MANARUKO
Jurnal Pengabdian Masyarakat
https://jmpe.ppj.unp.ac.id/index.php/manaruko/index
Vol.5, No.1, 2026
ISSN (Electronic) : 2986-9048

Edukasi Pencegahan *Phising* Melalui Peningkatan Literasi Keamanan Siber di SMP Negeri 61 Palembang

Migel Orvin Febryan[1], Siska Amelia[2], Siti Fatimah Az Zahrah[3*], Syalsabilla Valentisyesa[4], Joseph Eduard Uly Loni[5], Iis Pardesan[6], Dafid[7]
[1,2,3,4,5,6,7]Universitas Multi Data Palembang
*Corresponding author: sitifatimahazzahrah_2327250055@mhs.mdp.ac.id

DOI:
https://doi.org/10.24036/manaruko.v5i1.99
Diterima: 23-05-2026
Revisi : 10-06-2026
Available Online: 30-06-2026

KEYWORDS
Phishing, Cybersecurity, Digital Literacy, Students, Internet Security

KATA KUNCI
Phishing, Keamanan Siber, Literasi Digital.

A B S T R A C T

Cybercrime in the form of phishing has become a growing threat among students due to the high intensity of internet and social media usage without adequate digital security awareness. This community service activity aimed to improve students' understanding of phishing prevention through cyber security literacy education at SMP Negeri 61 Palembang. The activity involved 26 junior high school students and was conducted using educational methods consisting of material presentations, interactive discussions, case studies, and simple simulations. The materials covered the definition of phishing, types of attacks, identification of suspicious links, protection of personal data, and preventive measures in digital activities. The results showed that participants experienced increased understanding and awareness regarding phishing threats and digital security practices. Participants were also able to identify phishing characteristics and apply preventive actions in daily internet usage. This activity concluded that interactive cyber security education can effectively improve digital literacy and foster safer digital behavior among students.

A B S T R A K

Perkembangan teknologi digital meningkatkan risiko kejahatan siber, salah satunya phishing, terutama pada kalangan pelajar yang aktif menggunakan internet dan media sosial. Kegiatan pengabdian kepada masyarakat ini bertujuan meningkatkan literasi keamanan siber siswa melalui edukasi pencegahan phishing di SMP Negeri 61 Palembang. Kegiatan dilaksanakan kepada 26 siswa dengan metode penyampaian materi, diskusi interaktif, studi kasus, dan simulasi sederhana. Materi yang diberikan meliputi pengertian phishing, jenis serangan, identifikasi tautan mencurigakan, perlindungan data pribadi, serta langkah-langkah pencegahan dalam penggunaan teknologi digital. Hasil kegiatan menunjukkan adanya peningkatan pemahaman dan kesadaran peserta terhadap ancaman phishing serta pentingnya menjaga keamanan data pribadi. Peserta juga mampu mengenali ciri-ciri phishing dan menerapkan tindakan pencegahan dalam aktivitas digital sehari-hari. Kegiatan ini menunjukkan bahwa edukasi keamanan siber berbasis interaktif efektif meningkatkan literasi digital dan membentuk perilaku penggunaan internet yang lebih aman pada pelajar.

This is an open access article distributed under the Creative Commons Attribution-NonCommercial 4.0 International License. Some rights reserved

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah mendorong peningkatan signifikan dalam penggunaan internet di Indonesia, khususnya di kalangan generasi muda. Data dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2022 mencatat tingkat penetrasi internet Indonesia mencapai 77,02% dari total populasi, dengan kelompok usia 13–18 tahun sebagai salah satu segmen pengguna aktif terbesar (APJII, 2022). Pelajar tingkat sekolah menengah pertama (SMP) kini menggunakan internet tidak hanya untuk keperluan belajar, tetapi juga untuk berinteraksi di media sosial, mengakses hiburan digital, dan berbagai aktivitas daring lainnya. Namun, tingginya intensitas penggunaan internet ini tidak selalu diikuti dengan pemahaman yang memadai mengenai keamanan digital (Kominfo, 2023).

