

**STRATEGI PERLINDUNGAN DATA PRIBADI NASABAH
TERHADAP ANCAMAN *SOCIAL ENGINEERING* PADA
LAYANAN *MOBILE BANKING***

Azy Athoillah Yazid^{1,*}

Received: March 12, 2025 | Accepted: May 09, 2025 | Published: June 11, 2025

¹Sekolah Tinggi Agama Islam Darul Ulum Banyuwangi; azyathoillah@gmail.com

*Correspondence: azyathoillah@gmail.com

Abstract: The rapid adoption of mobile banking in Indonesia has been paralleled by an increase in digital financial crimes, particularly those leveraging social engineering tactics to compromise customer personal data. This study investigates the strategies employed by PT Bank Rakyat Indonesia (BRI) KCP Muncar to protect customer personal data from mobile banking fraud, specifically focusing on social engineering threats. A qualitative case study approach was utilized, with data collected through in-depth interviews with bank personnel (including the Branch Manager and Customer Service), direct observation during a one-month internship, and analysis of relevant documents and digital platforms. The findings reveal a landscape of evolving fraud *modus operandi*, including *phishing*, *vishing*, and impersonation scams. The bank's protective strategy is primarily preventive, focusing on continuous customer education through direct interaction, telemarketing, and in-app notifications, emphasizing the confidentiality of credentials like OTP and PIN. However, a critical gap exists in remedial action, as the bank cannot recover financial losses when customer negligence is involved. This research underscores the necessity of a shared responsibility model, combining institutional safeguards with enhanced customer digital literacy. The study contributes to the discourse on consumer protection in the digital banking era and highlights the need for more robust, responsive mechanisms to address the aftermath of successful social engineering attacks.

Keywords: Customer Data Protection; Mobile Banking; Social Engineering; Fraud; BRI

1. Pendahuluan

Industri perbankan, sebagai pilar utama perekonomian, beroperasi berdasarkan asas kepercayaan (Undang-undang RI nomor 10 Tahun 1998). Fungsi intermediasi

<https://doi.org/10.59943/economic>

Publisher's Note: Program Studi Ekonomi Syariah Sekolah Tinggi Agama Islam Darul Ulum Banyuwangi, Indonesia stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

bank, yang menghimpun dan menyalurkan dana masyarakat, sangat bergantung pada keyakinan nasabah bahwa dana dan data mereka aman (Lukman Santoso, 2011). Kepercayaan ini menjadi fondasi yang kokoh dalam hubungan antara bank dan nasabahnya. Namun, era digital telah membawa tantangan baru yang kompleks terhadap fondasi ini, menguji ketahanan sistem keamanan dan kesadaran individu.

Revolusi industri 4.0 telah mendorong transformasi digital di sektor jasa keuangan, ditandai dengan maraknya layanan *mobile banking* (m-banking). Layanan ini menawarkan kemudahan dan kecepatan transaksi yang belum pernah ada sebelumnya, mendorong pergeseran perilaku masyarakat dari transaksi tunai (*cash-based*) ke non-tunai (*cashless*). Bank Indonesia mencatat peningkatan signifikan dalam volume transaksi uang elektronik, mengindikasikan adopsi teknologi finansial yang masif di masyarakat (Bank Indonesia, 2020). Kemudahan ini, sayangnya, juga membuka celah baru bagi pelaku kejahatan.

Di balik kemudahan yang ditawarkan, muncul ancaman serius berupa kejahatan siber yang menargetkan nasabah bank. Salah satu modus yang paling meresahkan adalah *social engineering*, yaitu manipulasi psikologis yang mengeksploitasi kelengahan manusia untuk mendapatkan akses ke informasi rahasia (Hadrnagy, 2018). Pelaku tidak lagi membobol sistem keamanan bank secara teknis, melainkan "membobol" nasabah itu sendiri dengan menyamar sebagai pihak terpercaya, seperti petugas bank, kurir, atau bahkan teman.

