p-ISSN 2828-0563
e-ISSN 2828-0431

Jurnal Ilmiah Pengabdian kepada Masyarakat
JIPAM
Vol. 4, No. 1 September-Desember, 2024 hal. 1-120
Journal Page is available to https://jipam.stai-dq.org/index.php/home

Edukasi Literasi Keamanan Data Pribadi dan Mitigasi Social Engineering bagi Siswa SMAN 7 Kecamatan Cikokol Kota Tangerang

Try Setyo Slamet[1], Annisa Tsamratul'ain[2]
[1,2]Universitas Salakanagara
Email: trysetyoslamet@unsaka.ac.id[1]

ABSTRAK

Pesatnya transformasi digital di wilayah urban seperti Kota Tangerang meningkatkan risiko kejahatan siber, terutama teknik rekayasa sosial (*social engineering*) yang menyasar kelompok remaja. Siswa SMAN 7 Tangerang merupakan pengguna aktif media sosial namun sering kali memiliki literasi keamanan data pribadi yang rendah. Kegiatan Pengabdian Kepada Masyarakat (PKM) ini bertujuan untuk meningkatkan kesadaran dan kemampuan mitigasi siswa terhadap ancaman manipulasi psikologis di dunia maya. Metode pelaksanaan dilakukan melalui lokakarya interaktif yang meliputi tahap identifikasi, edukasi berbasis simulasi serangan *phishing*, dan evaluasi menggunakan *pre-test* serta *post-test*. Hasil kegiatan menunjukkan peningkatan pemahaman siswa yang signifikan, dengan skor rata-rata identifikasi serangan meningkat sebesar 52% setelah pelatihan. Siswa kini mampu mengimplementasikan langkah proteksi praktis seperti pengaktifan *Two-Factor Authentication* (2FA) dan mengenali pola komunikasi mencurigakan. Program ini membuktikan bahwa edukasi berbasis perilaku efektif dalam membentuk budaya sadar siber di lingkungan sekolah untuk meminimalkan risiko pencurian data pribadi.

Kata Kunci: Keamanan Data Pribadi, *Social Engineering*, Literasi Digital, Siswa SMA, Kota Tangerang.

ABSTRATC

The rapid digital transformation in urban areas like Tangerang City has increased the risk of cybercrime, particularly social engineering techniques targeting adolescents. Students at SMAN 7 Tangerang are active social media users but often possess low personal data security literacy. This Community Service (PKM) activity aims to enhance students' awareness and mitigation capabilities against psychological manipulation threats in cyberspace. The implementation method involved interactive workshops including identification stages, education based on phishing attack simulations, and evaluation using pre-tests and post-tests. The results indicated a significant increase in student understanding, with the average attack identification score rising by 52% following the training. Students are now able to implement practical protection steps, such as enabling Two-Factor Authentication (2FA) and recognizing suspicious communication patterns. This program proves that behavior-based education is effective in fostering a cyber-aware culture within the school environment to minimize the risk of personal data theft.

Keywords: Personal Data Security, Social Engineering, Digital Literacy, High School Students, Tangerang City.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di Indonesia telah membawa perubahan signifikan dalam pola interaksi sosial, terutama dengan meningkatnya penetrasi internet yang menyentuh berbagai lapisan masyarakat. Transformasi digital ini tidak hanya menawarkan kemudahan akses informasi, tetapi juga memunculkan risiko baru terkait keamanan data digital yang semakin kompleks (Kementerian Komunikasi dan Informatika RI, 2024). Di

DOI Artikel: doi.org/10.55883/jipam.v4i1.142

wilayah urban seperti Kota Tangerang, ketergantungan masyarakat terhadap platform digital untuk aktivitas sehari-hari menjadikannya wilayah yang sangat dinamis namun rentan terhadap ancaman siber (BPS Kota Tangerang, 2025).

Di tengah masifnya penggunaan internet, isu perlindungan data pribadi menjadi perhatian utama seiring dengan disahkannya regulasi kuat seperti UU PDP. Namun, pemahaman masyarakat mengenai hak-hak privasi dan cara melindungi identitas digital masih tergolong rendah, sehingga menciptakan celah bagi penyalahgunaan data (Lubis & Kartiwi, 2021). Literasi keamanan siber yang mumpuni menjadi fondasi krusial agar individu mampu menyaring informasi dan mengamankan aset digital mereka dari pihak yang tidak bertanggung jawab (Aini et al., 2022).

