JCoos: Journal of Community Outreach in Science & Society

Volume 01 Issue 01 Year 2026 | Page 43-54 | e-ISSN: xxxx-xxxx

Peningkatan Kesadaran Keamanan Siber melalui Edukasi Phishing dan Penipuan Digital bagi Siswa di Pekanbaru

Gunadi[1], Muhammad Jamaris[2], Susanti[3], Dewi Sari Wahyuni[4], T.Sy Eiva Fatdha[5]

[1,2,3,4,5] Universitas Sains dan Teknologi Indonesia

***Correspondence**: gunadi@usti.ac.id

Abstract

The rapid advancement of digital technology has significantly enhanced convenience in daily activities. However, it has also increased the risk of cybercrime, particularly phishing and digital fraud. Students, as active users of the internet and social media, constitute a vulnerable group due to their limited awareness and understanding of cybersecurity practices. This community service initiative was designed to improve students' awareness and knowledge of phishing threats, various forms of digital fraud, and effective preventive measures applicable in everyday contexts. The program was implemented through interactive outreach sessions, structured presentations, demonstrations of phishing case studies, guided discussions, and evaluations using pre-tests and post-tests to assess participants' learning outcomes. The activity was held at a school in Pekanbaru City, with lecturers and university students serving as facilitators. The findings demonstrated a notable improvement in participants' ability to recognize suspicious messages or links, understand the importance of safeguarding personal data, use strong passwords, implement two-factor authentication, and respond appropriately to potential digital fraud. Furthermore, participants exhibited high engagement during discussion sessions and were able to identify various forms of cybercrime commonly encountered in digital environments. This initiative is expected to strengthen digital literacy and enhance students' preparedness to address cybersecurity challenges in the era of digital transformation.

Keywords **:** *Cybersecurity***,** *Phishing***,** *Digital Fraud***,** *Digital Literacy***,** *Education*

Abstrak

Perkembangan teknologi digital yang semakin pesat memberikan berbagai kemudahan dalam aktivitas sehari-hari, namun di sisi lain juga meningkatkan risiko kejahatan siber, khususnya melalui praktik phishing *dan penipuan digital. Siswa sebagai pengguna aktif internet dan media sosial merupakan kelompok yang rentan menjadi korban akibat masih terbatasnya pemahaman mengenai keamanan siber. Kegiatan pengabdian kepada masyarakat ini bertujuan untuk meningkatkan kesadaran dan pengetahuan siswa mengenai ancaman* phishing,

berbagai bentuk penipuan digital, serta langkah-langkah pencegahan yang dapat dilakukan dalam kehidupan sehari-hari. Metode pelaksanaan kegiatan meliputi penyuluhan interaktif, penyampaian materi menggunakan media presentasi, demonstrasi contoh kasus phishing*, diskusi, serta evaluasi melalui pre-test dan post-test untuk mengukur peningkatan pemahaman peserta. Kegiatan dilaksanakan pada siswa di salah satu sekolah di Kota Pekanbaru dengan melibatkan dosen dan mahasiswa sebagai fasilitator. Hasil kegiatan menunjukkan adanya peningkatan pemahaman peserta mengenai karakteristik pesan atau tautan mencurigakan, pentingnya menjaga kerahasiaan data pribadi, penggunaan kata sandi yang kuat, autentikasi dua faktor, serta langkah yang harus dilakukan apabila menemukan indikasi penipuan digital. Selain itu, peserta menunjukkan antusiasme tinggi selama sesi diskusi dan mampu mengidentifikasi berbagai modus kejahatan siber yang sering terjadi di lingkungan digital. Kegiatan ini diharapkan dapat membentuk budaya literasi digital yang lebih baik serta meningkatkan kesiapsiagaan siswa dalam menghadapi ancaman keamanan siber di era transformasi digital.*

Kata Kunci: *keamanan siber, phishing, penipuan digital, literasi digital, edukasi*

Received: 05-05-2026 | Revised: 15-05-2026 | Accepted: 30-05-2026

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital di berbagai sektor, termasuk bidang pendidikan. Pemanfaatan internet, perangkat bergerak (mobile devices), media sosial, dan berbagai platform pembelajaran digital telah menjadi bagian dari aktivitas belajar siswa sehari-hari. Teknologi digital memberikan kemudahan dalam memperoleh informasi, meningkatkan efektivitas komunikasi, serta mendukung proses pembelajaran yang lebih fleksibel dan interaktif. Namun, pesatnya digitalisasi juga diikuti oleh meningkatnya berbagai ancaman keamanan siber (cybersecurity), khususnya serangan phishing dan berbagai bentuk penipuan digital yang menargetkan pengguna internet dengan tingkat literasi keamanan yang masih rendah (Hidayat & Wahid, 2025).