Sepanjang tahun 2022, berbagai modus penipuan *social engineering* bermunculan dan menyasar nasabah perbankan di Indonesia. Data dari Kepolisian dan pemberitaan media massa menunjukkan peningkatan kasus penipuan *online* dengan modus yang semakin canggih. Contohnya, penangkapan 12 pelaku di Lampung oleh Polres Tulang Bawang yang menggunakan situs aplikasi BRI Mobile palsu untuk menjebak korban dengan modus perubahan tarif transfer (Kompas.com, 2022). Modus ini menunjukkan bagaimana pelaku memanfaatkan isu yang relevan dan terstruktur untuk mengelabui korbannya.

Modus operandi penipuan m-banking sangat beragam dan terus berevolusi. Mulai dari *phishing* melalui tautan palsu di media sosial atau *email*, *vishing* (panggilan suara palsu) yang meminta kode OTP (One Time Password), hingga *impersonation* di aplikasi pesan instan dengan menggunakan foto profil dan nama yang mirip dengan akun resmi bank (CNN Indonesia, 2022). Keragaman modus ini menuntut kewaspadaan ekstra dari nasabah dan strategi perlindungan yang komprehensif dari pihak bank.

Bank Rakyat Indonesia (BRI), sebagai salah satu bank terbesar di Indonesia dengan basis nasabah yang luas, khususnya di segmen mikro, kecil, dan menengah, menghadapi tantangan besar dalam melindungi nasabahnya. Berdasarkan observasi dan wawancara di BRI Kantor Cabang Pembantu (KCP) Muncar, terjadi peningkatan signifikan jumlah pengguna BRI Mo (aplikasi *mobile banking* BRI) dari 2.105 (Des 2021-2022) menjadi 3.363 (hingga 19 Desember 2022), melebihi target. Peningkatan adopsi ini secara proporsional meningkatkan risiko nasabah terpapar modus penipuan.

Situasi ini menciptakan dilema. Di satu sisi, bank gencar mendorong digitalisasi untuk efisiensi dan inklusi keuangan. Di sisi lain, maraknya penipuan berbasis *social engineering* mengikis kepercayaan nasabah. Bahkan, beberapa nasabah menjadi sangat paranoid hingga menolak konfirmasi dari *customer service* asli karena takut tertipu. Hal ini mengindikasikan adanya kesenjangan antara upaya perlindungan bank dan pemahaman nasabah, yang berpotensi menghambat adopsi layanan digital itu sendiri. Penelitian ini bertujuan untuk menganalisis secara mendalam strategi perlindungan data pribadi yang diterapkan oleh BRI KCP Muncar dalam menghadapi ancaman *social engineering* pada layanan *mobile banking*.

2. Bahan dan Metode

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus. Pendekatan ini dipilih untuk memperoleh pemahaman yang mendalam dan kontekstual mengenai fenomena strategi perlindungan data nasabah di BRI KCP Muncar (Yin, 2018). Studi kasus memungkinkan peneliti untuk mengeksplorasi secara rinci bagaimana strategi dirumuskan, diimplementasikan, dan dihadapi tantangannya dalam setting organisasi yang nyata.

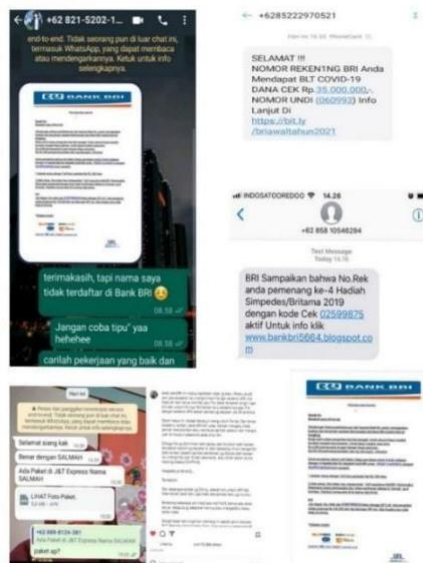
Lokasi penelitian dilaksanakan di PT Bank Rakyat Indonesia (Persero) Tbk. Kantor Cabang Pembantu (KCP) Muncar, Banyuwangi, selama satu bulan, mulai tanggal 5 Desember hingga 30 Desember 2022. Pemilihan lokasi ini didasarkan pada aksesibilitas dan relevansi permasalahan, mengingat KCP Muncar melayani basis nasabah yang beragam dan berpotensi besar menjadi target penipuan *online*. Kehadiran peneliti sebagai peserta Praktik Pengalaman Lapangan (PPL) memungkinkan dilakukannya observasi partisipatif secara intensif.

