

DAFTAR PUSTAKA

- Achmad Mukhlis, Baiq Laila Alfila, & Aliya Zhafira Wastuyana. (2023). Ancaman dan Langkah Pengamanan Sistem Informasi Menggunakan Metode *Systematic Literature Review*. *Jurnal ilmiah Sistem Informasi dan Ilmu Komputer*, 3(2), 143–152. <https://doi.org/10.55606/juisik.v3i2.496>
- Amoah, G. A., & J.B., H.-A. (2022). *QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing)*. *International Journal of Computer Applications*, 184(33), 34–39. <https://doi.org/10.5120/ijca2022922425>
- Bekavac, L., Mayer, S., & Strecker, J. (2024). *QR-Code Integrity by Design. Conference on Human Factors in Computing Systems - Proceedings*, 76–77. <https://doi.org/10.1145/3613905.3651006>
- Browne, T. O., Abedin, M., & Chowdhury, M. J. M. (2024). A Systematic Review on Research Utilising Artificial Intelligence for Open Source Intelligence (OSINT) Applications. *International Journal of Information Security*, 23(4), 2911–2938. <https://doi.org/10.1007/s10207-024-00868-2>
- Darumaya, B. A., Maarif, S., Toruan, T., & Swastanto, Y. (2023). Pemikiran Potensial Ancaman Perang Siber di Indonesia: Suatu Kajian Strategi Pertahanan. *Jurnal Keamanan Nasional*, IX(2), 299–324. <https://ejurnal.ubharajaya.ac.id/index.php/kamnas>
- Fridayani, & Cuaca, B. (2023). Transaksi Keuangan Digital Menggunakan QRIS Ditinjau dari Aspek Hukum. *Teaching and Learning Journal of Mandalika*, 4(2), 164–174.
- Galadima, S. A., Shrivastava, Dr. M., & Sonowal, Dr. G. (2024). *QR Code Phishing: A Review Of The Current Attacks And Countermeasures*. 15(1), 37–48.
- Ganesh, R., & Prabu, G. (2020). *Determination of Internet Banking Usage and Purpose with Explanation of Data Flow Diagram and Use Case Diagram*. *International Journal of Management and Humanities (IJMH)*, 0913(7), 52–58. <https://doi.org/10.35940/ijmh.G0674.034720>
- Greenspan, A. (2021). *QR Codes and The Sentient City*. *Studia Neophilologica*, 93(2), 206–218. <https://doi.org/10.1080/00393274.2021.1916993>
- Hayati, M., & Fata, D. (2021). Analisis Keamanan Informasi Pengguna Media Sosial Menggunakan SEToolkit Melalui Teknik Phising. *Djtechno Jurnal Teknologi Informasi*, 2(1), 21–28. <https://doi.org/10.46576/djtechno.v2i1.1252>
- Hevner, A. R., March, S. T., Ram, S., & Park, J. (2004). *Design Science in Information Systems Research*. 08(1), 75–105. <https://doi.org/10.1007/BF01205282>
- Hidayah, I. R. (2020). Representasi *Social Engineering* Dalam Tindak Kejahatan Dunia Maya (Analisis Semiotika Pada Film Firewall). *Tibannndaru : Jurnal Ilmu Perpustakaan dan Informasi*, 4(1), 30. <https://doi.org/10.30742/tb.v4i1.905>
- IDADX. (2024). Laporan Aktivitas *Abuse Domain .id*.
- Ingoldsby, T. R. (2021). *Attack Tree-based Threat Risk Analysis*.
- Kuipers, L. (2020). *Analysis of Attack Trees : Fast Algorithms for Subclasses*.