Phishing merupakan salah satu bentuk serangan social engineering yang memanfaatkan manipulasi psikologis untuk memperoleh informasi sensitif, seperti nama pengguna, kata sandi, kode OTP, maupun data keuangan korban melalui email, pesan singkat, media sosial, atau situs web palsu. Berbeda dengan serangan yang mengeksploitasi kelemahan perangkat lunak, phishing lebih menitikberatkan pada kelemahan perilaku manusia (human factor). Oleh karena itu, rendahnya kesadaran pengguna terhadap keamanan digital menjadi salah satu faktor utama yang menyebabkan tingginya keberhasilan serangan siber. Edukasi yang berkelanjutan, simulasi kasus, serta pelatihan keamanan siber terbukti mampu meningkatkan kemampuan pengguna dalam mengenali dan menghindari berbagai modus phishing (Prümmer et al., 2024; Daengsi et al., 2021).

Siswa sekolah menengah merupakan salah satu kelompok yang paling aktif memanfaatkan internet. Selain digunakan sebagai media pembelajaran, internet juga dimanfaatkan untuk mengakses media sosial, permainan daring, layanan komunikasi, hingga transaksi digital. Tingginya intensitas penggunaan teknologi tersebut belum sepenuhnya diimbangi dengan kemampuan dalam mengenali ancaman keamanan siber. Berbagai penelitian menunjukkan bahwa siswa masih rentan menjadi korban phishing, pencurian akun media sosial, penyalahgunaan data pribadi, penipuan berbasis tautan (malicious link), maupun berbagai bentuk rekayasa sosial (social engineering) akibat rendahnya literasi keamanan digital (Das et al., 2019; Mutlutürk, 2024; Tangka & Putra, 2025).

Berbagai kegiatan edukasi keamanan siber yang telah dilakukan menunjukkan hasil yang positif dalam meningkatkan pemahaman peserta mengenai perlindungan data pribadi, pengelolaan kata sandi yang aman, autentikasi dua faktor (two-factor authentication), serta kemampuan mengenali karakteristik pesan phishing. Hidayat dan Wahid (2025) melaporkan bahwa kegiatan edukasi yang dipadukan dengan simulasi kasus phishing berhasil meningkatkan kemampuan siswa dalam mengidentifikasi indikator-indikator serangan phishing hingga lebih dari 75%. Temuan tersebut menunjukkan bahwa pendekatan edukatif yang bersifat interaktif lebih efektif dibandingkan penyampaian materi secara konvensional.

Selain itu, berbagai kajian sistematis mengenai pelatihan keamanan siber juga menyimpulkan bahwa peningkatan cybersecurity awareness merupakan salah satu strategi yang paling efektif dalam mengurangi risiko keberhasilan serangan berbasis manusia. Program pelatihan yang memadukan penyuluhan, simulasi, studi kasus, dan evaluasi secara berkala mampu membentuk perubahan perilaku pengguna sehingga lebih waspada terhadap berbagai bentuk ancaman digital (Prümmer et al., 2024). Berdasarkan hasil observasi awal yang dilakukan pada salah satu sekolah di Kota Pekanbaru, diketahui bahwa sebagian besar siswa telah memiliki telepon pintar dan aktif menggunakan internet dalam aktivitas belajar maupun komunikasi sehari-hari. Meskipun demikian, masih ditemukan beberapa permasalahan, seperti rendahnya kemampuan siswa dalam membedakan tautan asli dan tautan palsu, kurangnya pemahaman mengenai bahaya membagikan kode OTP, penggunaan kata sandi yang sederhana dan sama pada beberapa akun, serta minimnya pengetahuan mengenai langkah-langkah pencegahan penipuan digital. Kondisi tersebut menunjukkan bahwa literasi keamanan siber di kalangan siswa masih perlu ditingkatkan agar mereka mampu memanfaatkan teknologi digital secara lebih aman dan bertanggung jawab.