Teknik pengumpulan data dilakukan melalui tiga cara utama: (1) Wawancara mendalam (*in-depth interview*) dengan narasumber kunci, yaitu Bapak Febry Kushargiyanto (Pimpinan BRI KCP Muncar), Ibu Maria (staf), dan Adinda (Customer Service). Wawancara berfokus pada pemahaman mereka tentang modus penipuan, strategi pencegahan dan penanganan, serta tantangan yang dihadapi. (2) Observasi partisipatif, di mana peneliti terlibat langsung dalam kegiatan operasional harian seperti membantu pembukaan rekening, melakukan telemarketing untuk edukasi nasabah, dan mengamati interaksi antara staf bank dengan nasabah. (3) Dokumentasi dan analisis konten, yang meliputi penelaahan terhadap profil perusahaan, laporan internal, konten edukasi dalam aplikasi BRImo, serta berita dan artikel terkait penipuan m-banking. Analisis data menggunakan model interaktif Miles, Huberman, dan Saldaña (2020) yang mencakup kondensasi data, penyajian data, dan penarikan kesimpulan/verifikasi. Keabsahan data diuji melalui triangulasi sumber dan teknik.

3. Hasil

3.1. Bentuk Modus Penipuan (*Social Engineering*) yang Dihadapi Nasabah

Hasil wawancara dengan Adinda (Customer Service) dan observasi lapangan mengungkapkan bahwa modus penipuan yang menargetkan nasabah BRI KCP Muncar sangat beragam dan terus berkembang. Berdasarkan laporan nasabah yang masuk, modus yang paling sering ditemui adalah modus perubahan tarif, di mana nasabah menerima pesan WhatsApp yang mengatasnamakan BRI dan memberitahukan adanya kenaikan tarif transaksi menjadi Rp150.000 per bulan, lalu diarahkan untuk mengklik tautan palsu. Modus lainnya termasuk permintaan kode OTP dengan berpura-pura sebagai petugas bank yang sedang melakukan verifikasi data, serta modus kurir palsu yang mengirimkan tautan pelacakan paket yang ternyata adalah *phishing link* untuk mencuri data *mobile banking*. Temuan ini selaras dengan pemberitaan nasional mengenai maraknya *typosquatting* dan *spoofing* domain yang meniru situs resmi bank (RedPoint, 2023; CNN Indonesia, 2022).



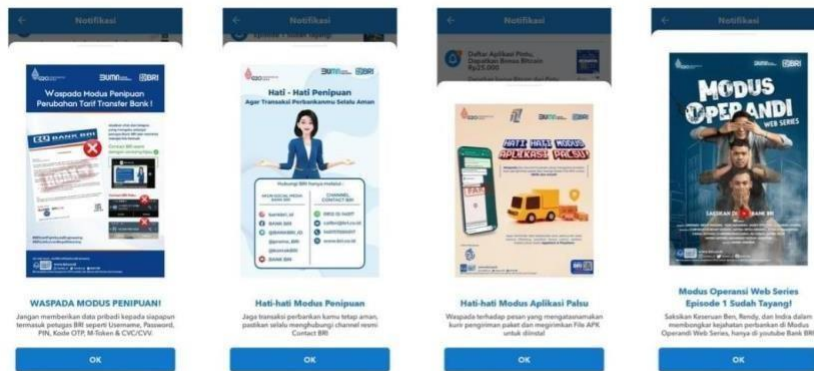
Gambar 1. Contoh tangkapan layar modus penipuan yang beredar di masyarakat, menunjukkan upaya *scammer* untuk meniru tampilan dan komunikasi resmi bank.

