e-ISSN: 2963-8771
DOI: 10.57254/eka.v4i3.152

Jurnal Pengabdian Kepada Masyarakat Indonesia
EKALAYA
Vol. 4, No. 3, September, 2025 hal. 621-627
Journal Page is available at http://ekalaya.nindikayla.com/index.php/home

Mitigasi Risiko Social Engineering dan Keamanan Identitas Digital pada Ekosistem Mobile Banking melalui Edukasi Preventif bagi Siswa SMA Kota Tangerang

Abdul Rahman[*1], Neng Wiwin[2], Afifah Khaerani A[3]
[1,2,3] Fakultas Sains dan Teknologi, Universitas Salakanagara
Email: abdulrahman@unsaka.ac.id[1)], nengwiwin@unsaka.ac.id[2)], afifah.khaerani@unsaka.ac.id[3)]

Abstrak

Transformasi digital di sektor perbankan telah meningkatkan aksesibilitas finansial bagi generasi muda, namun di sisi lain memperluas celah kerawanan terhadap serangan siber berbasis manipulasi psikologis. Siswa SMA sebagai pengguna aktif *mobile banking* sering kali menjadi sasaran utama kejahatan *social engineering* karena keterbatasan literasi mengenai keamanan identitas digital. Kegiatan Pengabdian kepada Masyarakat (PkM) ini bertujuan untuk meningkatkan kewaspadaan dan kemampuan teknis siswa dalam memitigasi risiko penipuan digital pada ekosistem perbankan. Metode pelaksanaan dilakukan melalui *expert-sharing* berbasis pengalaman praktisi IT perbankan, simulasi serangan *phishing*, serta edukasi proteksi kredensial seperti PIN dan OTP. Hasil kegiatan menunjukkan peningkatan signifikan pada kesadaran siswa dalam mengenali pola-pola manipulasi informasi dan teknik proteksi identitas berlapis. Evaluasi akhir membuktikan bahwa edukasi preventif ini berhasil mengubah perilaku digital siswa menjadi lebih waspada, yang menjadi faktor krusial dalam menjaga integritas ekosistem finansial digital di wilayah Kota Tangerang.
Kata kunci: *Social Engineering,* Keamanan Identitas*, Mobile Banking,* Edukasi *Preventif,* Siswa SMA*.*

Abstract

The digital transformation in the banking sector has increased financial accessibility for the younger generation, yet it has also expanded vulnerabilities to cyberattacks based on psychological manipulation. High school students, as active users of mobile banking, often become primary targets of social engineering crimes due to limited literacy regarding digital identity security. This Community Service (PkM) activity aims to enhance students' awareness and technical capabilities in mitigating digital fraud risks within the banking ecosystem. The implementation method was conducted through expert-sharing sessions based on the experience of banking IT practitioners, phishing attack simulations, and education on protecting credentials such as PINs and OTPs. The results indicated a significant increase in students' awareness of recognizing information manipulation patterns and multi-layered identity protection techniques. The final evaluation proved that this preventive education successfully changed students' digital behavior to be more vigilant, which is a crucial factor in maintaining the integrity of the digital financial ecosystem in the Tangerang City area.
Keywords: *Social Engineering, Identity Security, Mobile Banking, Preventive*

Education, High School Students.

1. PENDAHULUAN

Akselerasi transformasi digital di sektor finansial telah mengubah wajah layanan perbankan konvensional menjadi ekosistem berbasis aplikasi yang dapat diakses secara instan. Di Indonesia, penggunaan platform perbankan digital dan dompet elektronik telah menjangkau berbagai lapisan masyarakat, termasuk kelompok usia remaja atau Generasi Z (Biro Pusat Statistik, 2023). Pesatnya penetrasi *mobile banking* ini didorong oleh kemudahan transaksi, namun sering kali tidak dibarengi dengan literasi keamanan informasi yang memadai (Statista, 2024). Akibatnya, celah kerawanan beralih dari kelemahan sistem teknis menuju kerentanan pada sisi pengguna manusia, yang dalam terminologi keamanan siber dikenal sebagai "the weakest link" (Whitman & Mattord, 2021).

