

BAB V

PENUTUP

5.1 Kesimpulan

Penelitian menggunakan 202 respons pelaku UMKM pengguna *e-payment* yang diperoleh melalui penyebaran kuesioner secara langsung dan melalui media digital. Model pengukuran memenuhi kriteria yang digunakan karena seluruh *outer loading* berada pada rentang 0,722–0,909, nilai reliabilitas melebihi 0,70, AVE berada di atas 0,50, dan HTMT berada di bawah 0,90. Kondisi tersebut menunjukkan bahwa indikator yang digunakan mampu mengukur konstruk secara konsisten sebelum hubungan struktural ditafsirkan.

Fraud Awareness berpengaruh positif terhadap Persepsi Penipuan Keuangan Online dengan koefisien 0,318, *t-statistic* 5,803, dan *p-value* < 0,001. H1 diterima. Peningkatan kesadaran mengenai modus, tanda bahaya, serta praktik perlindungan berkaitan dengan penilaian yang lebih kuat terhadap keseriusan dan kerentanan penipuan keuangan online.

Literasi Keuangan Digital berpengaruh positif terhadap Persepsi Penipuan Keuangan Online dengan koefisien 0,259, *t-statistic* 4,270, dan *p-value* < 0,001. H2 diterima. Kemampuan memahami fungsi layanan, keamanan akun, autentikasi, pengaduan, dan hak pengguna membantu responden membaca risiko transaksi digital dengan lebih terarah.

Kepercayaan pada *E-Payment* berpengaruh positif terhadap Persepsi Penipuan Keuangan Online dengan koefisien 0,182, *t-statistic* 3,097, dan *p-value* 0,002. H3 diterima. Kepercayaan yang bertumpu pada kompetensi dan keandalan

penyedia berkaitan dengan penerimaan terhadap mekanisme keamanan dan informasi risiko yang tersedia pada layanan pembayaran digital.

Nilai R^2 PPKO sebesar 0,269 menunjukkan bahwa *Fraud Awareness*, Literasi Keuangan Digital, dan Kepercayaan pada *E-Payment* secara bersama-sama menjelaskan 26,9% variasi Persepsi Penipuan Keuangan Online. Proporsi sebesar 73,1% berada di luar model, sehingga kemampuan penjelasan model berada pada kategori lemah. FA mempunyai koefisien dan f^2 terbesar, diikuti LKD dan KEP, tetapi ketiga ukuran efek tetap berada pada kategori kecil.

5.2 Keterbatasan Penelitian

Penggunaan *non-probability purposive sampling* membatasi kemampuan hasil untuk mewakili seluruh pelaku UMKM pengguna *e-payment* di Indonesia. Responden dipilih berdasarkan kesesuaian dengan kriteria penelitian. Jumlah 202 responden telah melampaui kebutuhan minimum analisis, tetapi kecukupan jumlah sampel tidak menghilangkan batas representasi yang berasal dari teknik pemilihan responden.

Pengukuran dilakukan satu kali melalui kuesioner dengan desain *cross-sectional*, sehingga jawaban menggambarkan pengetahuan, kemampuan, kepercayaan, dan persepsi responden pada periode pengumpulan data. Perubahan pengalaman transaksi, paparan edukasi keamanan, atau pengalaman menghadapi modus penipuan setelah periode pengisian tidak tercakup pada data. Penggunaan jawaban berbasis persepsi juga membuat hasil menjelaskan cara responden menilai ancaman, bukan jumlah kejadian penipuan yang benar-benar dialami.

Nilai R^2 sebesar 0,269 memperlihatkan bahwa model baru menjelaskan 26,9% variasi Persepsi Penipuan Keuangan Online, sedangkan 73,1% berkaitan dengan faktor lain di luar tiga konstruk yang diuji. Nilai Q^2 juga belum tersedia pada keluaran analisis, sehingga relevansi prediktif model belum dapat dinilai secara numerik. Keterbatasan ini membuat kekuatan model perlu dibaca dari ukuran yang tersedia tanpa menganggap hubungan yang didukung secara statistik sebagai penjelasan penuh terhadap persepsi penipuan.

5.3 Saran

Penelitian berikutnya dapat memperluas representasi responden melalui teknik sampling probabilitas apabila kerangka sampel tersedia, atau menyusun pembagian sampel yang lebih terencana menurut wilayah, jenis usaha, dan karakteristik penggunaan *e-payment*. Jumlah responden yang lebih besar dapat dipadukan dengan distribusi sampel yang lebih merata agar hasil tidak hanya bertumpu pada kelompok pelaku usaha yang paling mudah dijangkau melalui jalur tertentu.

Pengembangan desain dapat menggunakan pengukuran pada lebih dari satu waktu atau melengkapi kuesioner dengan informasi perilaku yang relevan apabila dapat diperoleh secara etis dan konsisten. Pendekatan tersebut dapat membantu melihat apakah perubahan pengalaman transaksi, edukasi keamanan, atau paparan modus penipuan diikuti perubahan persepsi risiko. Pemisahan antara persepsi ancaman dan kejadian viktimisasi tetap perlu dipertahankan agar konstruk dependen tetap mengikuti definisi yang telah ditetapkan.