Sumber: internet, diakses 12 Desember 2022

3.2. Strategi Perlindungan Data Nasabah oleh BRI KCP Muncar

Strategi perlindungan data nasabah yang diterapkan oleh BRI KCP Muncar dapat dikategorikan menjadi dua pendekatan utama: preventif (pencegahan) dan reaktif (penanganan). Pendekatan preventif menjadi fokus utama. Berdasarkan wawancara dengan Ibu Maria, bank secara konsisten mengimbau nasabah untuk tidak pernah membagikan data pribadi seperti username, PIN, password, kode CVV, dan terutama kode OTP kepada siapa pun, termasuk pihak yang mengaku dari bank. Imbauan ini disampaikan melalui berbagai kanal: secara langsung oleh *customer service* di akhir setiap transaksi, melalui panggilan telepon (telemarketing) untuk konfirmasi dan edukasi, serta melalui fitur notifikasi dan banner di dalam aplikasi BRI Mo. Bank juga

menyediakan saluran resmi yang dapat dihubungi nasabah untuk konfirmasi, yaitu Contact Center 14017/1500017 dan WhatsApp Sabrina di 0812-12-14017. Upaya edukasi yang lebih masif juga dilakukan melalui kampanye digital, seperti web series "Modus Operandi" yang bertujuan meningkatkan kewaspadaan masyarakat.



Gambar 2. Tampilan fitur keamanan dan peringatan dalam aplikasi BRI Mo yang mendukung nasabah untuk menjaga kerahasiaan data pribadi mereka.

Sumber: Aplikasi BRI Mo, diakses 12 Desember 2022

Pendekatan reaktif dilakukan ketika nasabah melaporkan telah menjadi korban penipuan. Prosedur standar yang dilakukan *customer service* adalah mendengarkan kronologi kejadian, mengonfirmasi data apa saja yang telah diberikan nasabah kepada penipu, memberikan empati, dan membantu nasabah untuk mengamankan rekeningnya. Tindakan pengamanan meliputi pemblokiran rekening sementara, reset password, atau penggantian kartu ATM. Namun, berdasarkan penuturan Adinda, terdapat keterbatasan yang signifikan: bank tidak dapat mengembalikan dana nasabah yang telah hilang. Hal ini didasari oleh temuan bahwa kehilangan dana terjadi karena nasabah secara sukarela memberikan data rahasia seperti OTP dan password, yang mana hal tersebut merupakan kelalaian nasabah dan di luar kendali sistem keamanan bank. Ibu Maria menegaskan, "Jangan sesekali memberi kode OTP, password ke orang lain, ke orang terdekat sekalipun, suaminya, isterinya atau anaknya, itu rahasia pribadi."

4. Pembahasan

Temuan penelitian ini menunjukkan bahwa ancaman utama terhadap data nasabah bukan berasal dari lemahnya sistem keamanan teknis bank, melainkan dari teknik *social engineering* yang mengeksploitasi faktor manusia (Hadnagy, 2018). BRI KCP Muncar telah mengimplementasikan sistem keamanan berlapis, namun "lapisan terluar" yang paling rentan adalah nasabah itu sendiri. Keragaman modus yang ditemukan, mulai dari *phishing* hingga *vishing*, mengonfirmasi bahwa pelaku terus berinovasi dalam menciptakan skenario yang meyakinkan untuk mengelabui korban (Nobles, 2022). Hal ini memperkuat argumen bahwa literasi digital nasabah merupakan komponen krusial dalam ekosistem keamanan siber perbankan.

