezzi, V., & Barbaranelli, C. (2018). Understanding the Interplay Among Regulatory Self-Efficacy, Moral Disengagement, and Academic Cheating Behaviour During Vocational Education: A Three-Wave Study. *Journal of Business Ethics*, *153*(3), 725–740. https://doi.org/10.1007/s10551-016-3373-6

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.

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*. https://doi.org/10.2307/3151312

Furnell, S., & Clarke, N. (2012). Power to the people? the evolving recognition of human aspects of security. *Computers and Security*, *31*(8), 983–988. https://doi.org/10.1016/j.cose.2012.08.004

Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for

novice Internet users. *Computers and Security*, *27*(7–8), 235–240. https://doi.org/10.1016/j.cose.2008.01.001

G. Hassan, R., & O. Khalifa, O. (2016). E-Government - an Information Security Perspective. *International Journal of Computer Trends and Technology*, *36*(1), 1–9. https://doi.org/10.14445/22312803/ijctt-v36p101

Gamlo, A., & Bamasak, O. (2009). Towards securing E-transactions in E-government systems of Saudi Arabia. *International Conference for Internet Technology and Secured Transactions, ICITST 2009*. https://doi.org/10.1109/icitst.2009.5402546

Gao, W., Liu, Z., Guo, Q., & Li, X. (2018). The dark side of ubiquitous connectivity in smartphone-based SNS: An integrated model from information perspective. *Computers in Human Behavior*, *84*, 185–193. https://doi.org/10.1016/j.chb.2018.02.023

Gaston, A., & Prapavessis, H. (2014). Using a combined protection motivation theory and health action process approach intervention to promote exercise during pregnancy. *Journal of Behavioral Medicine*, *37*(2), 173–184. https://doi.org/10.1007/s10865-012-9477-2

Gillam, R. B., Montgomery, J. W., Evans, J. L., & Gillam, S. L. (2019). Cognitive predictors of sentence comprehension in children with and without developmental language disorder: Implications for assessment and treatment. *International Journal of Speech-Language Pathology*, *21*(3), 240–251. https://doi.org/10.1080/17549507.2018.1559883

Gill, F. J., Leslie, G. D., Grech, C., & Latour, J. M. (2013). Using a web-based survey tool to undertake a Delphi study: Application for nurse education research. *Nurse Education Today*, *33*(11), 1322-1328.

Giraldo, J., Sarkar, E., Cardenas, A. A., Maniatakos, M., & Kantarcioglu, M. (2017). Security and privacy in cyber-physical systems: A survey of surveys. *IEEE Design & Test*, *34*(4), 7-17.

Gold, A. H., Malhotra, A., & Segars, A. H. (2001). Knowledge management: an organizational capabilities perspective. Journal of Management Information Systems, 18(1), 185–214.

Görgens-Albino, M., & Kusek, J. Z. (2009). Making monitoring and evaluation systems work: a capacity development toolkit: World Bank Publications.

Graesser, A. C., Cai, Z., Louwerse, M. M., & Daniel, F. (2006). Question Understanding Aid (QUAID) a web facility that tests question comprehensibility. *Public Opinion Quarterly*, *70*(1), 3-22.

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

Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: an empirical investigation. *Information Management & Computer Security*.

Haenlein, M., & Kaplan, A. M. (2004). A beginner's guide to partial least squares analysis. *Understanding statistics*, *3*(4), 283-297.

Hameed, M. A., & Gamagedara Arachchilage, N. A. (2019). On the Impact of Perceived Vulnerability in the Adoption of Information Systems Security Innovations. *ArXiv*, *April*, 9–18. https://doi.org/10.5815/ijcnis.2019.04.02

Hammarstrand, J., & Fu, T. (2015). Information security awareness and behaviour: of trained and untrained home users in Sweden.

Hammond, S. T. (2019). Threat and coping appraisals on information security awareness training effectiveness: A quasi-experimental study (Doctoral dissertation, Capella University).

Hanus, B., & Wu, Y. "Andy." (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, *33*(1), 2–16. ttps://doi.org/10.1080/10580530.2015.1117842

Hardy, B., & Ford, L. R. (2014). It's not me, it's you: Miscomprehension in surveys. *Organizational Research Methods*, *17*(2), 138-162.

Harris, P. A., Taylor, R., Thielke, R., Payne, J., Gonzalez, N., & Conde, J. G. (2009). Research electronic data capture (REDCap)—a metadata-driven methodology and workflow process for providing translational research informatics support. *Journal of biomedical informatics*, *42*(2), 377-381.

Hair, Joseph F, Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2010). *Multivariate Data Analysis*. *Pearson Prentice Hall* (7th Editio). Pearson Prentice Hall.

Hair Jr, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European business review*.

Hair, Joseph F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. *Thousand Oaks: Sage*. https://doi.org/10.1016/j.lrp.2013.01.002

Hair, Joseph F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., & Thiele, K. O. (2017). Mirror, mirror on the wall: a comparative evaluation of composite-based structural equation modeling methods. *Journal of the Academy of Marketing Science*, *45*(5), 616–632. https://doi.org/10.1007/s11747-017-0517-x

Hair Jr., J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017). PLS-SEM or

CB-SEM: updated guidelines on which method to use. *International Journal of Multivariate Data Analysis*, *1*(2), 107.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice*, *19*(2), 139-152.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2018). The Results of PLS-SEM Article information. *European Business Review*, *31*(1), 2–24.