Berdasarkan permasalahan tersebut, diperlukan suatu kegiatan pengabdian kepada masyarakat berupa edukasi keamanan siber yang berfokus pada pengenalan phishing dan penipuan digital melalui metode penyuluhan interaktif, demonstrasi kasus, diskusi, serta evaluasi menggunakan pre-test dan post-test. Kegiatan ini diharapkan dapat meningkatkan pengetahuan, kesadaran, serta perilaku siswa dalam mengenali berbagai bentuk ancaman keamanan siber sehingga mampu meminimalkan risiko menjadi korban kejahatan digital. Oleh karena itu, tujuan kegiatan pengabdian kepada masyarakat ini adalah meningkatkan kesadaran keamanan siber melalui edukasi phishing dan penipuan digital

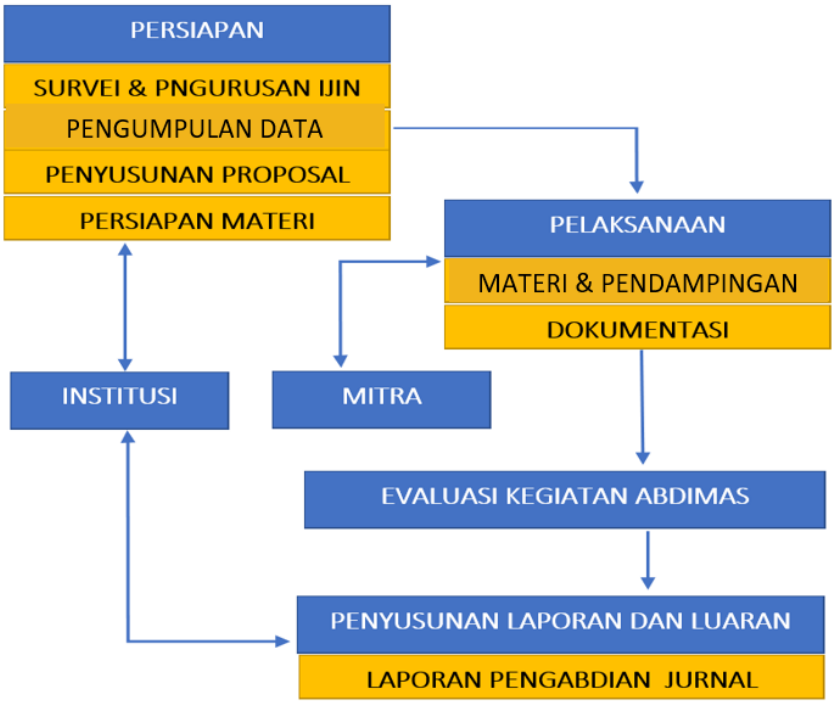
bagi siswa di Pekanbaru. Luaran yang diharapkan adalah meningkatnya literasi keamanan siber, kemampuan mengidentifikasi modus phishing, serta terbentuknya perilaku penggunaan teknologi digital yang lebih aman dalam kehidupan sehari-hari.

2. Metode

Pada bagian metodologi pelaksanaan kegiatan pengabdian kepada masyarakat dilakukan melalui beberapa tahapan, yaitu:

A. Mekanisme Pelaksanaan Kegiatan

Mekanisme pelaksanaan kegiatan abdimas dilakukan melalui empat tahap/alur mekanisme. Alur pelaksanaan abdimas dapat dilihat pada Gambar di bawah ini:



Gambar 1. Mekanisme Kegiatan Pengabdian Kepada Masyarakat

Keterangan Gambar :

a) Persiapan

Tahap pertama adalah melakukan segala persiapan yang berkaitan dengan segala kebutuhan pelaksanaan kegiatan pengabdian kepada masyarakat yang meliputi survei lokasi dan koordinasi dengan pihak sekolah sebagai mitra, pengurusan izin pelaksanaan kegiatan, identifikasi kebutuhan peserta melalui pengumpulan data awal, penyusunan proposal kegiatan, serta persiapan materi edukasi mengenai keamanan siber, *phishing*, dan penipuan digital. Tahap persiapan dilakukan bekerja sama dengan institusi pelaksana dan pihak mitra untuk memastikan kegiatan sesuai dengan kebutuhan peserta dan dapat berjalan secara optimal. Perencanaan yang baik dan

koordinasi dengan pemangku kepentingan merupakan bagian penting dalam keberhasilan program pengabdian masyarakat.

