COMSERVA: Jurnal Penelitian dan Pengabdian Masyarakat
e-ISSN: 2798-5210
p-ISSN: 2798-5652
Volume 6 No. 6 Juni 2026

Peningkatan Kesadaran Keamanan Siber Mahasiswa Melalui Edukasi dan Simulasi Serangan Phishing di Politeknik Piksi Input Serang

Dewi Holilah*, Bramantyo Ardi, Mokhammad Fakhrudin Ar-Rahji, Dede Anda, Julian Baja Gunawan, Afra Afiah Ayyasy
Universitas Pamulang, Indonesia
Email: dewholilah@gmail.com*, ardi0594@gmail.com, ajiarrahji@gmail.com, dedeanda19@gmail.com, julian.b.gunawan@gmail.com, afrafiah22@gmail.com

Keywords:
cybersecurity, phishing, digital literacy, phishing simulation, students

Abstract
The rapid development of digital technology has increased the risk of cybercrime, particularly phishing attacks that frequently target students as active internet users. Low levels of cybersecurity awareness and digital literacy make students vulnerable to data theft and misuse of digital accounts. This study aims to improve students' understanding and ability to recognize and prevent phishing attacks through cybersecurity education and phishing simulation activities at Politeknik Piksi Input Serang. The study employed a descriptive approach using the experiential learning concept through workshops, phishing simulations, and hands-on practices. Data were collected through observation, pre-tests, and post-tests to measure participants' understanding before and after the activities. The results showed an improvement in students' understanding of phishing identification, social engineering, the use of two-factor authentication (2FA), and cyber threat mitigation strategies. Simulations and hands-on practices were considered more effective in increasing students' awareness and skills compared to theoretical learning alone. This study contributes to the development of practice-based cybersecurity education methods for students. In conclusion, cybersecurity education and phishing simulations are effective in improving students' cybersecurity literacy; therefore, similar activities should be conducted continuously with more varied scenarios that adapt to the development of digital threats.

Kata Kunci:
keamanan siber, phishing, literasi digital, simulasi phishing, mahasiswa

Abstrak
Perkembangan teknologi digital yang pesat meningkatkan risiko kejahatan siber, khususnya serangan phishing yang banyak menargetkan mahasiswa sebagai pengguna internet aktif. Rendahnya kesadaran dan literasi keamanan siber menyebabkan mahasiswa rentan terhadap pencurian data dan penyalahgunaan akun digital. Penelitian ini bertujuan meningkatkan pemahaman dan kemampuan mahasiswa dalam mengenali serta mencegah serangan phishing melalui edukasi dan simulasi keamanan siber di Politeknik Piksi Input Serang. Metode yang digunakan adalah pendekatan deskriptif dengan konsep experiential learning melalui workshop, simulasi phishing, dan praktik langsung. Pengumpulan data dilakukan menggunakan observasi, pre-test, dan post-test untuk mengukur tingkat pemahaman peserta sebelum dan sesudah kegiatan. Hasil penelitian menunjukkan adanya peningkatan pemahaman mahasiswa terkait identifikasi phishing, social engineering, penggunaan autentikasi dua faktor (2FA), dan langkah mitigasi ancaman siber. Simulasi dan praktik langsung dinilai efektif dalam meningkatkan kesadaran serta keterampilan mahasiswa dibandingkan pembelajaran teoritis. Penelitian ini berkontribusi dalam pengembangan metode edukasi keamanan siber berbasis praktik bagi mahasiswa. Kesimpulannya, edukasi dan simulasi phishing mampu meningkatkan literasi keamanan siber mahasiswa sehingga kegiatan

serupa perlu dilakukan secara berkelanjutan dengan skenario yang lebih variatif dan mengikuti perkembangan ancaman digital.

PENDAHULUAN

Perkembangan teknologi digital telah membawa perubahan besar dalam aktivitas masyarakat, termasuk dalam bidang pendidikan, komunikasi, dan transaksi digital. Namun, peningkatan penggunaan teknologi tersebut juga diiringi dengan meningkatnya ancaman kejahatan siber, salah satunya adalah phishing. Phishing merupakan bentuk serangan siber yang bertujuan memperoleh informasi sensitif seperti username, password, dan data pribadi melalui teknik manipulasi dan penyamaran identitas digital (Gulo et al., 2020). Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN), jumlah anomali trafik siber di Indonesia terus meningkat setiap tahunnya, sementara laporan Anti-Phishing Working Group (APWG) menunjukkan bahwa phishing menjadi salah satu ancaman digital paling dominan secara global. Kondisi ini menunjukkan bahwa keamanan siber telah menjadi isu penting yang memerlukan perhatian serius, khususnya bagi kelompok pengguna internet aktif seperti mahasiswa (Arisanty et al., 2025; Azizah et al., 2026; Budiyanto & Mabruri, 2025).