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*.

Hardesty, D. M., & Bearden, W. O. (2004). The use of expert judges in scale development: Implications for improving face validity of measures of unobservable constructs. *Journal of Business Research*, *57*(2), 98-107.

Hasan, B. (2006). Delineating the effects of general and system-specific computer self-efficacy beliefs on IS acceptance. *Information & Management*, *43*(5), 565-571.

Haynes, S. N., Richard, D., & Kubany, E. S. (1995). Content validity in psychological assessment: A functional approach to concepts and methods. *Psychological assessment*, *7*(3), 238.

He, Y., Chen, Q., & Kitkuakul, S. (2018). Regulatory focus and technology acceptance: Perceived ease of use and usefulness as efficacy. *Cogent Business and Management*, *5*(1). https://doi.org/10.1080/23311975.2018.1459006

Henseler, J., & Chin, W. W. (2010). A comparison of approaches for the analysis of interaction effects between latent variables using partial least squares path modeling. *Structural Equation Modeling*, *17*(1), 82–109. https://doi.org/10.1080/10705510903439003

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the academy of marketing science*, *43*(1), 115-135.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hina, S., Panneer Selvam, D. D. D., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers and Security*, *87*, 101594. https://doi.org/10.1016/j.cose.2019.101594

Holdsworth, J., & Apeh, E. (2017, September). An effective immersive cyber security awareness learning platform for businesses in the hospitality sector. In *2017 IEEE 25th International Requirements Engineering Conference Workshops*

(REW) (pp. 111-117). IEEE.

Hong, Y., & Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications*, *57*, 102710.

Hong, S., Thong, J. Y., & Tam, K. Y. (2006). Understanding continued information technology usage behavior: A comparison of three models in the context of mobile internet. *Decision support systems*, *42*(3), 1819-1834.

Horst, M., Kuttschreuter, M., & Gutteling, J. M. (2007). Perceived usefulness, personal experiences, risk perception and trust as determinants of adoption of e-government services in The Netherlands. *Computers in human behavior*, *23*(4), 1838-1852.

Hsu, M. H., & Chiu, C. M. (2004). Internet self-efficacy and electronic service acceptance. *Decision Support Systems*, *38*(3), 369–381. https://doi.org/10.1016/j.dss.2003.08.001

Hughes, A. (2016). Student Information Security Behaviors and Attitudes at a Private Liberal Arts University in the Southeastern United States. July 2016. https://doi.org/10.13140/RG.2.2.17361.28008

Hulland, J., Baumgartner, H., & Smith, K. M. (2018). Marketing survey research best practices: evidence and recommendations from a review of JAMS articles. *Journal of the Academy of Marketing Science*, *46*(1), 92-108.

Hung, S. Y., Chang, C. M., & Yu, T. J. (2006). Determinants of user acceptance of the e-Government services: The case of online tax filing and payment system. *Government Information Quarterly*, *23*(1), 97–122. https://doi.org/10.1016/j.giq.2005.11.005

Hunt, S. D., Sparkman Jr, R. D., & Wilcox, J. B. (1982). The pretest in survey research: Issues and preliminary findings. *Journal of marketing research*, *19*(2), 269-273.

IBM. (2014). Analysis of cyber attack and incident data from IBM's worldwide security operations. *IBM Security Managing Security Services*, 11. http://public.dhe.ibm.com/common/ssi/ecm/en/sew03031usen/SEW03031USEN.PDF

Ibrahim, R. S. E.-D. (2015). It's all about me! The Influence of Personality on Susceptibility to Mobile Security Attacks. *International Journal of Applied Mathematics, Electronics and Computers*, *3*(3), 194. https://doi.org/10.18100/ijamec.47036

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P. (2019). *ASB 2014. September 2014*.

International Telecommunication Union. (2008). Overview Cybersecurity. *ITU-T X.1205 Recommendation*, *1205*(Rec. ITU-T X.1205 (04/2008)), 2–3. https://www.itu.int/rec/T-REC-X.1205-200804-I

Jain, S., & Agrawal, S. (2020). Perceived vulnerability of cyberbullying on social networking sites: effects of security measures, addiction and self-disclosure. *Indian Growth and Development Review*.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Johannesson, P., & Perjons, E. (2014). Research paradigms. In *An Introduction to Design Science* (pp. 167-179). Springer, Cham.

Johns, R. (2005). One size doesn't fit all: Selecting response scales for attitude items. *Journal of Elections, Public Opinion & Parties*, *15*(2), 237-264.

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

Jones, C. L., Jensen, J. D., Scherr, C. L., Brown, N. R., Christy, K., & Weaver, J. (2015). The Health Belief Model as an Explanatory Framework in Communication Research: Exploring Parallel, Serial, and Moderated Mediation. *Health Communication*, *30*(6), 566–576. https://doi.org/10.1080/10410236.2013.873363

Józsa, K., & Morgan, G. A. (2017). Reversed items in Likert scales: Filtering out invalid responders. *Journal of Psychological and Educational Research*, *25*(1), 7-25.