Salah satu ancaman yang paling dominan dan sulit dideteksi secara teknis adalah *social engineering* atau rekayasa sosial, yang memanfaatkan manipulasi psikologis manusia untuk mendapatkan akses informasi rahasia. Teknik ini tidak menyerang sistem perangkat lunak secara langsung, melainkan mengeksploitasi kepercayaan, rasa takut, atau rasa ingin tahu korbannya (Mouton et al., 2023). Dalam konteks ini, manusia sering kali dianggap sebagai mata rantai terlemah dalam sistem keamanan informasi, sehingga pendekatan berbasis perilaku menjadi sangat relevan untuk diimplementasikan (Widjaja & Kusuma, 2022).

Generasi remaja, khususnya siswa sekolah menengah atas, merupakan kelompok yang paling rentan terhadap serangan rekayasa sosial karena tingginya intensitas penggunaan media sosial yang tidak dibarengi dengan kewaspadaan yang cukup. Mereka cenderung memiliki perilaku berbagi informasi (*information sharing*) yang berlebihan tanpa menyadari risiko privasi yang mengintai di balik setiap unggahan (Nasution & Siregar, 2022). Kerentanan ini semakin diperparah oleh tren serangan *phishing* yang kini banyak menyasar platform yang populer di kalangan anak muda (Safitri & Rahman, 2024).

SMAN 7 Kota Tangerang yang berlokasi di Kecamatan Cikokol merupakan salah satu institusi pendidikan dengan profil siswa yang sangat aktif secara digital. Lokasinya yang strategis di pusat kota membuat siswa di sekolah ini memiliki aksesibilitas tinggi terhadap perangkat teknologi, namun sering kali mereka terjebak dalam zona nyaman digital tanpa menyadari bahaya manipulasi psikologis (Darmawan & Setiawan, 2023). Minimnya program edukasi formal mengenai mitigasi rekayasa sosial di tingkat sekolah menjadi alasan mendasar diperlukannya intervensi dari pakar akademisi bidang Sistem Informasi.

Melalui program pengabdian kepada masyarakat ini, tim dosen berupaya memberikan solusi nyata melalui edukasi literasi keamanan data pribadi yang bersifat preventif. Fokus utama kegiatan ini adalah membekali siswa dengan kemampuan mengenali pola-pola manipulasi psikologis dan teknik mitigasi praktis untuk melindungi akun digital mereka (Indriyatno & Prasetyo, 2024). Penggunaan metode ceramah yang dikombinasikan dengan demonstrasi simulasi serangan dianggap sebagai cara efektif untuk meningkatkan retensi pemahaman siswa terhadap materi yang diberikan (Purwanto & Sudargini, 2021).

Berdasarkan latar belakang tersebut, kegiatan PKM ini diharapkan dapat menciptakan budaya sadar siber di lingkungan SMAN 7 Kota Tangerang. Dengan meningkatnya literasi digital siswa, mereka diharapkan mampu menjadi garda

p-ISSN 2828-0563
e-ISSN 2828-0431

terdepan dalam melindungi data pribadi masing-masing serta mampu menyebarkan pengetahuan tersebut di lingkungan keluarga dan teman sebaya (Hadlow et al., 2022). Secara jangka panjang, edukasi ini merupakan langkah strategis dalam membangun ekosistem digital yang aman dan bertanggung jawab di Kota Tangerang.

Metode Pelaksanaan PKM

Metode pelaksanaan kegiatan pengabdian kepada masyarakat ini menggunakan pendekatan *Human-Centric Cyber Security* yang mengombinasikan transfer pengetahuan teoritis dengan simulasi praktis. Kegiatan dilaksanakan di SMAN 7 Kecamatan Cikokol, Kota Tangerang, dengan melibatkan siswa sebagai subjek utama. Tahapan pelaksanaan dibagi menjadi empat fase utama sebagai berikut:

1. Tahap Identifikasi dan Observasi (Pre-Project)

Pada tahap awal, tim melakukan survei pendahuluan untuk memetakan perilaku digital siswa di SMAN 7 Tangerang. Instrumen berupa kuesioner *pre-test* disebarkan untuk mengukur tingkat literasi awal mengenai perlindungan data pribadi dan mengenali jenis media sosial yang paling sering digunakan. Hasil observasi ini digunakan untuk menyesuaikan modul edukasi agar relevan dengan tren serangan siber yang sedang marak di kalangan remaja urban (Darmawan & Setiawan, 2023).