Strategi preventif yang dijalankan BRI KCP Muncar, yang berfokus pada edukasi berkelanjutan, merupakan langkah yang tepat dan sesuai dengan rekomendasi Otoritas Jasa Keuangan (OJK) dalam Surat Edaran No. 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data Dan/Atau Informasi Pribadi Konsumen. Edukasi ini bertujuan untuk membangun "human firewall" dengan meningkatkan kesadaran nasabah akan taktik yang digunakan penipu (Aldawood & Skinner, 2019). Penggunaan berbagai kanal komunikasi, dari interaksi tatap muka hingga konten digital seperti *web series*, menunjukkan upaya bank untuk menjangkau nasabah dengan segmen dan preferensi yang berbeda.

Namun, terdapat kelemahan struktural yang signifikan pada pendekatan reaktif. Ketidakmampuan bank untuk mengembalikan dana korban penipuan *social engineering* menciptakan kesenjangan perlindungan yang besar. Meskipun secara hukum, berdasarkan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, bank dapat terbebas dari tanggung jawab jika kerugian disebabkan oleh kelalaian nasabah, hal ini menimbulkan pertanyaan tentang keadilan dan perlindungan konsumen. Nasabah, yang mungkin tidak memiliki literasi digital memadai, menjadi pihak yang paling dirugikan. Situasi ini dapat memicu krisis kepercayaan jangka panjang, di mana nasabah merasa rentan dan tidak terlindungi meskipun telah menjadi korban kejahatan (Masyhur, 2017).

Temuan ini menyoroti perlunya model tanggung jawab bersama (*shared responsibility*) yang lebih kuat. Bank memang memiliki kewajiban untuk menyediakan sistem yang aman dan mengedukasi nasabah, sebagaimana diamanatkan dalam Pasal 40 UU No. 10 Tahun 1998 dan POJK tentang Perlindungan Konsumen. Namun, regulator seperti OJK dan Bank Indonesia juga perlu mendorong inovasi dalam mekanisme perlindungan, misalnya dengan mewajibkan otentikasi biometrik yang lebih kuat atau membentuk dana kompensasi korban kejahatan siber (Suleman, 2020). Peningkatan literasi digital harus menjadi program nasional yang berkelanjutan, bukan hanya tanggung jawab bank semata (Setiawan et al., 2019).

Lebih jauh lagi, temuan ini mengindikasikan bahwa pertumbuhan jumlah pengguna m-banking yang melampaui target (kenaikan 110% di KCP Muncar) harus dibarengi dengan peningkatan kualitas edukasi yang sebanding. Keberhasilan kuantitatif dalam adopsi teknologi tidak boleh mengorbankan aspek kualitatif, yaitu keamanan dan kenyamanan nasabah. Bank perlu mengevaluasi efektivitas metode edukasi yang ada dan mengembangkan pendekatan yang lebih personal dan mudah dipahami oleh berbagai lapisan masyarakat, terutama kelompok yang kurang melek teknologi (Rachmawati et al., 2020). Dengan demikian, strategi perlindungan data tidak hanya bersifat prosedural, tetapi juga transformasional dalam membangun budaya sadar keamanan siber.

5. Kesimpulan

Penelitian ini menyimpulkan bahwa strategi perlindungan data nasabah BRI KCP Muncar dalam menghadapi ancaman *social engineering* pada layanan *mobile banking*

lebih bersifat preventif daripada restitutif. Bank secara aktif mengedukasi nasabah untuk menjaga kerahasiaan data pribadi melalui berbagai kanal, sebagai upaya membangun kesadaran dan kewaspadaan terhadap modus penipuan yang semakin beragam dan canggih. Namun, strategi ini memiliki kelemahan fundamental pada aspek pemulihan kerugian, di mana bank tidak dapat mengembalikan dana nasabah yang hilang akibat kelalaian sendiri, seperti memberikan kode OTP. Hal ini menciptakan kerentanan bagi nasabah, terutama mereka dengan literasi digital rendah, dan berpotensi menggerus kepercayaan terhadap sistem perbankan digital.