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Kalech, M. (2019). Cyber-attack detection in SCADA systems using temporal pattern recognition techniques. *Computers and Security*, *84*, 225–238. https://doi.org/10.1016/j.cose.2019.03.007

Kaspersky Security Bulletin (2013). Overall statistics for 2013. https://media.kaspersky.com/pdf/KSB_2013_EN.pdf. (15 December 2019).

Kaur, P., Stoltzfus, J., & Yellapu, V. (2018). Descriptive statistics. *International Journal of Academic Medicine*, *4*(1), 60.

Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of

information security policy compliance. *The Scientific World Journal*, *2014*.

Kim, S., & Lee, J. S. (2013). Is satisfaction enough to ensure reciprocity with upscale restaurants? The role of gratitude relative to satisfaction. *International Journal of Hospitality Management*, *33*, 118-128.

Kitchenham, B., & Pfleeger, S. L. (2002). Principles of survey research: part 5: populations and samples. ACM SIGSOFT Software Engineering Notes, 27(5), 17-20.

Kline, R. B. (2011). Principles and Practice of Structural Equation Modelling. The GuilFord Press. New York: Guilford Press. https://doi.org/10.1017/CBO9781107415324.004

Klöckner, C. A., & Prugsamatz, S. (2012). Habits as barriers to changing behaviour. Psykologisk Tidsskrift, 16(3), 26-30.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security*, *64*, 122-134.

Kulas, J. T., & Stachowski, A. A. (2013). Respondent rationale for neither agreeing nor disagreeing: Person and item contributors to middle category endorsement intent on Likert personality indicators. Journal of Research in Personality, 47(4), 254-262.

Kumar, M. (2020). Effective Usage of E-CRM and Social Media Tools by Akshay Kumar: Most Prolific Bollywood Actor of Last Decade. *International Journal of Management (IJM)*, *11*(2).

Kumar, M., & Ayedee, D. (2021). Technology Adoption: A Solution for SMEs to overcome problems during COVID-19. *Forthcoming, Academy of Marketing Studies Journal*, *25*(1).

Lavrakas, P.J. (2008). Encyclopedia of Survey Research Methods. https://dx.doi.org/10.4135/9781412963947.n522

Le, T. T., Tran, T. T., Ho, H., Vu, A. T., & Lopata, A. L. (2018). Prevalence of food allergy in Vietnam: comparison of web-based with traditional paper-based survey. *World Allergy Organization Journal*, *11*(1), 1-10.

Lee, H., & Kobsa, A. (2017). Understanding user privacy in Internet of Things environments. *2016 IEEE 3rd World Forum on Internet of Things, WF-IoT 2016*, 407–412. https://doi.org/10.1109/WF-IoT.2016.7845392

Lee, Y., & Kozar, K. A. (2006). Investigating the effect of website quality on e-business success: An analytic hierarchy process (AHP) approach. *Decision*

Support Systems, *42*(3), 1383–1401. https://doi.org/10.1016/j.dss.2005.11.005

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives′ decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177–187. https://doi.org/10.1057/ejis.2009.11

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445-454.

Lee, Y. H., Hsieh, Y. C., & Ma, C. Y. (2011). A model of organizational employees'e-learning systems acceptance. *Knowledge-based systems*, *24*(3), 355-366.

Leidner, D. E., Lo, J., & Preston, D. (2011). An empirical investigation of the relationship of IS strategy with firm performance. *The Journal of Strategic Information Systems*, *20*(4), 419-437.

Lenzner, T., Kaczmirek, L., & Galesic, M. (2011). Seeing through the eyes of the respondent: An eye-tracking study on survey question comprehension. *International Journal of Public Opinion Research*, *23*(3), 361-373.

Leong, L. Y., Hew, T. S., Tan, G. W. H., & Ooi, K. B. (2013). Predicting the determinants of the NFC-enabled mobile credit card acceptance: A neural networks approach. *Expert Systems with Applications*, *40*(14), 5604-5620.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*(November 2018), 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS quarterly*, 71-90.

Lian, J. W. (2020). Understanding cloud-based BYOD information security protection behaviour in smart business: in perspective of perceived value. *Enterprise Information Systems*, 1–22. https://doi.org/10.1080/17517575.2020.1791966

Madnick, S. E., & Siegel, M. D. (2014). Global e-Readiness — For What GLOBAL E-READINESS – FOR WHAT ? Readiness for e-Banking Sloan School of Management. May 2004.

Maisey, M. (2014). Moving to analysis-led cyber-security. *Network Security*, *2014*(5), 5–12. https://doi.org/10.1016/S1353-4858(14)70049-2

Mandal, A., Eaden, J., Mayberry, M. K., & Mayberry, J. F. (2000). Questionnaire surveys in medical research. *Journal of Evaluation in Clinical practice*, *6*(4), 395-403.

