DAFTAR PUSTAKA

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological Bulletin*, *107*(2), 238–246. https://doi.org/10.1037/0033-2909.107.2.238

Blanthorne, C., Jones-Farmer, L. A., & Almer, E. D. (2006). Why you should consider SEM: A guide to getting started. *Advances in Accounting Behavioral Research*, *9*, 179–207. https://doi.org/10.1016/S1475-1488(06)09007-7/FULL/XML

Butler, R. (2020). A systematic literature review of the factors affecting smartphone user threat avoidance behaviour. *Information and Computer Security*, *28*(4), 555–574. https://doi.org/10.1108/ICS-01-2020-0016/FULL/XML

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, *44*(1), 380–407. https://doi.org/10.17705/1CAIS.04422

Choquette-Choo, C. A., Dullerud, N., Dziedzic, A., Zhang, Y., Jha, S., Papernot, N., & Wang, X. (2021). *CaPC Learning: Confidential and Private Collaborative Learning*. http://arxiv.org/abs/2102.05188

Djatsa, F. (2020). Threat Perceptions, Avoidance Motivation and Security Behaviors Correlations. *Journal of Information Security*, *11*(1), 19–45. https://doi.org/10.4236/JIS.2020.111002

Dzihni, A. S., Andreswari, R., & Hasibuan, M. A. (2019). Business process analysis and academic information system audit of helpdesk application using genetic algorithms a process mining approach. *Procedia Computer Science*, *161*, 903–909. https://doi.org/10.1016/j.procs.2019.11.198

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Ghozali, I., & Kusumadewi, K. A. (2023). *Partial least aquares : konsep, teknik dan aplikasi menggunakan program SmartPLS 4.0* (1st ed.). Yoga Pratama.

Gillam, A. R., & Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in Human Behavior*, *108*, 106319. https://doi.org/10.1016/J.CHB.2020.106319

Hair, J. F. J., Gabriel, M. L. D. da S., & Patel, V. K. (2014). Modelagem de Equações Estruturais Baseada em Covariância (CB-SEM) com o AMOS: Orientações sobre a sua aplicação como uma Ferramenta de Pesquisa de Marketing. *ReMark - Revista Brasileira de Marketing*, *13*(2), 44–55. https://doi.org/10.5585/remark.v13i2.2718

Hansch, N., & Benenson, Z. (2014). Specifying IT security awareness. *Proceedings - International Workshop on Database and Expert Systems Applications, DEXA*, 326–330. https://doi.org/10.1109/DEXA.2014.71

Huang, D. L., Rau, P. L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour and Information Technology*, *29*(3), 221–232. https://doi.org/10.1080/01449290701679361

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective Qerterly ^h^hb Avoidance of Information Technology Threats: a theoretical perspective1. In *Source: MIS Quarterly* (Vol. 33, Issue 1). http://www.jstor.orgStableURL:http://www.jstor.org/stable/20650279http://www.jstor.org/page/info/about/policies/terms.jsp

Liang, H., & Xue, Y. (2010a). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. https://doi.org/10.17705/1jais.00232

Liang, H., & Xue, Y. (2010b). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. https://doi.org/10.17705/1jais.00232

Liang, H., & Xue, Y. (2010c). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413. https://doi.org/10.17705/1jais.00232

Machali, I. (2021). *Metode Penelitian Kuantitatif Panduan Praktis Merencanakan, Melaksanakan dan Analisis dalam Penelitian Kuantitatif* (A. Q. Habib, Ed.). FakultasIlmuTarbiyahdanKeguruan.

Mark, M. S., Borda, O., Stroman, J., Member, C., & Wilson, T. C. (2021). *An Analysis Of Factors Influencing Phishing Threat Avoidance Behavior: A Quantitative Study*.

Raharjo, B. (2021). *Keamanan sistem informasi* (J. T. Santoso, Ed.). Yayasan Prima Agus Teknik.

Ramayani, Y., Oktarina, T., Palembang Jl Jenderal Yani No, D. A., Seberang Ulu, K. I., & Selatan, S. (2022). *Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA)*. *7*(2), 289–296.

Razzaq, A., Aditya, M., Widya, A., Kuncoro Putri, O., Musthofa, D. L., & Widodo, P. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator). *Global Political Studies Journal*, *6*. https://doi.org/10.34010/gpsjournal.v6i1

Restama, M., & Efni Salam, N. (2014). Efektifitas Portal Akademik Sebagai Sarana Penyampaian Informasi Akademik Bagi Mahasiswa Universitas Riau. In *Jom FISIP* (Vol. 1, Issue Oktober).

Rifai, A., Meliyani, A., Chyntia, P., & Sakti, I. A. (2023). Penerapan Metode Technology Threat Avoidance Theory Terhadap Tingkat Kesadaran Data Privasi Pengguna Media Sosial. *Journal of Information System Research (JOSH)*, *4*(3), 1026–1032. https://doi.org/10.47065/josh.v4i3.3081

Rosadi, S. D., & Pratama, G. G. (2018). Urgensi Perlindungandata Privasidalam Era Ekonomi Digital Di Indonesia. *Veritas et Justitia*, *4*(1), 88–110. https://doi.org/10.25123/VEJ.V4I1.2916

Saidi, K., & Prayudi, Y. (2021). *Analisis Indikator Utama Dalam Information Security-Personality Threat Terhadap Phishing Attack Menggunakan Metode Technology Threat Avoidance Theory (TTAT)*. Justindo.

Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017). Membership Inference Attacks Against Machine Learning Models. *Proceedings - IEEE Symposium on Security and Privacy*, 3–18. https://doi.org/10.1109/SP.2017.41

Siregar, Z. M. E., Parlaungan, A., Supriadi, Y. N., Ende, & Pristiyono. (2021). *Structural Equation Modeling Konsep Dan Implementasinya Pada Kajian Ilmu Manajemen Dengan Menggunakan AMOS*.

Sugiyono. (2019). *Metode Penelitian Kuantitatif* (Setiyawami, Ed.). Alfabeta.

Sylvester, F. L. (2022). Mobile Device Users' Susceptibility to Phishing Attacks. *International Journal of Computer Science and Information Technology*, *14*(1), 1–18. https://doi.org/10.5121/ijcsit.2022.14101

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

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 Behavior*, *101*, 286–296. https://doi.org/10.1016/J.CHB.2019.07.034

Waluyo, M., & Rachman, M. (2020). *Mudah Cepat Tepat Dalam Aplikasi Structural Equation Modeling* (N. A. Rahma, Ed.). Literasi Nusantara. www.penerbitlitnus.co.id