- Martawireja, A. R. H., Ridwan, R., Hafidzin, A. P., & Taufik, M. (2021). Proteksi Keamanan Data pada *Quick Response (QR) Code*. *Jurnal Teknologi dan Rekayasa Manufaktur*, 3(2), 99–110. <https://doi.org/10.48182/jtrm.v3i2.58>
- Muftiadi, A., Agustina, T. P. M., & Evi, M. (2022). Studi Kasus Keamanan Jaringan Komputer: Analisis Ancaman *Phising* terhadap Layanan Online Banking. *Hexatech: Jurnal Ilmiah Teknik*, 1(2), 60–65. <https://doi.org/10.55904/hexatech.v1i2.346>
- Nafilah, H. A., & Sujatmiko, B. (2024). Rancang Bangun E-Modul Berbasis Aplikasi Android Untuk Meningkatkan Kompetensi Siswa Pada Mata Pelajaran Desain Media Interaktif di SMKN 10 Surabaya. 09.
- Naik, N., Jenkins, P., Grace, P., Naik, D., Prajapat, S., & Song, J. (2024). *A Comparative Analysis of Threat Modelling Methods : STRIDE, DREAD, VAS, PASTA, OCTAVE, and LINDDUN*. https://doi.org/https://doi.org/10.1007/978-3-031-74443-3_16
- Nugraheni, T., Sinurat, A., & Kian, D. A. (2024). Analisis Yuridis Penerapan Perlindungan Hukum dalam Melindungi Pengguna Layanan *Internet Banking* dari *Cyber Crime*. *Jurnal Hukum, Politik dan Ilmu Sosial (JHPIS)*, 3(2). <https://doi.org/https://doi.org/10.55606/jhps.v3i2.3715>
- Pranata, E. J., & Ependi, L. (2023). *Phishing* terhadap Website Bank BCA. *Jurnal Trends*, 01(01), 34–40. <https://doi.org/https://doi.org/10.56772/trends.v1i1.293>
- Pratiwi, A. W., Widjajarto, A., & Budiyo, A. (2024). Pemodelan *Attack Tree* Pada *Spear Phishing Attack* di Instansi Publik dengan Metrik Granularitas Data. *Journal of Information System Research (JOSH)*, 6(1), 76–86. <https://doi.org/10.47065/josh.v6i1.5876>
- Putri, E. M. A., Febrianto, H. G., & Fitriana, A. I. (2023). *The Effect of Internet Banking, Credit Risk and Company Size on Financial Performance at Conventional Commercial Banks Listed on the IDX for the Period 2018-2022*. *International Social Sciences and Humanities UMJember Proceeding Series*, 2(3), 2023.
- Raharja, Y. (2024). Implementasi Metode OSINT untuk Mengidentifikasi Serangan Judi Online pada Website. *Jurnal Informatika Polinema*, 10(3), 359–364. <https://doi.org/10.33795/jip.v10i3.4847>
- Rahmadian, F., Maksum, M., & Rambe, M. S. (2021). Perlindungan Nasabah Bank Terhadap Tindakan *Phishing* Studi Pada PT Bank Rakyat Indonesia (Persero) Tbk. *Journal of Legal Reserch*, 2(2), 351–372. <https://doi.org/10.15408/jlr.v2i2.17933>
- Rains, T. (2020). *Cybersecurity Threats, Malware Trends, and Strategies*.
- ReliaQuest. (2023). *QR Code Phishing: 4 Ways Scanners are Being Scammed*. <https://reliaquest.com/blog/qr-code-phishing/>
- Safitri, M. E., Ameilindra, Z., & Yulianti, R. (2023). Analisis Teknik *Social Engineering* Sebagai Ancaman Dalam Keamanan Sistem Informasi: Studi Literatur. *Jurnal Ilmiah Teknologi Informasi dan Robotika*, 2(2), 21–26. <https://doi.org/10.33005/jifti.v2i2.26>
- Salahdine, F., & Kaabouch, N. (2019). *Social Engineering Attacks: A Survey*. *Future Internet*, 11(4). <https://doi.org/10.3390/FI11040089>

- Sharevski, F., Devine, A., Pieroni, E., & Jachim, P. (2022). *Phishing with Malicious QR Codes*. *ACM International Conference Proceeding Series*, 160–171. <https://doi.org/10.1145/3549015.3554172>
- Shostack, A. (2014). *Threat Modeling: Designing for Security*.
- Singh, A., Singh, N., Singh, S. K., & Nayak, S. K. (2021). *Cyber-Crime and Digital Forensics: Challenges Resolution*. *Solid State Technology*, May. <https://doi.org/10.1109/ICCCI56745.2023.10128333>
- Tabrizchi, H., & Rafsanjani, M. K. (2020). *A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions*. Dalam *Journal of Supercomputing* (Vol. 76, Nomor 12). Springer US. <https://doi.org/10.1007/s11227-020-03213-1>
- Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). *A Review of Threat Modelling Approaches for APT-Style Attacks*. *Heliyon*, 7(1), e05969. <https://doi.org/10.1016/j.heliyon.2021.e05969>
- Wibowo, B., & Hidayat, T. (2024). Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman *Phishing* di Lingkungan Perusahaan PT. XYZ. *Jurnal Pengabdian Masyarakat Sultan Indonesia*, 2(1), 1–9. <https://doi.org/10.58291/abdisultan.v2i1.294>
- Yanuar, A. P. (2021). Cyber war : Ancaman Baru Keamanan Nasional dan Internasional. *Jurnal Keamanan Nasional*, 7(1), 23–35. <https://doi.org/10.31599/jkn.v7i1.474>
- Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). *Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies*. *Cyber-Physical Energy Systems Security*, 9, 29775–29818. <https://doi.org/10.1109/ACCESS.2021.3058403>