Maqbool, Z., Pammi, V. S. C., & Dutt, V. (2018). Cyber security: Influence of patching

vulnerabilities on the decision-making of hackers and analysts. *2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2018, March*. https://doi.org/10.1109/CyberSA.2018.8551421

Marakanon, L., & Panjakajornsak, V. (2017). Perceived quality, perceived risk and customer trust affecting customer loyalty of environmentally friendly electronics products. *Kasetsart Journal of Social Sciences*, *38*(1), 24–30. https://doi.org/10.1016/j.kjss.2016.08.012

Marakas, G. M., Johnson, R. D., & Clay, P. F. (2007). The evolving nature of the computer self-efficacy construct: An empirical investigation of measurement construction, validity, reliability and stability over time. *Journal of the Association for Information Systems*, *8*(1), 16–46. https://doi.org/10.17705/1jais.00112

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 Behavior*, *92*(November 2018), 139–150. https://doi.org/10.1016/j.chb.2018.11.002

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*, 135-155.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36-58.

Maymone, M. B., Venkatesh, S., Secemsky, E., Reddy, K., & Vashi, N. A. (2018). Research techniques made simple: web-based survey research in dermatology: conduct and applications. *Journal of Investigative Dermatology*, *138*(7), 1456-1462.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151-156.

MCMC. (2018). Internet users survey 2018: Statistical brief number twenty-three. *Internet Users Survey 2018*, 1–39. https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Internet-Users-Survey-2018.pdf

MCMC. (2020). Internet Users Survey 2020. *Malaysian Communications And Multimedia Commission*, 25–39. https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Internet-Users-Survey-2018-(Infographic).pdf

McNeish, D. (2017). Thanks Coefficient Alpha, We'll Take It From Here. *Psychological Methods*, (February). https://doi.org/10.1037/met0000144

Member, S. S., & Karaulia, D. S. (2015). E-Governance : Information Security Issues E-Governance : Information Security Issues. DECEMBER 2011.

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers and Security*, *75*, 147–166. https://doi.org/10.1016/j.cose.2018.01.020

Merhi, M., Hone, K., & Tarhini, A. (2019). A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. *Technology in Society*, *59*(January), 101151. https://doi.org/10.1016/j.techsoc.2019.101151

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security*, *9*(1), 47-67.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, *147*, 424-428.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106–143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x

Mishra, A., Awal, A., Elijah, J., & Rabiu, I. (2017). An Assessment of the Level of Information Security Awareness among Online Banking Users in Nigeria. *International Journal of Computer Science and Mobile Computing*, *6*(5), 373–387. www.ijcsmc.com

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers and Security*, *48*, 267–280. https://doi.org/10.1016/j.cose.2014.10.015

Mooi, E., & Sarstedt, M. (2011). A concise guide to market research: The process, data, and methods using IBM SPSS statistics: Springer. Heidelberg.

Mwagwabi, F., McGill, T., & Dixon, M. (2018). Short-term and long-term effects of fear appeals in improving compliance with password guidelines. *Communications of the Association for Information Systems*, *42*(1), 147–182. https://doi.org/10.17705/1CAIS.04207

MyCERT. (2019). Incident Statistics. Retrieved from https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=ac188e88-67b5-4e39-bfed-5512036b87ac.

National Security Council. (2019). Malaysia Cybersecurity Strategy 2020-2024. Retrieved from https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf.

National Cyber Security Alliance. (2012, October 1). 2012 Online Safety Survey – Majority Of Americans Do Not Feel Completely Safe Online. Retrieved from https://www.mcafee.com/blogs/internet-security/online-safety-survey2012/.

Ng, B. Y., & Xu, Y. (2007). Studying users' computer security behavior using the Health Belief Model. PACIS 2007 - 11th Pacific Asia Conference on Information Systems: Managing Diversity in Digital Enterprises, June.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.

Nobles, C. (2015). *Exploring pilots' experiences of integrating technologically advanced aircraft within general aviation: A case study*. Northcentral University.

Obermiller, C., & Spangenberg, E. R. (1998). Development of a scale to measure consumer skepticism toward advertising. *Journal of consumer psychology*, *7*(2), 159-186.

Ohana, M., & Meyer, M. (2010). Should I stay or should I go now? Investigating the intention to quit of the permanent staff in social enterprises. *European Management Journal*, *28*(6), 441-454.

Oostrom, J. K., & Born, M. P. (2014). Using cognitive pretesting to explore causes for ethnic differences on role-plays. *International Journal of Intercultural Relations*, *41*, 138-149.

Oppenheimer, A. J., Pannucci, C. J., Kasten, S. J., & Haase, S. C. (2011). Survey says? A primer on web-based survey design and distribution. *Plastic and Reconstructive surgery*, *128*(1), 299.

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 156b-156b). IEEE.

Palladino, B. E., Menesini, E., Nocentini, A., Luik, P., Naruskov, K., Ucanok, Z., Dogan, A., Schultze-Krumbholz, A., Hess, M., & Scheithauer, H. (2017). Perceived severity of cyberbullying: Differences and similarities across four countries. *Frontiers in Psychology*, *8*(SEP), 1–12. https://doi.org/10.3389/fpsyg.2017.01524

Papadopoulos, N., & Martín, O. M. (2010). Toward a model of the relationship between

internationalization and export performance. *International Business Review*, *19*(4), 388-406.