Mahasiswa merupakan kelompok yang memiliki intensitas penggunaan internet tinggi dalam berbagai aktivitas akademik maupun sosial. Menurut Muammar et al. (2026), Penggunaan email, media sosial, layanan perbankan digital, dan platform pembelajaran daring menyebabkan mahasiswa menjadi kelompok yang rentan terhadap serangan phishing dan social engineering (Banjarnahor, 2025; Efendi et al., 2025). Meskipun mahasiswa sering dianggap memiliki kemampuan teknologi yang baik, penelitian Zwilling et al. (2022) menunjukkan bahwa kelompok usia muda justru memiliki tingkat risiko lebih tinggi terhadap kejahatan siber akibat rendahnya kewaspadaan keamanan digital. Selain itu, rendahnya tingkat literasi digital dan kesadaran keamanan siber masih menjadi permasalahan di Indonesia. Data Kominfo (2021) menunjukkan bahwa sub-indeks keamanan digital masyarakat Indonesia masih berada pada kategori rendah, sehingga diperlukan upaya edukasi yang lebih terstruktur dan aplikatif.

Cybercrime sebagai kejahatan baru yang muncul akibat perkembangan teknologi informasi melibatkan komputer dan mengancam kerahasiaan, integritas, serta keberadaan data dan sistem komputer (Chintia et al., 2018). Kejahatan ini mencakup berbagai aktivitas ilegal seperti hacking, cracking, penyebaran malware, pencurian identitas, carding, ransomware, dan phishing. Serangan siber terus berkembang seiring meningkatnya penggunaan internet dan rendahnya kesadaran pengguna terhadap keamanan digital, sehingga masyarakat, termasuk mahasiswa, menjadi kelompok yang rentan (Octavia et al., 2024; Putri et al., 2025). Mahasiswa sebagai pengguna aktif teknologi digital sering menjadi target serangan phishing karena tingginya aktivitas digital mereka. Phishing adalah kejahatan siber berupa penipuan untuk memperoleh informasi sensitif dengan meniru entitas tepercaya (Gulo et al., 2020). Dalam hukum Indonesia, phishing dapat dijerat dengan UU ITE Pasal 35 dan 36 serta KUHP (Putri Ramadhani Rangkuti et al., 2025).

Social engineering merupakan teknik yang memanfaatkan kelemahan manusia seperti rasa takut, percaya, dan keinginan membantu (Tyas Darmaningrat et al., 2022). Teknik ini sering digunakan dalam phishing untuk meyakinkan korban bahwa pesan atau website berasal dari pihak resmi (Hasanudin & Babussalam, 2024; Kainde et al., 2024; Sulistyo et al., 2024).

Kesadaran terhadap keamanan siber menjadi sangat penting karena banyak insiden terjadi akibat kelalaian pengguna. Simulasi phishing adalah metode pelatihan yang menyerupai serangan nyata dalam lingkungan aman dan terkontrol untuk melatih pengguna mengenali karakteristik phishing serta mengukur efektivitas pelatihan (Tan et al., 2024). Pengguna yang mengikuti simulasi secara rutin cenderung memiliki kewaspadaan lebih tinggi dibandingkan yang hanya mendapat teori.

Berbagai penelitian sebelumnya lebih banyak berfokus pada aspek teknis keamanan sistem dan pengembangan teknologi deteksi serangan siber, sedangkan penelitian terkait peningkatan kesadaran keamanan siber berbasis praktik langsung pada mahasiswa masih relatif terbatas. Padahal, faktor manusia merupakan salah satu celah utama yang sering dimanfaatkan pelaku kejahatan siber melalui teknik social engineering (Tyas Darmaningrat et al., 2022). Lallie et al. (2021) juga menegaskan bahwa rendahnya kesadaran keamanan siber individu menjadi faktor dominan dalam keberhasilan serangan siber dibandingkan kelemahan teknis sistem. Oleh karena itu, diperlukan pendekatan pembelajaran yang tidak hanya bersifat teoritis, tetapi juga memberikan pengalaman langsung kepada pengguna dalam mengenali dan menghadapi ancaman phishing (Hakim et al., 2025).