2. Tahap Perancangan Materi dan Modul

Berdasarkan hasil identifikasi, tim menyusun modul pelatihan yang berfokus pada dua aspek utama:

a. Literasi Data Pribadi: Edukasi mengenai jenis data sensitif, hak subjek data berdasarkan UU PDP, dan pengaturan privasi pada perangkat *smartphone*.
b. Mitigasi Social Engineering: Pengenalan pola *phishing*, *baiting*, dan *pretexting* melalui studi kasus nyata.

Materi disusun menggunakan media visual interaktif untuk memastikan pesan tersampaikan dengan efektif kepada Generasi Z (Purwanto & Sudargini, 2021).

3. Tahap Sosialisasi dan Edukasi (Workshop)

Pelaksanaan kegiatan dilakukan melalui metode lokakarya (*workshop*) tatap muka yang terdiri dari dua sesi:

a. Sesi Teoretis: Penyampaian materi mengenai pentingnya keamanan informasi dan bagaimana rekayasa sosial bekerja memanipulasi psikologi pengguna (Raharjo, 2022).
b. Sesi Praktis/Simulasi: Demonstrasi langsung cara membedakan URL asli dan palsu, pengecekan keamanan akun melalui *two-factor authentication* (2FA), serta simulasi deteksi pesan singkat (SMS/WhatsApp) yang mengandung unsur penipuan.

4. Tahap Evaluasi dan Keberlanjutan

Untuk mengukur keberhasilan program, dilakukan evaluasi melalui beberapa instrumen:

a. Post-Test: Mengukur peningkatan skor pemahaman siswa setelah menerima materi dibandingkan dengan skor *pre-test*.
b. Simulasi Uji Petik: Memberikan tantangan instan kepada siswa untuk mengidentifikasi sebuah skenario serangan rekayasa sosial secara *real-time*.
c. Penyusunan Laporan: Data yang diperoleh dianalisis secara deskriptif untuk melihat efektivitas metode edukasi yang diberikan (Indriyatno & Prasetyo, 2024).

DOI Artikel: doi.org/10.55883/jipam.v4i1.142

Tabel 1. Kerangka Kerja Pelaksanaan PKM

Tahapan	Aktivitas Utama	Output
Persiapan	Koordinasi dengan pihak SMAN 7 Tangerang & Perizinan	Jadwal Pelaksanaan & Izin
Diagnosa	Penyebaran kuesioner literasi digital awal	Data Profil Literasi Siswa
Edukasi	Workshop Literasi Keamanan Data & Mitigasi *Social Engineering*	Peningkatan *Awareness*
Simulasi	Praktik pengamanan akun dan deteksi *phishing*	Keterampilan Teknis Dasar
Evaluasi	Pengisian kuesioner akhir dan analisis hasil	Laporan Publikasi & Sertifikat

Hasil Kegiatan

1. Profil Literasi Digital Siswa SMAN 7 Tangerang

Berdasarkan hasil kuesioner awal (*pre-test*) terhadap 60 responden siswa SMAN 7 Tangerang, ditemukan bahwa 95% siswa memiliki setidaknya tiga akun media sosial aktif (Instagram, TikTok, dan WhatsApp). Namun, hanya 12% dari mereka yang memahami konsep dasar perlindungan data pribadi sesuai dengan regulasi yang berlaku di Indonesia. Sebagian besar siswa cenderung memberikan izin akses aplikasi (*app permissions*) secara otomatis tanpa membaca syarat dan ketentuan, yang merupakan celah utama dalam keamanan data (Lubis & Kartiwi, 2021).

2. Peningkatan Pemahaman Melalui Edukasi Interaktif

Pelaksanaan edukasi dilakukan dengan membedah anatomi serangan rekayasa sosial. Hasil evaluasi menunjukkan adanya peningkatan pemahaman yang signifikan antara sebelum dan sesudah kegiatan.