b) Pelaksanaan

Tahap kedua adalah pelaksanaan kegiatan pengabdian yang meliputi penyampaian materi, simulasi, diskusi, dan dokumentasi seluruh rangkaian kegiatan agar pelatihan dapat berjalan secara efektif. Tim pengabdian menyampaikan materi melalui metode penyuluhan interaktif, demonstrasi contoh kasus *phishing*, simulasi identifikasi tautan atau pesan mencurigakan, diskusi, serta sesi tanya jawab. Seluruh rangkaian kegiatan didokumentasikan sebagai bukti pelaksanaan dan bahan evaluasi kegiatan. Pendekatan edukatif yang melibatkan partisipasi aktif peserta bertujuan untuk meningkatkan pemahaman siswa mengenai pentingnya menjaga keamanan data pribadi, mengenali berbagai modus penipuan digital, serta menerapkan praktik penggunaan internet yang aman.

Gambar 2. Kegiatan Pembukaan dan Perkenalan dari Tim Pengabdi

Gambar 3. Penyampaian Materi dari Tim Pengabdi

Gambar 4. Pendekatan Edukatif yang Melibatkan Partisipasi Peserta

c) Evaluasi Kegiatan
Pada Tahap ini yang dilakukan untuk mengukur ketercapaian tujuan pengabdian melalui analisis hasil *pre-test* dan *post-test*, observasi partisipasi peserta selama kegiatan, serta umpan balik dari siswa dan pihak sekolah. Hasil evaluasi digunakan sebagai dasar untuk mengetahui peningkatan pengetahuan dan kesadaran siswa terhadap ancaman *phishing* dan penipuan digital, sekaligus sebagai bahan perbaikan kegiatan pada pelaksanaan berikutnya. Evaluasi merupakan bagian penting dalam program pengabdian karena memberikan gambaran mengenai efektivitas pelaksanaan dan dampak kegiatan terhadap sasaran.

d) Penyusunan Laporan dan Luaran
Pada tahap keempat ini mencakup penyusunan laporan akhir kegiatan pengabdian, dokumentasi hasil pelaksanaan, publikasi artikel ilmiah pada jurnal pengabdian kepada masyarakat, serta penyusunan rekomendasi sebagai tindak lanjut bagi pihak sekolah dalam meningkatkan literasi keamanan siber siswa secara berkelanjutan. Luaran tersebut diharapkan dapat menjadi referensi bagi institusi pendidikan dalam mengembangkan program edukasi keamanan siber yang berkesinambungan.

B. Personil Pelaksanaan Kegiatan

Guna mendukung keberhasilan program pengabdian pada masyarakat (abdimas) kolaborasi ini melibatkan personil dari Universitas Sains dan Teknologi Indonesia. Susunan personil pengabdian pada masyarakat yang diusulkan ini terdiri atas Ketua Pelaksana 1 orang dan anggota pelaksana 4 orang dan 2 orang mahasiswa, dengan uraian:

1. Ketua pengabdi : Gunadi, M.Kom
2. Anggota pengabdi 1 : Muhammad Jamaris, M.Kom
3. Anggota pengabdi 2 : Susanti, M.IT
4. Anggota pengabdi 3 : Dr. Dewi Sari Wahyuni, M.Pd

5. Anggota pengabdi 4 : T. Sy. Eiva Fatdha, M.Kom

Gambar 5. Tim Pengabdi Universitas Sains dan Teknologi Indonesia

3. Hasil dan Pembahasan

3.1 Pelaksanaan Kegiatan

Kegiatan Pengabdian kepada Masyarakat dengan judul "Peningkatan Kesadaran Keamanan Siber melalui Edukasi Phishing dan Penipuan Digital bagi Siswa di Pekanbaru" dilaksanakan di salah satu sekolah menengah di Kota Pekanbaru dengan melibatkan 30 siswa sebagai peserta. Kegiatan diawali dengan registrasi peserta, dilanjutkan dengan pemberian pre-test untuk mengetahui tingkat pengetahuan awal mengenai keamanan siber.
Materi yang diberikan meliputi:

a) Konsep dasar keamanan siber (Cybersecurity)
b) Pengertian dan jenis-jenis phishing
c) Modus penipuan digital yang sering terjadi
d) Pentingnya menjaga data pribadi
e) Penggunaan password yang kuat
f) Two-Factor Authentication (2FA)
g) Cara mengenali website dan tautan palsu
h) Simulasi kasus phishing

Selama kegiatan berlangsung peserta terlihat aktif mengikuti penyampaian materi dan diskusi. Beberapa siswa menceritakan pengalaman menerima pesan hadiah palsu, tautan mencurigakan, maupun akun media sosial yang pernah diretas.