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk meningkatkan kesadaran dan kemampuan mahasiswa dalam mengenali serta mencegah serangan phishing melalui edukasi keamanan siber dan simulasi phishing berbasis experiential learning di Politeknik Piksi Input Serang. Metode experiential learning dipilih karena mampu mengintegrasikan pemahaman teori dengan praktik langsung melalui workshop, simulasi serangan phishing, dan pelatihan mitigasi ancaman siber. Pendekatan ini diharapkan dapat membantu mahasiswa memahami karakteristik serangan phishing secara lebih nyata serta meningkatkan kemampuan mereka dalam menerapkan langkah-langkah perlindungan digital (Harefa, 2025).

Artikel ini memberikan kontribusi dalam pengembangan metode edukasi keamanan siber berbasis praktik bagi mahasiswa sebagai kelompok pengguna teknologi digital aktif. Selain memperkuat literasi keamanan siber, penelitian ini juga memberikan gambaran mengenai efektivitas simulasi phishing dalam meningkatkan kesadaran dan keterampilan mahasiswa terhadap ancaman digital. Hasil penelitian diharapkan dapat menjadi referensi bagi institusi pendidikan dalam merancang program pelatihan keamanan siber yang lebih interaktif, aplikatif, dan relevan dengan perkembangan ancaman siber saat ini.

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam kegiatan pengabdian kepada masyarakat ini meliputi bagaimana tingkat kesadaran keamanan siber mahasiswa sebelum diberikan edukasi dan simulasi phishing, bagaimana pengaruh edukasi keamanan siber terhadap pemahaman mahasiswa mengenai ancaman phishing dan social engineering, serta bagaimana peningkatan kemampuan mahasiswa dalam mengidentifikasi serangan phishing setelah mengikuti simulasi berbasis praktik langsung. Selain itu, rumusan masalah juga mencakup efektivitas metode *experiential learning* dalam meningkatkan *cybersecurity awareness* mahasiswa, perubahan tingkat pemahaman mahasiswa berdasarkan hasil pre-test dan post-test setelah mengikuti kegiatan, serta rekomendasi metode edukasi keamanan siber berbasis praktik yang efektif diterapkan di lingkungan perguruan tinggi.

Berdasarkan rumusan masalah tersebut, kegiatan pengabdian kepada masyarakat ini bertujuan untuk mengetahui tingkat kesadaran keamanan siber mahasiswa sebelum diberikan

edukasi dan simulasi phishing, menganalisis pengaruh edukasi keamanan siber terhadap pemahaman mahasiswa mengenai ancaman phishing dan social engineering, serta mengukur peningkatan kemampuan mahasiswa dalam mengidentifikasi serangan phishing setelah mengikuti simulasi berbasis praktik langsung. Tujuan lainnya adalah mengetahui efektivitas metode *experiential learning* dalam meningkatkan *cybersecurity awareness* mahasiswa, menganalisis perubahan tingkat pemahaman mahasiswa berdasarkan hasil pre-test dan post-test, serta memberikan rekomendasi metode edukasi keamanan siber berbasis praktik yang efektif diterapkan di lingkungan perguruan tinggi.

Kegiatan pengabdian ini diharapkan memberikan manfaat bagi mahasiswa, yaitu meningkatkan kesadaran dan pemahaman mengenai keamanan siber sehingga mereka mampu menerapkan perilaku digital yang lebih aman. Bagi institusi pendidikan, hasil kegiatan dapat menjadi referensi dalam mengembangkan program edukasi, pelatihan, maupun kebijakan keamanan siber. Bagi pengembangan ilmu pengetahuan, penelitian ini memberikan kontribusi dalam pengembangan metode pembelajaran keamanan siber berbasis *experiential learning* yang lebih interaktif dan aplikatif. Bagi peneliti selanjutnya, hasil penelitian ini dapat menjadi bahan rujukan dan dasar pengembangan penelitian lanjutan. Sementara bagi masyarakat, kegiatan ini diharapkan dapat membantu meningkatkan budaya keamanan digital melalui penyebaran pemahaman mengenai perlindungan data pribadi dan kewaspadaan terhadap ancaman sibe

METODE

Metode Kegiatan

Metode kegiatan dalam Pengabdian Kepada Masyarakat (PKM) ini menggunakan pendekatan deskriptif dengan metode *experiential learning*, yang menggabungkan pembelajaran teoritis dengan praktik langsung agar peserta tidak hanya memahami konsep keamanan siber, tetapi juga mampu menerapkannya dalam situasi nyata. Kegiatan dilaksanakan dalam bentuk workshop intensif yang terdiri atas sesi edukasi, simulasi, diskusi interaktif, dan praktik hands-on terkait identifikasi serta mitigasi serangan phishing.