Tabel 2. Perbandingan Skor Pre-Test dan Post-Test Siswa

Indikator Penilaian	Pre-Test (Rata-rata %)	Post-Test (Rata-rata %)	Peningkatan (%)
Pemahaman Jenis Data Pribadi	45%	88%	43%
Identifikasi Teknik *Phishing*	30%	82%	52%
Kesadaran *Social Engineering*	25%	75%	50%
Praktik Keamanan (2FA/Password)	40%	90%	50%

Data pada Tabel 2 menunjukkan bahwa peningkatan tertinggi terjadi pada indikator Identifikasi Teknik Phishing sebesar 52%. Hal ini membuktikan bahwa metode demonstrasi visual lebih efektif dalam memberikan gambaran nyata mengenai ancaman digital dibandingkan

p-ISSN 2828-0563
e-ISSN 2828-0431

sekadar pemaparan teori (Purwanto & Sudargini, 2021).

3. Analisis Mitigasi *Social Engineering*

Dalam sesi diskusi, ditemukan bahwa mayoritas siswa pernah menerima pesan berisi tautan mencurigakan atau pengumuman hadiah palsu melalui WhatsApp. Melalui simulasi yang diberikan, siswa diajarkan untuk melakukan *cross-check* terhadap pengirim pesan dan menghindari respons emosional yang mendesak (*sense of urgency*)—sebuah taktik umum dalam rekayasa sosial (Mouton et al., 2023).

Gambar 1. Sesi Diskusi

Diskusi mendalam juga mengungkap bahwa kerentanan siswa di SMAN 7 Tangerang dipengaruhi oleh tren "ikut-ikutan" fitur media sosial, seperti fitur *Add Yours* di Instagram yang sering kali secara tidak sadar memancing pengguna membagikan data privasi (nama ibu kandung, tanggal lahir, atau alamat). Tim PKM menekankan bahwa perlindungan data bukan sekadar masalah teknis (seperti enkripsi), melainkan masalah perilaku dan kewaspadaan individu (Widjaja & Kusuma, 2022).

4. Respon dan Keberlanjutan Program

Siswa menunjukkan antusiasme tinggi saat sesi praktik pengamanan akun menggunakan *Two-Factor Authentication* (2FA). Banyak siswa yang langsung mengaktifkan fitur tersebut pada akun Google dan media sosial mereka selama sesi berlangsung. Hal ini menunjukkan bahwa edukasi yang diberikan tidak hanya berhenti pada level kognitif, tetapi mencapai level perubahan perilaku siber (*cyber behavior*) (Darmawan & Setiawan, 2023).

Pihak sekolah SMAN 7 Tangerang juga memberikan respon positif dan menyatakan perlunya integrasi materi keamanan siber ini ke dalam kegiatan ekstrakurikuler atau mata pelajaran informatika. Sinergi antara akademisi dan institusi pendidikan menengah di Kota Tangerang sangat krusial untuk meminimalkan angka korban kejahatan siber di kalangan remaja yang terus meningkat (Safitri & Rahman, 2024).

Kesimpulan

Kegiatan pengabdian kepada masyarakat yang dilaksanakan di SMAN 7 Kecamatan Cikokol, Kota Tangerang, telah berhasil meningkatkan kesadaran dan keterampilan siswa dalam menghadapi ancaman digital. Berdasarkan hasil evaluasi, terdapat peningkatan literasi keamanan data pribadi yang signifikan, di mana skor pemahaman rata-rata siswa meningkat dari kategori "Rendah" menjadi "Sangat Baik" setelah diberikan edukasi.

Siswa kini mampu mengidentifikasi berbagai teknik manipulasi psikologis dalam

DOI Artikel: doi.org/10.55883/jipam.v4i1.142

social engineering, seperti *phishing* dan penipuan berbasis media sosial, serta memahami pentingnya perlindungan data pribadi sesuai amanat UU PDP. Kesimpulan utama dari kegiatan ini adalah bahwa pendekatan edukasi yang bersifat interaktif dan berbasis simulasi sangat efektif dalam mengubah perilaku digital remaja dari yang sebelumnya permisif terhadap akses data menjadi lebih waspada dan protektif.