Parent, M., Vandebeek, C. A., & Gemino, A. C. (2005). Building citizen trust through e-government. *Government Information Quarterly*, *22*(4), 720-736.

Pavlou, P. A., & O. A. El Sawy. 2006. From IT leveraging competence to competitive advantage in turbulent environments. *Information Systems Research* 17 (3), 198-227.

Peng, D. X., & Lai, F. (2012). Using partial least squares in operations management research: A practical guideline and summary of past research. *Journal of operations management*, *30*(6), 467-480.

Pitchan, M. A., & Omar, S. Z. (2019). Dasar Keselamatan Siber Malaysia: Tinjauan Terhadap Kesedaran Netizen dan Undang-Undang (Cyber Security Policy: Review on Netizen Awareness and Laws). *Jurnal Komunikasi: Malaysian Journal of Communication*, *35*(1), 103–119. https://doi.org/10.17576/jkmjc-2019-3501-08

Pitchan, M. A., Omar, S. Z., Bolong, J., & Ahmad Ghazal, A. H. (2017). Analisis keselamatan siber dari perspektif persekitaran sosial: kajian terhadap pengguna internet di Lembah Klang. *Journal of Social Sciences and Humanities*, *12*(2), 016-029.

Poelmans, S., Wessa, P., Milis, K., Bloemen, E., & Doom, C. (2008, November). Usability and acceptance of e-learning in statistics education, based on the compendium platform. In *Proceedings of the International Conference of Education, Research and Innovation* (Vol. 1, No. 10).

Ponto, J. (2015). Understanding and evaluating survey research. *Journal of the advanced practitioner in oncology*, *6*(2), 168.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179–214. https://doi.org/10.1080/07421222.2015.1138374

Presser, S., Couper, M. P., Lessler, J. T., Martin, E., Martin, J., Rothgeb, J. M., & Singer, E. (2004). Methods for testing and evaluating survey questions. *Methods for testing and evaluating survey questionnaires*, 1-22.

Proctor, R. W., & Chen, J. (2015). The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. *Human factors*, *57*(5), 721-727.

Purdey, B. (2013). Occupant stimulus response workplace productivity and the vexed question of measurement. *Facilities*.

Raaijmakers, Q. A., Van Hoof, J. T. C., t Hart, H., Verbogt, T. F. M. A., & Vollebergh, W. A. (2000). Adolescents' midpoint responses on Likert-type scale items: neutral or missing values?. *International Journal of Public Opinion Research*, *12*, 208-216.

Rada, V. D. D., & Domínguez-Álvarez, J. A. (2014). Response quality of self-administered questionnaires: A comparison between paper and web questionnaires. *Social Science Computer Review*, *32*(2), 256-269.

Rahim, A. A., Zainudin, T. N. A. T., & Rajamanickam, R. (2015). The involvement of school students in criminal activities and its position in the Malaysian Law. *Mediterranean Journal of Social Sciences*, *6*(4S3), 403–407. https://doi.org/10.5901/mjss.2015.v6n4s3p403

Rahman, M. S., Ko, M., Warren, J., & Carpenter, D. (2016). Healthcare Technology Self-Efficacy (HTSE) and its influence on individual attitude: An empirical study. *Computers in Human Behavior*, *58*, 12-24.

Ramayah, T., Ahmad, N. H., & Lo, M. C. (2010). The role of quality factors in intention to continue using an e-learning system in Malaysia. *Procedia-Social and Behavioral Sciences*, *2*(2), 5422-5426.

Ramayah, T., Lee, J. W. C., & Mohamad, O. (2010). Green product purchase intention: Some insights from a developing country. *Resources, conservation and recycling*, *54*(12), 1419-1427.

Ramayah, T., Jacky, C., Chuah, F., Ting, H., & Memon, M. A. (2018). *Partial Least Squares Structural Equation Modeling (PLS-SEM) using SmartPLS 3.0*. *Handbook of Market Research* (2th Editio). Pearson Malaysia Sdn Bhd. https://doi.org/10.1007/978-3-319-05542-8_15-1

Ramayah, T., Jasmine, Y. A. L., Ahmad, N. H., Halim, H. A., & Rahman, S. A. (2017). Testing a Confirmatory model of Facebook Usage in SmartPLS using Consistent PLS. *International Journal of Business and Innovation*, *3*(2), 1–14.

Ravindran, S. K. (2018). Impact of Probable and Guaranteed Monetary Value on Cybersecurity Behavior of Users. *ProQuest Dissertations and Theses*, 102. https://login.pallas2.tcl.sc.edu/login?url=https://search.proquest.com/docview/2115826716?accountid=13965%0Ahttp://resolver.ebscohost.com/openurl?ctx_ver=Z39.882004&ctx_enc=info:ofi/enc:UTF8&rfr_id=info:sid/ProQuest+Dissertations+%26+Theses+Global&rft_v

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

Revilla, M., & Ochoa, C. (2017). Ideal and maximum length for a web survey. *International Journal of Market Research*, *59*(5), 557-565.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & security*, *28*(8), 816-826.