Tempat dan Waktu

Kegiatan Pengabdian Kepada Masyarakat (PKM) ini akan dilaksanakan di Laboratorium Komputer Politeknik Piksi Input Serang yang berlokasi di Kota Serang, Banten. Pemilihan lokasi tersebut didasarkan pada ketersediaan fasilitas laboratorium komputer, jaringan lokal, serta sarana pendukung yang memadai untuk pelaksanaan edukasi keamanan siber, simulasi phishing, dan workshop praktik secara langsung. Selain itu, lingkungan laboratorium memungkinkan kegiatan simulasi dilakukan secara aman dan terkontrol tanpa mengganggu jaringan publik.

Pelaksanaan kegiatan direncanakan berlangsung selama satu hari penuh dengan pembagian tiga sesi utama, yaitu sesi edukasi kejahatan siber, sesi simulasi serangan phishing, serta sesi workshop pencegahan dan mitigasi ancaman siber. Adapun waktu pelaksanaan kegiatan direncanakan pada bulan, menyesuaikan dengan jadwal akademik dan kesiapan pihak mitra. Kegiatan akan dimulai pada pukul 08.00 WIB hingga selesai agar seluruh rangkaian materi dan praktik dapat dilaksanakan secara optimal.

Khalayak Sasaran

Khalayak sasaran dalam kegiatan Pengabdian Kepada Masyarakat (PKM) ini adalah mahasiswa Program Studi Teknik Informatika di Politeknik Piksi Input Serang. Mahasiswa dipilih sebagai sasaran utama karena merupakan kelompok pengguna teknologi digital yang aktif dalam kegiatan akademik maupun aktivitas sehari-hari, seperti penggunaan email, media sosial, layanan perbankan digital, dan platform pembelajaran daring. Tingginya intensitas penggunaan teknologi tersebut menyebabkan mahasiswa memiliki risiko yang cukup besar terhadap ancaman kejahatan siber, khususnya serangan phishing dan social engineering.

Kerangka Pemecahan Masalah

Kerangka pemecahan masalah dalam kegiatan PKM ini disusun berdasarkan dua permasalahan utama, yaitu rendahnya kesadaran dan literasi keamanan siber mahasiswa serta minimnya keterampilan praktis dalam mengidentifikasi serangan phishing. Untuk mengatasi permasalahan tersebut, dirancang tiga solusi yang dilaksanakan secara sistematis dan saling berkaitan menggunakan pendekatan experiential learning, yaitu metode pembelajaran yang menggabungkan pemahaman teori dengan pengalaman praktik secara langsung. Pendekatan ini dipilih agar mahasiswa tidak hanya memahami konsep keamanan siber secara akademis, tetapi juga mampu menerapkannya dalam situasi nyata.

Solusi pertama dilakukan melalui edukasi komprehensif mengenai kejahatan siber dan serangan phishing. Kegiatan edukasi dilaksanakan menggunakan metode ceramah interaktif, diskusi berbasis studi kasus, dan tanya jawab langsung. Materi yang diberikan mencakup klasifikasi kejahatan siber, anatomi serangan phishing, teknik social engineering, serta dampak hukum kejahatan siber berdasarkan UU ITE. Melalui kegiatan ini diharapkan mahasiswa memiliki pemahaman yang lebih baik mengenai ancaman siber dan meningkatnya kesadaran terhadap pentingnya keamanan digital.

Solusi kedua berupa simulasi serangan phishing berbasis skenario nyata yang dilaksanakan dalam jaringan lokal terisolasi dan aman. Pada tahap ini, peserta diperlihatkan bagaimana pelaku melakukan email spoofing, membuat situs phishing palsu, dan memanfaatkan manipulasi psikologis untuk memperoleh data korban. Selanjutnya, peserta diberikan latihan identifikasi phishing menggunakan berbagai contoh email dan pesan mencurigakan. Kegiatan ini bertujuan meningkatkan kemampuan mahasiswa dalam mengenali ciri-ciri serangan phishing secara langsung sehingga mereka mampu mengambil keputusan yang tepat ketika menghadapi ancaman siber.