Saran

Berdasarkan pelaksanaan kegiatan ini, tim pengabdi memberikan beberapa saran untuk pengembangan ke depan:

1. Bagi Pihak Sekolah: Diharapkan SMAN 7 Tangerang dapat menginisiasi "Duta Literasi Digital" di lingkungan siswa untuk memastikan penyebaran informasi mengenai keamanan siber dilakukan secara berkelanjutan di kalangan teman sebaya.
2. Bagi Siswa: Disarankan untuk melakukan pembaharuan kata sandi secara berkala dan tetap mengaktifkan fitur autentikasi dua faktor (2FA) pada seluruh platform digital yang digunakan.
3. Bagi Pengabdian Selanjutnya: Perlu dilakukan kegiatan serupa dengan materi yang lebih spesifik, seperti aspek hukum pidana siber atau teknis keamanan data pada transaksi keuangan digital (*fintech*), mengingat tingginya penggunaan dompet digital di kalangan pelajar Kota Tangerang.

References

Aini, Q., Rahardja, U., & Tangmanee, C. (2022). Pengaruh literasi digital terhadap keamanan data pribadi pengguna media sosial di kalangan remaja. *Journal of Informatics and Business*, 10(2), 145–158.

Anderson, C. L., & Agarwal, R. (2021). The role of digital literacy in mitigating social engineering threats: A behavioral study of high school students. *Journal of Cybersecurity Education, Research and Practice*, 2021(1), 12–30.

BPS Kota Tangerang. (2025). *Kota Tangerang dalam angka 2025: Statistik teknologi informasi dan komunikasi*. Badan Pusat Statistik Kota Tangerang.

Darmawan, A., & Setiawan, H. (2023). Strategi edukasi keamanan siber bagi generasi Z di lingkungan sekolah menengah atas. *Jurnal Pengabdian Kepada Masyarakat (JPKM)*, 9(3), 210–222.

Hadlow, J. J., Kritzinger, E., & Loock, M. (2022). Framework for cyber-safety awareness for school learners in developing countries. *International Journal of Information and Communication Technology Education (IJICTE)*, 18(1), 1–15.

Indriyatno, H., & Prasetyo, A. (2024). Peningkatan kesadaran keamanan informasi melalui simulasi serangan social engineering. *Jurnal Sistem Informasi dan Edukasi*, 11(1), 45–56.

Kementerian Komunikasi dan Informatika RI. (2024). *Laporan tahunan literasi digital Indonesia: Segmen pendidikan dan tantangan keamanan data*. Kominfo.

Lubis, M., & Kartiwi, M. (2021). Privacy and personal data protection in Indonesia: The role of literacy and legal framework. *Procedia Computer Science*, 197, 603–610.

Mouton, F., Leenen, L., & Venter, H. S. (2023). Social engineering attack examples, templates and scenarios. *Computers & Security*, 115, 102–118.

Nasution, M. K., & Siregar, R. (2022). Analisis perilaku berbagi informasi (Information Sharing) dan risiko privasi pada siswa SMA di wilayah urban. *Jurnal Ilmu Komunikasi*, 14(2), 88–104.

Purwanto, A., & Sudargini, Y. (2021). Penggunaan metode ceramah dan

p-ISSN 2828-0563
e-ISSN 2828-0431

demonstrasi dalam meningkatkan pemahaman cyber security bagi siswa. *Journal of Education and Teaching (JET)*, 2(4), 312–325.

Raharjo, B. (2022). *Keamanan sistem informasi: Mengenal ancaman social engineering di era digital*. PT Elex Media Komputindo.

Ramadhani, S., & Fitriani, D. (2023). Edukasi perlindungan data pribadi berbasis UU PDP bagi masyarakat sekolah di Tangerang. *Jurnal Pengabdian Masyarakat Teknik*, 5(2), 177–189.

Safitri, N., & Rahman, A. (2024). Dampak paparan media sosial terhadap kerentanan serangan phising pada remaja. *Indonesian Journal of Cyber Security*, 7(1), 22–35.

Widjaja, S., & Kusuma, W. (2022). Pendekatan human-centric dalam mitigasi social engineering di institusi pendidikan. *Jurnal Teknologi dan Sistem Komputer*, 10(4), 267–275.