Riffenburgh, R. H. (2012). Questionnaires and Surveys. In *Statistics in Medicine* (pp. 571-579). Academic Press, Elsevier.

Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures. *Journal of consumer affairs*, *39*(2), 339-362.

Ringle, C., Wende, S., & Becker, J. (2015). SmartPLS 3. *Retrieved From*. https://doi.org/http://www.smartpls.com

Roberts, N., & Grover, V. (2009). Theory development in information systems research using structural equation modeling: Evaluation and recommendations. In *Handbook of research on contemporary theoretical models in information systems* (pp. 77-94). IGI Global.

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers and Security*, *59*, 26–44. https://doi.org/10.1016/j.cose.2016.01.004

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*, 153-176.

Rosenstock, I. M., & Ph, D. (1960). Historical Origins of the Health Belief Model. *Health Education Monographs*, *2*(4), 328–335.

Rosenthal, J. A. (2011). *Statistics and data interpretation for social work*. Springer publishing company.

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 and Security*, *53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Salman, A., Yusoff, M. A., Salleh, M. A. M., & Abdullah, M. Y. H. (2018). Pengunaan media sosial untuk sokongan politik di Malaysia [The use of social media for political support in Malaysia]. *Journal of Nusantara Studies (JONUS)*, *3*(1), 51-63.Aloul, F. A. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, *3*(3). https://doi.org/10.4304/jait.3.3.176-183

Sani, A. S., Yuan, D., Jin, J., Gao, L., Yu, S., & Dong, Z. Y. (2019). Cyber security framework for Internet of Things-based Energy Internet. *Future Generation Computer Systems*, *93*, 849–859. https://doi.org/10.1016/j.future.2018.01.029

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320–330. https://doi.org/10.1016/j.techfore.2015.08.012

Sarrina Li, S.-C. (2013). Lifestyle orientations and the adoption of Internet-related technologies in Taiwan. *Telecommunications Policy, 37*(8), 639-650.

Sanchez-Franco, M. J., & Roldán, J. L. (2010). Expressive aesthetics to ease perceived community support: Exploring personal innovativeness and routinised behaviour as moderators in Tuenti. *Computers in Human Behavior, 26*(6), 1445-1457.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, *19*(3), 122-131.

Sauro, J., & Lewis, J. R. (2012). Standardized Usability Questionnaires. In *Quantifying the User Experience*. https://doi.org/10.1016/b978-0-12-384968-7.00008-4

Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2016). CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. *Proceedings - International Conference on Distributed Computing Systems*, *2016-Augus*, 303–312. https://doi.org/10.1109/ICDCS.2016.46

Schottmann, S. A. (2012). Malaysia's foreign policy: the first fifty years. *Global Change, Peace & Security*, *24*(1), 197–198. https://doi.org/10.1080/14781158.2012.641291

Schwarz, N., Grayson, C. E., & Knauper, B. (1998). Formal features of rating scales and the interpretation of question meaning. *International Journal of Public Opinion Research*, *10*(2), 177-184.

Scott, M., Delone, W., & Golden, W. (2016). Measuring eGovernment success: A public value approach. *European Journal of Information Systems, 25*(3), 187–208. https://doi.org/10.1057/ejis.2015.11

Seguí, M., Cabrero-García, J., Crespo, A., Verdú, J., & Ronda, E. (2015). A reliable and valid questionnaire was developed to measure computer vision syndrome at the workplace. *Journal of clinical epidemiology*, *68*(6), 662-673.

Shafie, S. (2007). e-Government Initiatives in Malaysia and the Role of the National Archives of Malaysia in Digital Records Management. *National Archives of Malaysia*, 1–15. http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan041040.pdf

Shahraki, A. S., & Nikmaram, M. (2013). Human errors in computer related abuses. *Journal of Theoretical and Applied Information Technology*, *47*(1), 93–97.

Sharma, G. (2017). Pros and cons of different sampling techniques. *International journal of applied research*, *3*(7), 749-752.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92-100.

Sheeran, P., Maki, A., Montanaro, E., Avishai-Yitshak, A., Bryan, A., Klein, W. M. P., Miles, E., & Rothman, A. J. (2016). The impact of changing attitudes, norms, and self-efficacy on health-related intentions and behavior: A meta-analysis. *Health Psychology*, *35*(11), 1178–1188. https://doi.org/10.1037/hea0000387

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. *Computers in Human Behavior*, *48*, 199–207. https://doi.org/10.1016/j.chb.2015.01.046

Shillair, R. J. (2018). Mind the Gap: Perceived Self-Efficacy, Domain Knowledge and Their Effects on Responses to a Cybersecurity Compliance Message (Doctoral dissertation, Michigan State University).

Shillair, R., & Dutton, W. H. (2016). Supporting a cybersecurity mindset: getting internet users into the cat and mouse game. *Available at SSRN 2756736*.