Implikasi dari penelitian ini menegaskan bahwa keamanan siber di sektor perbankan tidak dapat hanya bertumpu pada teknologi, tetapi membutuhkan sinergi yang kuat antara penguatan sistem keamanan bank, edukasi nasabah yang masif dan efektif, serta dukungan regulasi dari otoritas terkait. Ke depan, diperlukan pengembangan mekanisme perlindungan yang lebih komprehensif, termasuk kemungkinan adanya skema kompensasi atau asuransi bagi korban kejahatan siber yang tidak terbantahkan. Bank juga perlu terus berinovasi dalam metode edukasi agar pesan keamanan dapat terserap dengan baik oleh seluruh segmen nasabah. Penelitian lebih lanjut dapat difokuskan pada pengukuran efektivitas berbagai metode edukasi terhadap perubahan perilaku nasabah dalam menjaga kerahasiaan data pribadinya.

6. Referensi

- Aldawood, H., & Skinner, G. (2019). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. *2019 IEEE International Conference on Industrial Technology (ICIT)*, 726-731. <https://doi.org/10.1109/ICIT.2019.8755022>
- Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. *International Journal of Information Security*, 18(3), 251-266. <https://doi.org/10.1007/s10207-018-0412-9>
- Bank Indonesia. (2020). *Peraturan Bank Indonesia Nomor 22/20/PBI/2020 tentang Sistem Pembayaran*. Jakarta: Bank Indonesia.
- Button, M., & Cross, C. (2017). *Cyber Frauds, Scams and their Victims*. London: Routledge. <https://doi.org/10.4324/9781315671655>
- CNN Indonesia. (2022, September 30). 4 Modus Penipuan di Medsos Incar Nasabah BRI dan BCA. Diakses pada 11 Januari 2023, dari https://www.cnnindonesia.com/teknologi/20220930102423_192-854585/4-modus-penipuan-di-medsos-incar-nasabah-bri-dan-bca
- Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*, 20(3), 302-318. <https://doi.org/10.1177/1748895818805922>
- Furnell, S., & Moore, L. (2020). Security fatigue: The key to unlocking a major cybersecurity challenge. *Computer Fraud & Security*, 2020(5), 8-12. [https://doi.org/10.1016/S1361-3723\(20\)30050-8](https://doi.org/10.1016/S1361-3723(20)30050-8)

- Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, 28(12), 3629-3654. <https://doi.org/10.1007/s00521-016-2275-y>
- Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking* (2nd ed.). Indianapolis, IN: Wiley.
- Jansen, J., & Leukfeldt, R. (2018). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. *Computers & Security*, 73, 364-376. <https://doi.org/10.1016/j.cose.2017.11.015>
- [Kompas.com](https://www.kompas.com). (2022, November 11). 12 Penipu Berkedok Kenaikan Tarif BRI di Lampung Ditangkap, Tiru Aplikasi BRI Mobile Palsu. Diakses pada 5 Januari 2023, dari <https://amp.kompas.com/money/read/2022/12/19/063800026/kaleidoskop-2022-modus-penipuan-incar-saldo-rekening-bank>
- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113-122. <https://doi.org/10.1016/j.jisa.2014.09.005>
- Lee, M. C. (2018). Predicting and explaining the adoption of online banking: An extension of the theory of planned behavior. *Internet Research*, 28(4), 1036-1061. <https://doi.org/10.1108/IntR-01-2017-0018>
- Lukman Santoso. (2011). *Hukum Perbankan di Indonesia*. Yogyakarta: Pustaka Pelajar.
- Masyhur, F. (2017). Perlindungan Hukum Terhadap Nasabah Bank Sebagai Konsumen Pengguna Layanan Mobile Banking (M-Banking). *Jurnal Hukum IUS QUIA IUSTUM*, 24(3), 445-466. <https://doi.org/10.20885/iustum.vol24.iss3.art6>
- Miles, M. B., Huberman, A. M., & Saldaña, J. (2020). *Qualitative Data Analysis: A Methods Sourcebook* (4th ed.). Thousand Oaks, CA: SAGE Publications.
- Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, 59, 186-209. <https://doi.org/10.1016/j.cose.2016.03.004>
- Nobles, C. (2022). Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. In *Research Anthology on Advancements in Cybersecurity Education* (pp. 689-710). IGI Global. <https://doi.org/10.4018/978-1-6684-3554-0.ch036>
- Otoritas Jasa Keuangan. (2014). *Surat Edaran Otoritas Jasa Keuangan Nomor 14/SEOJK.07/2014 tentang Kerahasiaan dan Keamanan Data Dan/Atau Informasi Pribadi Konsumen*. Jakarta: OJK.
- Pienta, D., Thatcher, J. B., & Johnston, A. (2020). A taxonomy of phishing: Attack types spanning economic, temporal, and target boundaries. *Journal of the Association for Information Systems*, 21(5), 1258-1296. <https://doi.org/10.17705/1jais.00635>
- Rachmawati, Y., Ma'arif, M., Fadhilah, N., Inayah, N., Ummah, K., Siregar, M. N. F., Amalyaningsih, R., F., A. A. C., & F., A. A. (2020). Studi Eksplorasi Pembelajaran Pendidikan IPA Saat Masa Pandemi COVID-19 di UIN Sunan Ampel Surabaya. *Indonesian Journal of Science Learning*, 1(1), 32-36.

- RedPoint. (2023). *Apa Itu Cybersquatting dan TypoSquatting?*. Diakses pada 10 Januari 2023.
- Republik Indonesia. (1998). *Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan*. Lembaran Negara RI Tahun 1998 Nomor 182. Jakarta: Sekretariat Negara.
- Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara RI Tahun 2016 Nomor 251. Jakarta: Sekretariat Negara.
- Rocha Flores, W., & Ekstedt, M. (2016). A model for investigating organizational impact on information security behavior. *Information Management & Computer Security*, 24(2), 150-173. <https://doi.org/10.1108/IMCS-11-2014-0071>
- Setiawan, A. R., Puspaningrum, M., & Umam, K. (2019). Pembelajaran Fiqh Mu'Āmalāt Berorientasi Literasi Finansial. *TARBAWY: Indonesian Journal of Islamic Education*, 6(2), 187-192. <https://doi.org/10.17509/t.v6i2.20887>
- Shaikh, A. A., & Karjaluoto, H. (2015). Mobile banking adoption: A literature review. *Telematics and Informatics*, 32(1), 129-142. <https://doi.org/10.1016/j.tele.2014.05.003>
- Suleman, A. R. (2020). Tanggung Jawab Bank Terhadap Kerugian Nasabah Akibat Kejahatan Social Engineering Dalam Transaksi Perbankan Elektronik. *Jurnal Hukum & Pembangunan*, 50(3), 728-751. <https://doi.org/10.21143/jhp.vol50.no3.2807>
- Tam, L., & Glassman, M. (2020). What drives mobile banking usage? A meta-analysis. *International Journal of Bank Marketing*, 38(5), 1115-1141. <https://doi.org/10.1108/IJBM-08-2019-0301>
- Wang, J., Li, Y., & Rao, H. R. (2017). Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, 18(11), 784-806. <https://doi.org/10.17705/1jais.00472>
- Williams, E. J., & Polage, D. (2019). How persuasive is phishing email? The role of authenticity, timeliness, and individual differences in predicting click rates. *Journal of Cybersecurity Education, Research and Practice*, 2019(1), 4.
- Yin, R. K. (2018). *Case Study Research and Applications: Design and Methods* (6th ed.). Thousand Oaks, CA: SAGE Publications.