3.2 Hasil Pre-test dan Post-test

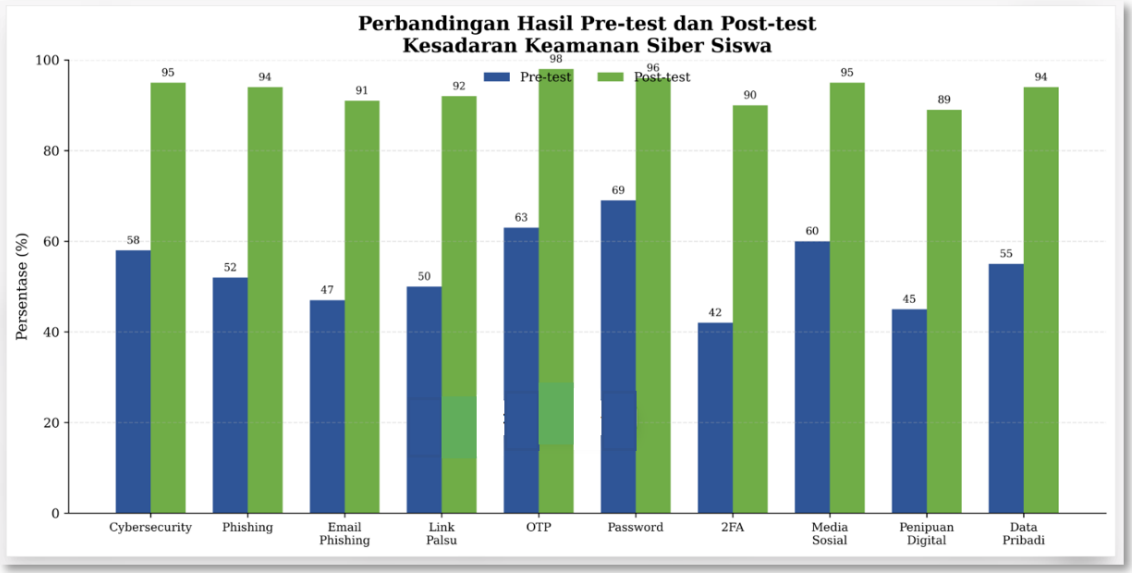
Untuk mengetahui efektivitas kegiatan dilakukan evaluasi menggunakan pre-test dan post-test yang terdiri dari 10 pertanyaan mengenai keamanan siber.

Tabel 1. Hasil Pre-test dan Post-test

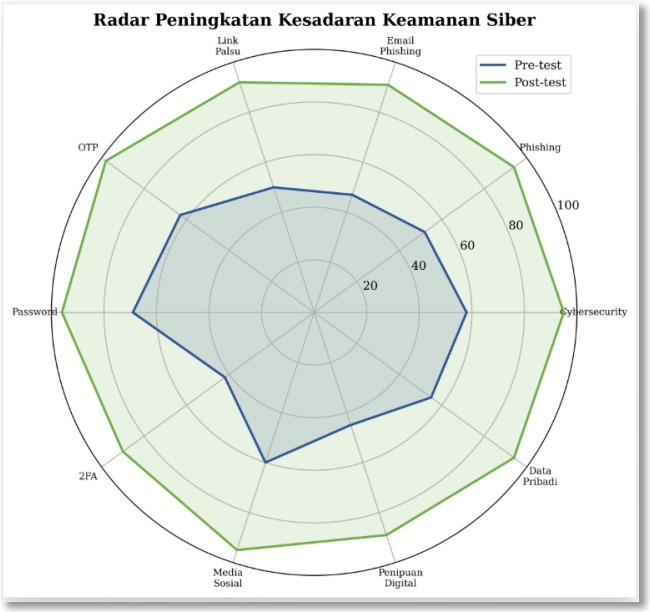
No	Indikator Pengetahuan	Pre-test (%)	Post-test (%)	Peningkatan
1	Memahami pengertian Cybersecurity	58	95	37%
2	Mengetahui pengertian Phishing	52	94	42%
3	Mengenali Email Phishing	47	91	44%
4	Mengenali Link Palsu	50	92	42%
5	Bahaya Membagikan OTP	63	98	35%
6	Pentingnya Password Kuat	69	96	27%
7	Autentikasi Dua Faktor (2FA)	42	90	48%
8	Keamanan Media Sosial	60	95	35%
9	Cara Melaporkan Penipuan Digital	45	89	44%
10	Perlindungan Data Pribadi	55	94	39%
Rata-rata	54,1	93,4	39,3%	