Siau, K., & Hall, R. (2019). Impact of Framing And Base Size of Computer Security Risk Information on User Behavior by Presented to the Faculty of the Graduate School of the Missouri University Of Science And Technology

Silver, L., Stevens, R. E., Wrenn, B., & Loudon, D. L. (2012). *The essentials of marketing research*. Routledge

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management*, *51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Solon, O., & Hern, A. (2017). Petya'ransomware attack: what is it and how can it be stopped. *The Guardian*.

Soltanmohammadi, S., Asadi, S., & Ithnin, N. (2013). Main human factors affecting information system security. *Interdisciplinary Journal of Contemporary Research in Business*, *5*(7), 329-354.

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

Soumia, A., Rabah, I., Mohamed, M., & Abdelaziz, K. (2012). An approach for evaluation of e-government information systems agility. In *International*

Conference on Information Society (i-Society 2012) (pp. 193-198). IEEE.

Sullivan, G. M., & Feinn, R. (2012). Using effect size—or why the P value is not enough. *Journal of graduate medical education*, *4*(3), 279-282.

Svilicic, B., Kamahara, J., Celic, J., & Bolmsten, J. (2019). Assessing ship cyber risks: a framework and case study of ECDIS security. *WMU Journal of Maritime Affairs*, *18*(3), 509–520. https://doi.org/10.1007/s13437-019-00183-x

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers and Security*, *90*. https://doi.org/10.1016/j.cose.2019.101709

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems*, *98*, 660–671. https://doi.org/10.1016/j.future.2019.03.042

Teo, T. S., Srivastava, S. C., & Jiang, L. I. (2008). Trust and electronic government success: An empirical study. *Journal of management information systems*, *25*(3), 99-132.

Teoh, C. S., Kamil Mahmood, A., & Dzazali, S. (2018). Cyber Security Challenges in Organisations: A Case Study in Malaysia. 2018 4th International Conference on Computer and Information Sciences: Revolutionising Digital Landscape for Sustainable Smart Society, ICCOINS 2018 - Proceedings. https://doi.org/10.1109/ICCOINS.2018.8510569

The Star. (2016, March 11). Malaysia is the most vulnerable country to internet scams in this region. Retrieved from https://www.thestar.com.my/business/business-news/2016/03/11/malaysia-is-the-most-vulnerable-country-to-internet-scams-in-this-region/.

The Star. (2014, September 23). Malaysia is sixth most vulnerable to cyber crime. Retrieved from https://www.thestar.com.my/news/nation/2014/09/23/cyber-crime-malaysians-sixth-most-vulnerable.

Tholen, B. (2010). The changing border: Developments and risks in border control management of western countries. *International Review of Administrative Sciences*, *76*(2), 259–278. https://doi.org/10.1177/0020852309365673

Torous, J., Staples, P., Fenstermacher, E., Dean, J., & Keshavan, M. (2016). Barriers, benefits, and beliefs of brain training smartphone apps: an internet survey of younger US consumers. *Frontiers in Human Neuroscience*, 180.

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awarness on information technology professionals' behavior. *Computers and Security*, *79*, 68–79. https://doi.org/10.1016/j.cose.2018.08.007

Tounsi, W. (2019). What is cyber threat intelligence and how is it evolving?. Cyber-Vigilance and Digital Trust: Cyber Security in the Era of Cloud Computing and IoT, 1-49.

Tourangeau, R., Rips, L. J., & Rasinski, K. (2000). The psychology of survey response.

Tsai, H. Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers and Security*, *59*(1318885), 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Tse, A., L. Y. M. Sin, O. H. M. Yau, J. S. Y. Lee, and R. Chow. 2003. Market orientation and business performance in a Chinese business environment. *Journal of Business Research* 56: 227-239.

Tu, C. Z., Adkins, J., & Zhao, G. Y. (2019). Complying with BYOD Security Policies: A Moderation Model Based on Protection Motivation Theory. *MWAIS 2018 Proceedings*, *2019*(1), 25. https://aisel.aisnet.org/jmwais

Tullis, T., & Albert, B. (2013). Self-reported metrics. *Measuring the user experience: collecting, analyzing, and presenting usability metrics. 2nd ed. Boston (MA): Morgan Kaufmann*, 121-161.

Turja, T., Rantanen, T., & Oksanen, A. (2019). Robot use self-efficacy in healthcare work (RUSH): development and validation of a new measure. *AI and Society*, *34*(1), 137–143. https://doi.org/10.1007/s00146-017-0751-2

Urbach, N., & Ahlemann, F. (2010). Structural equation modeling in information systems research using Partial Least Squares. *Journal of Information Technology Theory and Application (JITTA)*, *11*(2), 5–40.

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

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019b). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human Computer Studies*, *123*(November 2017), 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

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

Van Eerde, W., & Thierry, H. (1996). Vroom's expectancy models and work-related criteria: A meta-analysis. *Journal of applied psychology*, *81*(5), 575.

van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and

privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283–297. https://doi.org/10.1016/j.chb.2017.10.007

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547–559. https://doi.org/10.1016/j.chb.2017.05.038

Van Thiel, S. (2014). Research methods in public administration and public management: An introduction. Routledge.

Vasantha Raju, N., & Harinarayana, N. S. (2016). Online survey tools: A case study of Google Forms. In National Conference on Scientific, Computational & Information Research Trends in Engineering, GSSS-IETW, Mysore.