Ancaman paling dominan yang mengeksploitasi sisi psikologis pengguna adalah *social engineering*. Teknik ini tidak menyerang infrastruktur server bank secara langsung, melainkan memanipulasi kepercayaan pengguna untuk menyerahkan informasi rahasia seperti kata sandi, PIN, atau *One-Time Password* (OTP) (Mouton et al., 2016). Laporan ancaman siber global menunjukkan bahwa serangan berbasis manipulasi psikologis tetap menjadi vektor utama dalam insiden kebocoran data finansial (Enisa, 2022). Bagi industri perbankan, perlindungan terhadap aspek ini sangat krusial karena menyangkut integritas sistem dan kepercayaan nasabah, sebagaimana diatur secara ketat dalam standar manajemen keamanan informasi internasional (ISO/IEC 27001, 2022).

Siswa SMA di kota besar seperti Kota Tangerang merupakan salah satu segmen pengguna *mobile banking* yang paling rentan. Secara teknis, aplikasi perbankan modern telah dilengkapi dengan pengamanan berlapis (Luo et al., 2020). Namun, karakteristik remaja yang cenderung impulsif dan eksposif di media sosial membuat mereka menjadi target empuk bagi pelaku kejahatan siber (Sari & Setiadi, 2022). Pelaku sering kali menggunakan skenario penipuan yang sangat meyakinkan, mulai dari memalsukan identitas institusi hingga memanfaatkan rasa takut atau urgensi korbannya (Krombholz et al., 2015). Tanpa adanya pemahaman tentang *cyber hygiene*, identitas digital siswa dapat dengan mudah dikompromikan, yang berujung pada kerugian finansial yang signifikan (Aldawood & Skinner, 2018).

Di Indonesia, otoritas terkait telah menerbitkan regulasi ketat mengenai penyelenggaraan teknologi informasi oleh bank umum untuk memastikan perlindungan konsumen (Otoritas Jasa Keuangan, 2022). Namun, regulasi di sisi penyedia layanan harus diimbangi dengan edukasi preventif di sisi pengguna. Studi mengenai perilaku keamanan informasi menunjukkan bahwa faktor kesadaran individu memiliki pengaruh besar terhadap efektivitas mitigasi risiko siber (Purnomo & Ashari, 2021). Oleh karena itu, diperlukan sebuah pendekatan edukasi yang tidak hanya teoritis, tetapi juga praktis berdasarkan pengalaman nyata di industri keamanan siber (Peltier, 2016).

Kesenjangan antara kapabilitas keamanan sistem perbankan dengan perilaku pengguna di lapangan menjadi latar belakang utama dilaksanakannya kegiatan pengabdian ini. Sebagai praktisi yang terlibat langsung dalam pengelolaan infrastruktur IT perbankan, penulis memandang bahwa transfer pengetahuan mengenai standar keamanan industri kepada siswa SMA merupakan langkah strategis untuk menciptakan

ekosistem digital yang sehat. Edukasi ini bertujuan untuk memberikan simulasi nyata mengenai taktik-taktik *social engineering* yang berkembang saat ini dan bagaimana prosedur standar operasional perbankan dalam menangani data sensitif (Anderson, 2020).

Berdasarkan urgensi tersebut, kegiatan Pengabdian kepada Masyarakat (PkM) ini difokuskan pada mitigasi risiko *social engineering* dan penguatan keamanan identitas digital bagi siswa SMA di Kota Tangerang. Fokus utama dari pengabdian ini adalah memberikan pemahaman preventif agar siswa mampu mengidentifikasi ancaman secara dini dan mengimplementasikan perlindungan identitas berlapis pada aplikasi perbankan mereka. Melalui pendekatan ini, diharapkan para siswa tidak hanya cerdas secara finansial digital, tetapi juga memiliki ketahanan (*resilience*) terhadap berbagai modus kejahatan siber yang terus berevolusi.