Solusi ketiga diwujudkan melalui workshop pencegahan dan mitigasi ancaman siber yang bersifat praktik langsung atau hands-on. Dalam workshop ini peserta mempraktikkan penggunaan password manager, aktivasi autentikasi dua faktor (2FA), pemeriksaan keamanan tautan dan email, serta strategi mitigasi ketika menjadi korban phishing. Dengan adanya workshop ini, mahasiswa diharapkan mampu menerapkan langkah-langkah perlindungan digital secara mandiri dalam kehidupan sehari-hari maupun di lingkungan kerja. Seluruh rangkaian solusi tersebut diharapkan dapat meningkatkan pengetahuan, keterampilan, dan kesadaran mahasiswa terhadap keamanan siber secara menyeluruh.

Realisasi Pemecahan Masalah

Realisasi pemecahan masalah dalam kegiatan PKM ini dilaksanakan melalui rangkaian workshop intensif yang mengintegrasikan edukasi teoritis, simulasi praktik, serta pelatihan langsung mengenai keamanan siber dan ancaman phishing. Kegiatan dilaksanakan di

Laboratorium Komputer Politeknik Piksi Input Serang dengan melibatkan mahasiswa program studi Teknik Informatika sebagai peserta utama. Pelaksanaan program dilakukan secara bertahap sesuai dengan solusi yang telah dirancang agar setiap permasalahan dapat ditangani secara sistematis dan efektif.

Realisasi solusi pertama dilakukan melalui kegiatan edukasi komprehensif mengenai kejahatan siber dan serangan phishing. Pada tahap ini, peserta mengikuti sesi penyampaian materi menggunakan metode ceramah interaktif, diskusi studi kasus, dan tanya jawab langsung dengan narasumber. Materi yang diberikan meliputi jenis-jenis kejahatan siber, teknik phishing dan social engineering, anatomi serangan phishing, serta dampak hukum kejahatan siber berdasarkan UU ITE. Selain itu, peserta juga diperlihatkan berbagai studi kasus nyata yang pernah terjadi di Indonesia agar mahasiswa lebih memahami dampak nyata ancaman siber dalam kehidupan sehari-hari. Untuk mengetahui tingkat pemahaman awal peserta, kegiatan diawali dengan pelaksanaan pre-test sebelum materi diberikan.

Realisasi solusi kedua dilakukan melalui simulasi serangan phishing berbasis skenario nyata yang dilaksanakan dalam jaringan lokal terisolasi sehingga aman dan tidak terhubung ke internet publik. Pada tahap ini, fasilitator mendemonstrasikan secara langsung bagaimana pelaku melakukan email spoofing, membuat pesan phishing, serta merancang situs palsu yang menyerupai portal resmi. Setelah demonstrasi, peserta diberikan latihan identifikasi phishing menggunakan berbagai contoh email dan pesan WhatsApp yang merupakan campuran antara pesan resmi dan serangan phishing. Peserta diminta menganalisis setiap skenario menggunakan checklist identifikasi yang telah disiapkan. Selanjutnya, dilakukan sesi diskusi dan evaluasi bersama untuk membahas indikator phishing yang sering terlewat dan langkah yang tepat dalam menghadapi serangan tersebut.

Realisasi solusi ketiga diwujudkan melalui workshop pencegahan dan mitigasi ancaman siber yang bersifat hands-on. Dalam kegiatan ini, peserta mempraktikkan secara langsung penggunaan password manager Bitwarden, aktivasi autentikasi dua faktor (2FA), pemeriksaan keamanan tautan menggunakan VirusTotal, serta konfigurasi pengaturan privasi akun digital. Peserta juga diberikan panduan mengenai langkah-langkah yang harus dilakukan apabila menjadi korban phishing, seperti pengamanan akun, pelaporan insiden siber, dan strategi pencadangan data menggunakan prinsip 3-2-1. Selama praktik berlangsung, fasilitator mendampingi peserta untuk memastikan seluruh langkah dapat diterapkan dengan baik.

Sebagai bentuk evaluasi pelaksanaan program, peserta mengerjakan post-test menggunakan instrumen yang sama dengan pre-test untuk mengukur peningkatan pemahaman dan kesadaran keamanan siber setelah mengikuti kegiatan. Selain itu, peserta juga diminta mengisi kuesioner kepuasan terkait kualitas materi, efektivitas metode simulasi, serta manfaat kegiatan yang dirasakan. Hasil evaluasi tersebut digunakan untuk menilai keberhasilan program sekaligus menjadi dasar pengembangan kegiatan edukasi keamanan siber selanjutnya.