Vehovar, V., Petrovčič, A., & Slavec, A. (2014). E-social science perspective on survey process: Towards an integrated web questionnaire development platform. In *Improving survey methods* (pp. 170-183). Routledge.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. *MIS quarterly*, 157-178.

Verkijika, S. F. (2018). Understanding smartphone security behaviors: 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

Verma, S., Gautam, R. K., Pandey, S., Mishra, A., & Shukla, S. (2017). Sampling typology and techniques. *International Journal for Scientific Research and Development*, *5*(9), 298-301.

Verplanken, B., & Orbell, S. (2003). Reflections on past behavior: a self-report index of habit strength 1. *Journal of applied social psychology*, *33*(6), 1313-1330.

Vina, G. (2016). Patients in limbo after cyber attack. *Financial Times*, 2.

Vijandren, 2019. Electronic sources: Universiti Malaya Staff Personal Data, Banking and Salary Details Leaked Online. https://www.lowyat.net/2019/196895/universiti-malaya-staff-data-leaked-online/ (20 November 2019)

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Journal of Information Privacy and Security*, *9*(4), 52-79.

Wang, F., & Chen, Y. (2012). From potential users to actual users: Use of e-government service by Chinese migrant farmer workers. *Government*

Information Quarterly, *29*, S98-S111.

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, *20*(3), 267-284.

Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law and Security Review*, *32*(5), 715–728. https://doi.org/10.1016/j.clsr.2016.07.002

Wedutenko, A. (2015). Cyber attacks: Get your governance in order. *Governance Directions*, *67*(10), 598-601.

Weijters, B., & Baumgartner, H. (2012). Misresponse to reversed and negated items in surveys: A review. *Journal of Marketing Research*, *49*(5), 737-747.

Weinstein, N. D. (1989). Effects of personal experience on self-protective behavior. *Psychological bulletin*, *105*(1), 31.

Wilding, S., Conner, M., Sandberg, T., Prestwich, A., Lawton, R., Wood, C., Miles, E., Godin, G., & Sheeran, P. (2016). The question-behaviour effect: A theoretical and methodological review and meta-analysis. *European Review of Social Psychology*, *27*(1), 196–230. https://doi.org/10.1080/10463283.2016.1245940

William, G. Z., & Barry, J. B. (2007). *Exploring Marketing Research*. United States of America: South-Western Publishing Co.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly: Management Information Systems*, *37*(1), 1–20. https://doi.org/10.25300/MISQ/2013/37.1.01

Wirth, O. (2017). COMMENTARY: Process Safety: Look Looking Beyond Personal Safety to Address Occupational Hazards and Risks. *Journal of Organizational Behavior Management*, *37*(3-4), 347-355.

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education and Behavior*, *27*(5), 591–615. https://doi.org/10.1177/109019810002700506

Wold, H. (1974). Causal flows with latent variables: partings of the ways in the light of NIPALS modelling. *European economic review*, *5*(1), 67-86.

Wold, H. (1975). Path models with latent variables: The NIPALS approach. In *Quantitative sociology* (pp. 307-357). Academic Press.

Wold, H. (1982). Soft modelling: the basic design and some extensions. *Systems under indirect observation, Part II*, 36-37.

Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). a P Rotection M Otivation T Heory a Pproach To H Ome W Ireless S Ecurity. *Information Systems*, 367–380.

Wong, K. K. K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, *24*(1), 1-32.

Wright, K. B. (2005). Researching Internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. *Journal of computer-mediated communication*, *10*(3), JCMC1034.

Wright, S. (1921). Correlation and causation. *Journal of Agricultural Research*, 20, 557- 585

Yaghmaie, F. (2003). Content validity and its estimation. *Journal of medical education*, *3*(1).

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior*, *84*, 375–382. https://doi.org/10.1016/j.chb.2018.02.019

Ye, C., & Potter, R. (2011). The role of habit in post-adoption switching of personal information technologies: An empirical investigation. *Communications of the Association for Information Systems*, *28*(1), 35.

Yildiz, M. (2017). Y ı ld ı z, Mete (2007), "Decision-Making in E-government Projects: The Case of Turkey", Goktug Morcol (Ed.), Handbook of Decision-Making, Marcel Dekker Publications, pp. 395-416. January 2007, 395–416.

Yoon, C., Hwang, J. W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of information systems education*, *23*(4), 407-416.

Zhan, X. (2019). Impact of framing and base size of computer security risk information on user behavior. 88.

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

Zissis, D., & Lekkas, D. (2011). Securing e-Government and e-Voting with an open cloud computing architecture. *Government Information Quarterly*, *28*(2), 239–251. https://doi.org/10.1016/j.giq.2010.05.010

Zulhuda, S. (2012). The state of e-government security in Malaysia : reassessing the legal and regulatory framework on the threat of information theft. *1st Taibah University International Conference on Computing and Information Technology (ICCIT 2012)*, 812–817. http://irep.iium.edu.my/27226/

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *00*(00), 1–16. https://doi.org/10.1080/08874417.2020.1712269