Tabel 2. Nilai Rata-rata Peserta

Keterangan	Nilai
Jumlah Peserta	30
Rata-rata Pre-test	54,1
Rata-rata Post-test	93,4
Peningkatan	39,3 poin
Persentase Peningkatan	72,64%



Gambar 6. Perbandingan Hasil Pre-test dan Post-test Pada Setiap Indikator Kesadaran Keamanan Siber



Gambar 7. Visualisasi Peningkatan Hasil Pre-test dan Post-test Menggunakan Grafik Radar.

3.3 Pembahasan

Hasil pre-test menunjukkan bahwa sebagian besar siswa telah mengenal penggunaan internet dan media sosial, namun masih memiliki pemahaman yang rendah mengenai keamanan siber, khususnya terkait phishing, keamanan akun, serta perlindungan data pribadi. Hal tersebut terlihat dari nilai rata-rata pre-test sebesar 54,1**,** yang menunjukkan bahwa lebih dari separuh peserta belum mampu mengidentifikasi berbagai bentuk ancaman digital secara tepat. Setelah diberikan edukasi melalui penyampaian materi, demonstrasi kasus phishing, simulasi identifikasi tautan berbahaya, serta sesi diskusi interaktif, terjadi peningkatan pengetahuan yang cukup signifikan. Nilai rata-rata post-test meningkat menjadi 93,4, atau mengalami kenaikan sebesar 39,3 poin dibandingkan sebelum kegiatan dilaksanakan. Peningkatan tertinggi terjadi pada indikator pemahaman mengenai autentikasi dua faktor (2FA) dengan kenaikan sebesar 48%.

Sebelum pelatihan sebagian besar siswa belum mengetahui fungsi 2FA sebagai lapisan keamanan tambahan pada akun digital. Setelah diberikan demonstrasi secara langsung, hampir seluruh peserta memahami pentingnya mengaktifkan fitur tersebut. Selain itu, peningkatan juga terlihat pada kemampuan siswa mengenali email phishing, tautan palsu, serta modus penipuan digital yang sering beredar melalui media sosial maupun aplikasi pesan instan. Selama sesi simulasi, sebagian besar peserta mampu membedakan pesan asli dengan pesan phishing berdasarkan alamat pengirim, isi pesan, tautan yang digunakan, serta permintaan informasi pribadi. Keberhasilan kegiatan ini tidak terlepas dari penggunaan metode pembelajaran yang bersifat partisipatif. Penyampaian materi tidak hanya

dilakukan melalui ceramah, tetapi juga menggunakan studi kasus nyata, simulasi, video pendek, serta diskusi sehingga peserta lebih mudah memahami materi yang diberikan.

Hasil kegiatan ini sejalan dengan penelitian Hidayat dan Wahid (2025) yang menyatakan bahwa edukasi keamanan digital mampu meningkatkan kemampuan peserta dalam mengenali serangan phishing dan menjaga keamanan data pribadi. Temuan ini juga mendukung penelitian Prümmer et al. (2024) yang menyebutkan bahwa pelatihan keamanan siber berbasis simulasi merupakan salah satu metode paling efektif dalam meningkatkan *cybersecurity awareness*. Secara keseluruhan, kegiatan pengabdian ini berhasil meningkatkan literasi keamanan siber siswa di Pekanbaru. Peserta tidak hanya memperoleh pengetahuan baru mengenai ancaman phishing dan penipuan digital, tetapi juga memiliki kemampuan untuk menerapkan langkah-langkah pencegahan dalam kehidupan sehari-hari sehingga risiko menjadi korban kejahatan siber dapat diminimalkan.