2. METODE

Metode pelaksanaan kegiatan pengabdian kepada masyarakat ini menggunakan pendekatan Edukasi Preventif Berbasis Simulasi (*Simulation-Based Preventive Education*). Pendekatan ini dipilih agar siswa tidak hanya menerima teori, tetapi merasakan pengalaman langsung menghadapi skenario ancaman siber yang menyerupai kondisi riil di industri perbankan. Sasaran kegiatan adalah siswa kelas 11 dan 12 di SMA Kota Tangerang yang telah aktif menggunakan aplikasi *mobile banking* atau dompet digital. Kerangka kerja pelaksanaan dibagi menjadi empat tahapan utama:

1. Fase Asesmen dan Identifikasi Celah Keamanan: Tahap awal dilakukan dengan menyebarkan kuesioner berbasis skenario untuk mengukur tingkat kerentanan siswa terhadap manipulasi informasi. Siswa diberikan beberapa contoh pesan teks (SMS), email, dan panggilan telepon yang menyerupai modus *social engineering* populer (seperti tawaran hadiah, ancaman blokir akun, atau pembaruan sistem). Hasil dari asesmen ini digunakan untuk memetakan jenis serangan yang paling efektif mengelabui responden.
2. Fase *Expert Sharing* & Bedah Kasus Industri: Sebagai praktisi IT perbankan, penulis memaparkan standar operasional prosedur (SOP) perbankan dalam berinteraksi dengan nasabah. Pada tahap ini, dipaparkan perbedaan mendasar antara komunikasi resmi institusi keuangan dengan pola komunikasi pelaku kejahatan. Fokus materi mencakup prinsip "Zero Trust", yaitu edukasi untuk tidak memberikan data sensitif (PIN, OTP, CVV) kepada pihak manapun, termasuk pihak yang mengaku sebagai pegawai bank.
3. Fase Simulasi Interaktif *Phishing* & *Vishing*: Tahap ketiga merupakan inti dari kegiatan teknis, di mana tim PkM melakukan simulasi serangan terukur. Siswa diajak masuk ke dalam laboratorium simulasi untuk melihat bagaimana sebuah situs *phishing* bekerja menangkap kredensial secara *real-time*. Selain itu, dilakukan *role-playing* serangan *vishing* (voice phishing) untuk melatih kemampuan siswa dalam melakukan terminasi komunikasi secara tegas ketika menghadapi upaya tekanan psikologis dari penipu.
4. Fase Penguatan Proteksi Identitas Digital: Tahap akhir difokuskan pada aspek teknis preventif yang dapat dilakukan langsung pada perangkat siswa. Tim membimbing siswa untuk mengaktifkan fitur keamanan berlapis, seperti *Two-Factor Authentication* (2FA), fitur biometrik, manajemen kata sandi yang kuat,

e-ISSN: 2963-8771
DOI: 10.57254/eka.v4i3.152

serta cara melakukan pelaporan insiden keamanan melalui kanal resmi perbankan. Evaluasi keberhasilan dilakukan melalui *post-test* untuk memverifikasi perubahan perilaku dan peningkatan ketajaman analisis siswa terhadap ancaman digital.

3. HASIL DAN PEMBAHASAN

Pelaksanaan kegiatan pengabdian ini mengungkap fakta kritis mengenai perilaku digital siswa SMA di Kota Tangerang. Hasil asesmen awal menunjukkan bahwa meskipun 94% peserta aktif menggunakan aplikasi *mobile banking* dan dompet digital, hanya 12% yang memahami perbedaan antara komunikasi resmi bank dengan upaya *phishing*. Temuan ini memperkuat teori bahwa keakraban dengan teknologi (*tech-savvy*) tidak berbanding lurus dengan literasi keamanan informasi (Whitman & Mattord, 2021). Sebagian besar siswa cenderung merespons pesan yang mengandung unsur urgensi atau ancaman (seperti pemberitahuan akun diblokir), yang merupakan inti dari efektivitas serangan *social engineering* (Mouton et al., 2016).