Instrumen dan Analisis Data

Instrumen yang digunakan adalah soal *pre-test* dan *post-test* (dengan materi yang sama) untuk mengukur perubahan tingkat pemahaman peserta, serta kuesioner kepuasan untuk menilai kualitas materi, efektivitas metode simulasi, dan manfaat kegiatan. Analisis data dilakukan secara deskriptif dengan membandingkan nilai rata-rata pre-test dan post-test serta mengamati peningkatan individual peserta. Sebagai evaluasi akhir, peserta mengerjakan post-

test dan mengisi kuesioner kepuasan. Hasil evaluasi digunakan untuk menilai keberhasilan program sekaligus menjadi dasar pengembangan kegiatan edukasi keamanan siber selanjutnya.

HASIL DAN PEMBAHASAN

Hasil Kegiatan

Tabel 1. Hasil *Pre Test* dan *Post Test Peserta*

No.	Nama Peserta	Nilai Pre Test	Nilai Post Test
1.	Mafrohah	150	150
2.	Andika Rendi Prakarsa	150	150
3.	Ahmad Ibrahim	150	150
4.	Syafiq Amali	120	140
5.	Solahudin Al Ayubi	140	140
6.	Maulana Jaka Purnama	110	110

Sumber: Data primer hasil evaluasi kegiatan PKM Politeknik Piksi Input Serang, 2026

Berdasarkan hasil evaluasi pre-test dan post-test, sebagian besar peserta menunjukkan pemahaman yang baik terhadap materi keamanan siber dan phishing. Hal ini terlihat dari banyaknya peserta yang memperoleh nilai tinggi pada post-test, khususnya pada materi identifikasi phishing, social engineering, dan keamanan akun digital. Selain itu, peserta juga menunjukkan peningkatan kemampuan praktis selama sesi simulasi dan workshop berlangsung.

Pelaksanaan kegiatan Pengabdian Kepada Masyarakat (PKM) mengenai edukasi keamanan siber dan simulasi serangan phishing menunjukkan bahwa mahasiswa memiliki ketertarikan yang tinggi terhadap isu keamanan digital, khususnya ancaman phishing dan social engineering yang saat ini semakin sering terjadi. Selama kegiatan berlangsung, peserta terlihat aktif dalam mengikuti sesi edukasi, diskusi, maupun simulasi praktik yang diberikan oleh fasilitator. Antusiasme tersebut menunjukkan bahwa materi keamanan siber merupakan kebutuhan yang relevan bagi mahasiswa sebagai pengguna aktif teknologi digital.

Berdasarkan hasil pre-test dan post-test, sebagian besar peserta menunjukkan pemahaman yang baik terhadap materi yang diberikan. Meskipun rata-rata nilai keseluruhan tidak menunjukkan peningkatan yang signifikan, beberapa peserta mengalami peningkatan nilai setelah mengikuti kegiatan. Selain itu, terdapat peserta yang mampu mempertahankan nilai tinggi pada post-test, yang menunjukkan bahwa peserta telah memiliki pemahaman dasar yang baik mengenai keamanan siber dan mampu memahami materi lanjutan yang diberikan selama workshop. Hasil ini menunjukkan bahwa kegiatan edukasi dan simulasi phishing tetap memberikan dampak positif terhadap pemahaman peserta.

Pada sesi simulasi phishing, peserta memperoleh pengalaman langsung mengenai cara kerja serangan phishing, mulai dari email spoofing, pembuatan situs palsu, hingga teknik manipulasi psikologis yang digunakan pelaku. Pengalaman praktik tersebut membantu peserta memahami indikator-indikator phishing seperti alamat pengirim mencurigakan, tautan palsu, penggunaan bahasa yang mendesak, serta permintaan data pribadi yang tidak wajar. Selama sesi latihan identifikasi phishing, sebagian besar peserta mampu membedakan pesan resmi dan pesan phishing dengan cukup baik setelah mendapatkan penjelasan dari fasilitator.

Workshop pencegahan dan mitigasi ancaman siber juga memberikan manfaat praktis bagi peserta. Mahasiswa dapat mempraktikkan secara langsung penggunaan password

manager, aktivasi autentikasi dua faktor (2FA), pemeriksaan keamanan tautan menggunakan tools digital, serta langkah-langkah penanganan apabila menjadi korban phishing. Kegiatan praktik langsung ini dinilai efektif karena peserta tidak hanya menerima teori, tetapi juga memperoleh keterampilan yang dapat diterapkan dalam kehidupan sehari-hari maupun di lingkungan kerja.