4. Kesimpulan

Kegiatan pengabdian kepada masyarakat dengan judul "Peningkatan Kesadaran Keamanan Siber melalui Edukasi Phishing dan Penipuan Digital bagi Siswa di Pekanbaru" telah terlaksana dengan baik dan mendapat respons positif dari peserta. Kegiatan ini mampu meningkatkan pemahaman siswa mengenai pentingnya keamanan siber, khususnya dalam mengenali ancaman phishing, penipuan digital, tautan palsu, penyalahgunaan data pribadi, serta pentingnya menjaga kerahasiaan kata sandi dan kode OTP.
Hasil evaluasi melalui pre-test dan post-test menunjukkan adanya peningkatan pengetahuan peserta setelah mengikuti edukasi. Siswa menjadi lebih memahami cara mengidentifikasi pesan mencurigakan, menerapkan penggunaan kata sandi yang kuat, mengaktifkan autentikasi dua faktor, serta bersikap lebih waspada dalam menggunakan internet dan media sosial. Dengan demikian, kegiatan ini berkontribusi dalam meningkatkan literasi digital dan kesadaran keamanan siber siswa agar dapat menggunakan teknologi secara lebih aman, cerdas, dan bertanggung jawab.
Kegiatan serupa perlu dilakukan secara berkelanjutan dengan cakupan peserta yang lebih luas agar edukasi keamanan siber dapat menjadi bagian dari pembentukan budaya digital yang aman di lingkungan sekolah.

Daftar Pustaka

Baharuddin, M. F., Jalil, A., Amin, Z. M., Rahmad, F., & Shuhidan, S. M. (2025). Digital Literacy and Cybersecurity in Higher Education: The Unseen Power of Academic Librarians. International Journal of Evaluation and Research in Education. https://doi.org/10.11591/ijere.v14i2.34916

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying Phishing Susceptibility for Detection and Behavior Decisions. Human Factors, 58(8), 1158–1172. https://doi.org/10.1177/0018720816665025

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2021). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. Education and Information Technologies, 26(4), 4729–4745. https://doi.org/10.1007/s10639-021-10487-3

Das, S., Kim, A., Tingle, Z., & Nippert-Eng, C. (2019). All About Phishing: Exploring User Research through a Systematic Literature Review. ACM Digital Library. https://doi.org/10.1145/3338500.3360336

Gallo, L., Gentile, D., & Ferraiolo, A. (2024). The Human Factor in Phishing: Collecting and Analyzing Users' Behaviour. Computers & Security, 138, 103684. https://doi.org/10.1016/j.cose.2023.103684

Hendrawan, F. R., et al. (2025)
Cybersecurity Awareness and Community Response to Phishing Threats DOI https://doi.org/10.32664/smatika.v16i02.2332

Hidayat, W., Wahid, S. N., & Nasrullah, A. H. (2025). *Enhancing Students' Digital Security Awareness through Data Protection and Phishing Prevention Education in a Secondary Education Institution*. **Jurnal Sipakatau: Inovasi Pengabdian Masyarakat, 3**(1), 387–395. https://doi.org/10.66314/sipakatau.v3i1.264

Jabir, R., Le, J., & Nguyen, C. (2025). Phishing Attacks in the Age of Generative Artificial Intelligence: A Systematic Review of Human Factors. AI, 6(8), 174. https://doi.org/10.3390/ai6080174

Khadka, K., & Ullah, A. (2025). Human Factors in Cybersecurity: An Interdisciplinary Review and Framework Proposal. International Journal of Information Security. https://doi.org/10.1007/s10207-025-01032-0

Mutlutürk, M. (2024). Phishing and the Human Factor: Insights from a Bibliometric Analysis (2006–2024). Information, 15(10), 643. https://doi.org/10.3390/info15100643

Natasya, C., Irvin, I., & Gunawan, A. A. S. (2024). Cyber Attack: Phishing Environments, Techniques, and Detection Mechanism: A Systematic Literature Review. International Journal of Computer Science and Humanitarian AI, 1(1), 9–13. https://doi.org/10.21512/ijcshai.v1i1.12155

Prümmer, J., Böhm, F., & Pernul, G. (2024). A Systematic Review of Current Cybersecurity Training Methods. Computers & Security, 138, 103663. https://doi.org/10.1016/j.cose.2023.103663

Rahman, T.,(2021). Human Factors in Cybersecurity: A Scoping Review. ACM International Conference Proceedings. https://doi.org/10.1145/3468784.3468789

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. Future Internet, 11(4), 89. https://doi.org/10.3390/fi11040089

Schmitt, M., & Flechais, I. (2023). Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing. arXiv. https://doi.org/10.48550/arXiv.2310.13715

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/1753326.1753687

Tangka, G. M. W., & Putra, E. Y. (2025).
Classification of Indonesian Undergraduate Students' Awareness Level of Phishing Attacks Using Decision Tree Algorithm DOI https://doi.org/10.47065/josh.v6i4.7859