Pada fase simulasi interaktif, terjadi transformasi kesadaran yang signifikan. Melalui peragaan situs *phishing* secara langsung, siswa dapat melihat bagaimana data kredensial yang mereka masukkan pada laman palsu dapat tercuri hanya dalam hitungan detik. Pembahasan ditekankan pada konsep "Zero Trust" di mana siswa diajarkan untuk meragukan setiap permintaan data sensitif terlepas dari seberapa meyakinkan identitas pengirimnya. Hasil observasi selama simulasi menunjukkan bahwa setelah diberikan edukasi mengenai SOP perbankan, kemampuan siswa dalam mendeteksi kejanggalan pada tautan (URL) dan struktur kalimat pesan penipuan meningkat dari 15% menjadi 88%. Hal ini membuktikan bahwa pendekatan simulasi lebih efektif dalam mengubah perilaku dibandingkan metode ceramah konvensional.

Gambar 1 Persiapan kegiatan simulasi

Analisis lebih mendalam dilakukan pada aspek proteksi identitas digital. Sebagai praktisi IT perbankan, penulis menekankan pentingnya otentikasi berlapis yang sering kali diabaikan oleh siswa karena alasan kepraktisan. Dalam sesi praktik, seluruh

peserta berhasil mengaktifkan fitur *Two-Factor Authentication* (2FA) dan sistem biometrik pada perangkat masing-masing. Diskusi kelompok mengungkapkan bahwa siswa sebelumnya tidak menyadari bahwa OTP (*One-Time Password*) adalah "kunci terakhir" yang tidak boleh dibagikan kepada siapa pun, termasuk pihak bank sendiri. Pemahaman ini sangat krusial mengingat regulasi OJK Nomor 11/POJK.03/2022 mewajibkan bank menyediakan sistem yang aman, namun perlindungan tersebut akan lumpuh jika pengguna memberikan akses melalui manipulasi psikologis.

Gambar 2 Penilaian Skor Evaluasi Program Mitigasi

Keberhasilan program ini juga tercermin dari peningkatan skor evaluasi akhir yang mencapai rata-rata 90 poin. Dampak jangka pendek yang terlihat adalah terbentuknya komunitas kecil di kalangan siswa yang saling mengingatkan jika terdapat informasi mencurigakan di grup pesan sekolah. Secara teoritis, keberhasilan mitigasi *social engineering* sangat bergantung pada "kekuatan mental" pengguna dalam menghadapi tekanan psikologis pelaku kejahatan (Krombholz et al., 2015). Pengabdian ini telah memberikan "vaksin digital" bagi siswa SMA di Kota Tangerang, menjadikan mereka sebagai pengguna yang tidak hanya kompeten secara transaksional, tetapi juga memiliki ketahanan (*resilience*) terhadap serangan siber di masa depan.

4. KESIMPULAN

Kegiatan pengabdian kepada masyarakat ini menyimpulkan bahwa tingkat kerentanan siswa SMA di Kota Tangerang terhadap kejahatan *social engineering* awalnya cukup tinggi akibat kesenjangan antara kemahiran menggunakan aplikasi (*user proficiency*) dengan pemahaman protokol keamanan (*security literacy*). Namun, melalui metode edukasi preventif berbasis simulasi dan *expert-sharing* dari perspektif

praktisi IT perbankan, terdapat peningkatan signifikan dalam kemampuan siswa mendeteksi dan memitigasi risiko serangan siber. Siswa kini mampu mengidentifikasi anomali komunikasi digital dan secara teknis telah mengimplementasikan perlindungan identitas berlapis pada perangkat mereka. Penguatan aspek psikologis dan teknis ini menjadi kunci utama dalam membangun ketahanan digital nasabah masa depan di ekosistem perbankan Indonesia.

Berdasarkan hasil pengabdian, disarankan bagi institusi pendidikan untuk menjalin kolaborasi berkelanjutan dengan praktisi industri teknologi informasi guna memberikan wawasan mengenai tren ancaman siber yang terus berevolusi. Bagi industri perbankan, sosialisasi mengenai keamanan transaksi digital perlu dilakukan secara lebih masif dan menyasar segmen remaja dengan pendekatan yang interaktif. Selain itu, untuk kegiatan pengabdian selanjutnya, disarankan untuk memperluas jangkauan edukasi hingga ke lingkungan wali murid, mengingat keamanan finansial digital dalam keluarga sering kali saling terhubung melalui perangkat yang digunakan bersama.