Pengembangan model dapat mempertimbangkan konstruk lain yang memiliki dasar teori dan dukungan penelitian terdahulu, seperti pengalaman penipuan, perilaku keuangan, efikasi diri, paparan informasi keamanan, atau persepsi risiko. Penambahan variabel diarahkan untuk memperluas penjelasan terhadap 73,1% variasi PPKO yang belum tercakup, bukan sekadar menaikkan R^2 . Pengujian berikutnya juga perlu melengkapi ukuran prediktif melalui Q^2 atau prosedur prediksi yang tersedia pada SmartPLS agar evaluasi model mencakup daya jelas sekaligus relevansi prediktif.

DAFTAR PUSTAKA

- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Aljaradat, A., & Shukla, S. (2026). Cybersecurity and trust formation in digital payment use behaviour in North India. *Discover Sustainability*, 7, 498. <https://doi.org/10.1007/s43621-026-02769-x>
- Alrawad, M., Lutfi, A., Almaiah, M. A., & Elshaer, I. A. (2023). Examining the influence of trust and perceived risk on customers' intention to use NFC mobile payment system. *Journal of Open Innovation: Technology, Market, and Complexity*, 9(2), 100070. <https://doi.org/10.1016/j.joitmc.2023.100070>
- Bosnjak, M., Ajzen, I., & Schmidt, P. (2020). The theory of planned behavior: Selected recent advances and applications. *Europe's Journal of Psychology*, 16(3), 352–356. <https://doi.org/10.5964/ejop.v16i3.3107>
- Chen, L., Li, H., Chua, Y. P., & Chen, J. (2026). When awareness is not enough: Online fraud susceptibility, threat awareness, anti-fraud self-efficacy and online scam prevention behavior among Chinese university students. *Frontiers in Psychology*, 17, 1857855. <https://doi.org/10.3389/fpsyg.2026.1857855>
- Isaia, E., Oggero, N., & Sandretto, D. (2024). Is financial literacy a protection tool from online fraud in the digital era? *Journal of Behavioral and Experimental Finance*, 44, 100977. <https://doi.org/10.1016/j.jbef.2024.100977>

Jangir, K., Sharma, V., Taneja, S., & Rupeika-Apoga, R. (2023). The moderating effect of perceived risk on users' continuance intention for FinTech services. *Journal of Risk and Financial Management*, 16(1), 21.

<https://doi.org/10.3390/jrfm16010021>

Koning, L., Junger, M., & Veldkamp, B. (2024). Risk factors for fraud victimization: The role of socio-demographics, personality, mental, general, and cognitive health, activities, and fraud knowledge. *International Review of Victimology*, 30(3), 443–479. <https://doi.org/10.1177/02697580231215839>

Koskelainen, T., Kalmi, P., Scornavacca, E., & Vartiainen, T. (2023). Financial literacy in the digital age—A research agenda. *Journal of Consumer Affairs*, 57(1), 507–528. <https://doi.org/10.1111/joca.12510>

Kubilay, E., Raiber, E., Spantig, L., Cahlíková, J., & Kaaria, L. (2023). Can you spot a scam? Measuring and improving scam identification ability. *Journal of Development Economics*, 165, 103147.

<https://doi.org/10.1016/j.jdeveco.2023.103147>

Musa, H. G., Fatmawati, I., Nuryakin, N., & Suyanto, M. (2024). Marketing research trends using Technology Acceptance Model (TAM): A comprehensive review of researches (2002–2022). *Cogent Business & Management*, 11(1), 2329375. <https://doi.org/10.1080/23311975.2024.2329375>

Puri, L., Kumar, A., & Singh, R. (2025). What drives or discourages fraud-safe behavior in digital transactions? A BRT perspective. *Acta Psychologica*, 260, 105675. <https://doi.org/10.1016/j.actpsy.2025.105675>

Ringle, C. M., Wende, S., & Becker, J.-M. (2024). *SmartPLS 4* [Computer software]. SmartPLS. <https://www.smartpls.com>

Setiawan, M., Effendi, N., Santoso, T., Dewi, V. I., & Sapulette, M. S. (2022). Digital financial literacy, current behavior of saving and spending and its future foresight. *Economics of Innovation and New Technology*, 31(4), 320–338. <https://doi.org/10.1080/10438599.2020.1799142>

Widjanarko, K., Budiono, C. B., & Evelyn. (2025). Digital financial literacy, financial stress, and scam awareness: The moderating role of financial behavior. *Jurnal Terapan Ilmu Manajemen dan Bisnis*, 8(2), 130–155. <https://doi.org/10.58303/hhgs4010>

Balakrishnan, V., Ahhmed, U., & Basheer, F. (2025). Personal, environmental and behavioral predictors associated with online fraud victimization among adults. *PLOS ONE*, 20(1), e0317232. <https://doi.org/10.1371/journal.pone.0317232>

DeLiema, M., & 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>

Ravikumar, T., Suresha, B., Prakash, N., Vazirani, K., & Krishna, T. A. (2022). Digital financial literacy among adults in India: Measurement and validation. *Cogent Economics & Finance*, 10(1), 2132631. <https://doi.org/10.1080/23322039.2022.2132631>

Sleiman, K. A. A., Juanli, L., Lei, H., Liu, R., Ouyang, Y., & Rong, W. (2021).

User trust levels and adoption of mobile payment systems in China: An empirical analysis. *SAGE Open*, 11(4), 1–16.

<https://doi.org/10.1177/21582440211056599>

Williams, E. J., & Joinson, A. N. (2020). Developing a measure of information seeking about phishing. *Journal of Cybersecurity*, 6(1), tyaa001.

<https://doi.org/10.1093/cybsec/tyaa001>

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N.

(2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82–97.

<https://doi.org/10.1080/08874417.2020.1712269>