Secara keseluruhan, kegiatan PKM ini berhasil meningkatkan kesadaran peserta terhadap pentingnya keamanan siber dan kewaspadaan terhadap ancaman phishing. Metode pembelajaran berbasis simulasi dan praktik langsung terbukti membantu peserta memahami ancaman siber secara lebih nyata dibandingkan pembelajaran teori semata. Oleh karena itu, kegiatan edukasi keamanan siber serupa perlu dilakukan secara berkelanjutan agar literasi digital dan kemampuan perlindungan diri mahasiswa terhadap ancaman siber dapat terus meningkat.

KESIMPULAN

Berdasarkan hasil pelaksanaan kegiatan Pengabdian Kepada Masyarakat (PKM) mengenai edukasi keamanan siber dan simulasi serangan phishing kepada mahasiswa Politeknik Piksi Input Serang, dapat disimpulkan bahwa kegiatan yang dilaksanakan mampu meningkatkan kesadaran mahasiswa terhadap pentingnya keamanan siber dan ancaman phishing di lingkungan digital. Melalui kegiatan edukasi, peserta memperoleh pemahaman mengenai jenis-jenis kejahatan siber, teknik social engineering, serta dampak yang dapat ditimbulkan oleh serangan phishing. Pelaksanaan simulasi phishing berbasis skenario nyata memberikan pengalaman langsung kepada peserta dalam mengenali ciri-ciri serangan phishing, seperti email spoofing, tautan mencurigakan, dan website palsu. Selain itu, workshop praktik pencegahan dan mitigasi ancaman siber membantu peserta memahami langkah-langkah perlindungan akun digital, penggunaan autentikasi dua faktor (2FA), serta strategi penanganan apabila menjadi korban serangan siber. Berdasarkan hasil evaluasi pre-test, post-test, serta observasi selama kegiatan berlangsung, peserta menunjukkan pemahaman dan keterampilan yang lebih baik dalam mengenali serta menghadapi ancaman phishing. Secara keseluruhan, kegiatan PKM ini berjalan dengan baik dan memberikan manfaat positif bagi mahasiswa dalam meningkatkan literasi keamanan siber serta kewaspadaan terhadap ancaman digital yang semakin berkembang.

Berdasarkan hasil pelaksanaan kegiatan Pengabdian Kepada Masyarakat (PKM) mengenai edukasi keamanan siber dan simulasi serangan phishing, terdapat beberapa saran yang dapat diberikan untuk pengembangan kegiatan selanjutnya. Pertama, kegiatan edukasi dan pelatihan keamanan siber sebaiknya dilaksanakan secara berkala agar kesadaran dan kewaspadaan mahasiswa terhadap ancaman siber dapat terus meningkat seiring berkembangnya metode serangan digital. Kedua, materi dan simulasi yang diberikan dapat dikembangkan dengan skenario yang lebih beragam dan menyesuaikan tren serangan siber terbaru, seperti phishing melalui media sosial, aplikasi mobile, maupun serangan berbasis kecerdasan buatan. Dengan demikian, peserta dapat memperoleh pengalaman yang lebih luas dalam mengenali berbagai bentuk ancaman digital. Ketiga, pihak kampus diharapkan dapat mendukung peningkatan literasi keamanan siber melalui penyediaan program pelatihan, seminar, maupun integrasi materi keamanan informasi dalam proses pembelajaran. Selain itu, mahasiswa juga diharapkan dapat menerapkan pengetahuan dan keterampilan yang diperoleh

selama kegiatan dalam kehidupan sehari-hari serta membagikan pemahaman tersebut kepada lingkungan sekitarnya agar kesadaran keamanan siber di masyarakat semakin meningkat.

REFERENSI

Arisanty, M., Riady, Y., Kharis, S. A. A., Permatasari, S. M., & Sukatmi, S. (2025). Cerdas Dan Aman Bermedia Digital: Peningkatan Kesadaran Keamanan Siber Di Era Hoaks Dan Phishing. *Jurnal Pengabdian Kepada Masyarakat Patikala*, *4*(4), 1407–1418.

Arisanty, M., Riady, Y., Kharis, S. A. A., Permatasari, S. M., & Sukatmi, S. (2025). Cerdas dan aman bermedia digital: Peningkatan kesadaran keamanan siber di era hoaks dan phishing. *Jurnal Pengabdian Kepada Masyarakat Patikala, 4*(4), 1407–1418.

Azizah, N., Mudjiyanto, B., Yanuar, F., Nursyamsi, N., & Launa, L. (2026). Literasi digital dan kewaspadaan siber: Analisis tingkat kesadaran privasi pengguna terhadap ancaman doxing. *Jurnal Ilmu Komunikasi AKRAB, 11*(1).