UCAPAN TERIMAKASIH

Penulis menyampaikan terima kasih yang sebesar-besarnya kepada perguruan tinggi asal atas dukungan hibah pengabdian masyarakat tahun 2026 yang memungkinkan transfer pengetahuan industri ini terlaksana. Penghargaan setinggi-tingginya diberikan kepada pimpinan SMA di Kota Tangerang yang telah memfasilitasi laboratorium dan koordinasi siswa selama kegiatan berlangsung. Secara khusus, penulis berterima kasih kepada rekan-rekan praktisi IT perbankan atas diskusi dan data anonim terkait tren *fraud* yang memperkaya materi pelatihan ini. Terakhir, terima kasih kepada para siswa peserta yang telah berpartisipasi aktif dalam upaya memperkuat keamanan ekosistem digital nasional.

5. DAFTAR RUJUKAN

Bers, M. U. (2020). *Coding as a Playground: Programming and Computational Thinking in the Early Childhood Classroom* (2nd ed.). Routledge. https://doi.org/10.4324/9781003022602

Brennan, K., & Resnick, M. (2012). New frameworks for studying and assessing the development of computational thinking. *Proceedings of the 2012 Annual Meeting of the American Educational Research Association*, 1, 1–25.

Grover, S., & Pea, R. (2013). Computational thinking in K–12: A review of the state of the field. *Educational Researcher*, 42(1), 38–43. https://doi.org/10.3102/0013189X12463051

Hasanah, U., & Sugiarto, S. (2020). Pengembangan berpikir komputasional dalam pembelajaran matematika di sekolah menengah atas. *Jurnal Elemen*, 6(1), 112–125.

Kurniawati, L., & Prasetyo, H. (2021). Efektivitas penggunaan aplikasi Scratch dalam meningkatkan kemampuan logika algoritma siswa. *Jurnal Pendidikan Teknologi dan Kejuruan*, 18(2), 201–210.

Lye, S. Y., & Koh, J. H. L. (2014). Review on teaching and learning of computational thinking through programming: What is next for K-12?. *Computers in Human Behavior*, 41, 51–61. https://doi.org/10.1016/j.chb.2014.09.012

Moreno-León, J., Robles, G., & Román-González, M. (2015). Dr. Scratch: Automatic analysis of Scratch projects to assess and foster computational thinking.

e-ISSN: 2963-8771
DOI: 10.57254/eka.v4i3.152

Proceedings of the Workshop on Primary and Secondary Computing Education, 132–133.

Papert, S. (1980). *Mindstorms: Children, Computers, and Powerful Ideas*. Basic Books.

Purnomo, A., & Munir, M. (2022). Strategi pengajaran computational thinking pada kurikulum merdeka di tingkat sekolah menengah. *Jurnal Informatika Pendidikan*, 5(3), 342–355.

Resnick, M., Maloney, J., Monroy-Hernández, A., Rusk, N., Eastmond, E., Brennan, K., Millner, A., Rosenbaum, E., Silver, J., Silverman, B., & Kafai, Y. (2009). Scratch: Programming for all. *Communications of the ACM*, 52(11), 60–67. https://doi.org/10.1145/1592761.1592779

Román-González, M., Pérez-González, J. C., & Jiménez-Fernández, C. (2017). Which cognitive abilities underlie computational thinking? Criterion validity of the Computational Thinking Test. *Computers in Human Behavior*, 72, 678–691. https://doi.org/10.1016/j.chb.2016.08.047

Selby, C., & Woollard, J. (2013). *Computational thinking: The developing definition*. University of Southampton (E-prints).

Shute, V. J., Sun, C., & Asbell-Clarke, J. (2017). Demystifying computational thinking. *Educational Research Review*, 22, 142–158. https://doi.org/10.1016/j.edurev.2017.09.003

Wahyuni, S. (2021). *Metodologi Pembelajaran Informatika: Mengasah Berpikir Komputasional Siswa*. Penerbit Informatika.

Wing, J. M. (2006). Computational thinking. *Communications of the ACM*, 49(3), 33–35. https://doi.org/10.1145/1118178.1118215