Banjarnahor, A. R. (2025). Edukasi keamanan digital dalam penggunaan dompet digital di kalangan mahasiswa: Upaya meningkatkan kesadaran dan keamanan transaksi. *Jurnal DIKMAS, 7*(1), 20–32.

Budiyanto, D., & Mabruri, M. (2025). Pentingnya keamanan siber dalam era digital: Tinjauan global dan kondisi di Indonesia. *Prosiding Seminar Nasional Sains dan Teknologi "SainTek," 2*(1), 981–994.

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Rakhmawati, N. A. (2018). Kasus kejahatan siber yang paling banyak terjadi di Indonesia dan penanganannya. *Journal Information Engineering and Educational Technology, 2*.

Efendi, N. A., Harahap, M. I., & Syahbudi, M. (2025). Pengaruh social engineering dan cyber crime terhadap persepsi keamanan pada aplikasi BSI Mobile. *Jurnal Manajemen Terapan dan Keuangan, 14*(3), 1237–1250.

Gulo, A. S., Lasmadi, S., & Nawawi, K. (2020). Cyber crime dalam bentuk phishing berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *Journal of Criminal, 1*.

Hakim, A. S., Mustaqim, P. J., & Naufal, A. (2025). Peran pendidikan digital dalam melindungi privasi pengguna dan mencegah dampak sosial. *Jurnal Ilmiah Sistem Informasi, 4*(2), 162–174.

Harefa, A. M. L. (2025). Sosialisasi bahaya phishing dan tips aman menggunakan internet bagi mahasiswa. *Jurnal Pengabdian Kepada Masyarakat Teknologi Informasi dan Komunikasi, 2*(2), 39–44.

Hasanudin, A. F., & Babussalam, A. B. (2024). Perlindungan hukum bagi korban kejahatan phishing yang menguras saldo m-banking. *Jurnal Gagasan Hukum, 6*(1), 16–29.

Kainde, Q. C., Tambanaung, J. S., Inkiriwang, V. T., & Mile, A. A. P. (2024). Forensic analysis of phishing attacks: Investigative approach. *Jurnal Teknik Informatika (JUTIF), 5*(4), 631–640.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105*, Article 102248. https://doi.org/10.1016/j.cose.2021.102248

Muammar, Y., Juliana, J., Azizah, M., Hafizah, H., & Sari, M. B. (2026). Studi keamanan akun media sosial mahasiswa terhadap serangan phishing berbasis social engineering. *JIKUM: Jurnal Ilmu Komputer, 2*(2), 144–148.

Octavia, A. N., Fauzi, A., Kurniawan, G. A., Putri, N. F., Alghifari, R. D., Rasim, R., Manrejo, S., & Adienda, Y. M. (2024). Peran pemahaman cyber security untuk keamanan akun media sosial Instagram mahasiswa. *Orbit: Jurnal Ilmu Multidisiplin Nusantara, 1*(2),

75–85.
Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2025). Keamanan online dalam media sosial: Pentingnya perlindungan data pribadi di era digital (Studi kasus Desa Pematang Jering). *Jurnal Pengabdian Nasional (JPN) Indonesia, 6*(1), 38–52.
Putri Ramadhani Rangkuti, P., Khoiri, M. A., Ritonga, S., & Pane, P. N. S. (2025). Sanksi pidana terhadap kejahatan phishing menurut hukum pidana Indonesia. *Konstitusi: Jurnal Hukum, Administrasi Publik, dan Ilmu Komunikasi, 2*(3), 291–305. https://doi.org/10.62383/konstitusi.v2i3.908
Sulistyo, A. D., Wicaksono, B. D., Saputra, R. N., & Ramadhani, R. (2024). Strategi penanggulangan serangan phishing di media sosial. *Prosiding Seminar Nasional Teknologi Informasi dan Bisnis*, 385–396.
Tan, T., Sama, H., Wibowo, T., Wijaya, G., & Aboagye, O. E. (2024). Kesadaran keamanan siber pada kalangan mahasiswa universitas di Kota Batam. *Jurnal Teknologi dan Informasi (JATI), 14*.
Tyas Darmaningrat, E. W., Noor Ali, A. H., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi bahaya dan upaya pencegahan social engineering untuk meningkatkan kesadaran masyarakat tentang keamanan informasi. *Jurnal Pengabdian Kepada Masyarakat*.
Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269