Kejahatan siber merupakan salah satu dampak negatif yang muncul seiring pesatnya perkembangan teknologi digital. *Phishing* adalah salah satu bentuk kejahatan siber yang paling umum dan terus berkembang. *Phishing* merupakan teknik penipuan digital di mana pelaku menyamar sebagai entitas terpercaya untuk mencuri informasi sensitif pengguna, seperti kata sandi, nomor rekening, kode OTP, atau data pribadi lainnya (Heartfield & Loukas, 2016). Serangan *phishing* umumnya disampaikan melalui email, pesan singkat, media sosial, serta situs web palsu yang meniru tampilan layanan resmi. Badan Siber dan Sandi Negara (BSSN) dalam Laporan Lanskap Keamanan Siber Indonesia 2024 melaporkan bahwa *phishing* masih menjadi ancaman siber dominan yang terus mengalami peningkatan jumlah kasus dari tahun ke tahun (BSSN, 2024).

Pelajar merupakan kelompok yang rentan terhadap serangan *phishing* karena tingginya aktivitas digital mereka yang belum diimbangi dengan kecakapan literasi keamanan siber yang memadai. Pengguna usia muda cenderung memiliki kemampuan yang lebih rendah dalam mengenali indikator tautan atau situs berbahaya dibandingkan pengguna dewasa yang lebih berpengalaman (Zwilling et al., 2022). Selain itu, kebiasaan pengguna muda yang sering berbagi informasi pribadi di media sosial tanpa mempertimbangkan risiko privasi turut meningkatkan potensi mereka menjadi korban *phishing* dan penyalahgunaan data (Diaz et al., 2018; Shahbazi et al., 2025).

Pemerintah Indonesia telah memberikan perhatian khusus terhadap pentingnya literasi digital dan keamanan siber bagi masyarakat, termasuk kalangan pelajar. Melalui program Gerakan Nasional Literasi Digital (GNLD) yang dikelola oleh Kementerian Komunikasi dan Informatika (Kominfo) sejak 2017, pemerintah mendorong peningkatan kompetensi digital masyarakat dalam empat pilar, salah satunya adalah keamanan digital (Kominfo, 2023). ilar keamanan digital mencakup kemampuan mengenali ancaman siber, melindungi data pribadi, memahami etika digital, serta menggunakan teknologi secara aman dan bertanggung jawab. Meskipun demikian, implementasi literasi keamanan siber pada tingkat sekolah menengah masih perlu diperkuat melalui kegiatan edukasi yang lebih interaktif dan aplikatif agar mudah dipahami oleh siswa (Riandari et al., 2024).

Berbagai penelitian menunjukkan bahwa pendekatan edukasi interaktif terbukti efektif dalam meningkatkan kesadaran dan kemampuan pengguna dalam mengenali serangan *phishing*. Program pelatihan berbasis simulasi phishing mampu meningkatkan kemampuan peserta dalam mengidentifikasi email maupun tautan *phishing* secara signifikan (Frauenstein & Flowerday, 2020). Selain itu, faktor kepribadian dan perilaku pengguna juga berpengaruh terhadap tingkat kerentanan seseorang terhadap serangan *phishing*, terutama pada pengguna dengan tingkat impulsivitas dan pengambilan risiko yang tinggi (Moustafa et al., 2021). Pendekatan pembelajaran berbasis studi kasus, simulasi, dan gamifikasi dinilai mampu meningkatkan motivasi belajar sekaligus efektivitas penyampaian materi keamanan siber kepada pelajar (Riandari et al., 2024). Di sisi lain, perkembangan teknologi kecerdasan buatan (*Artificial Intelligence*/AI) menyebabkan teknik *phishing* menjadi semakin sulit dikenali karena pesan yang dihasilkan tampak lebih realistis dan meyakinkan (Kavvadias & Kotsilieris, 2025).

Berdasarkan permasalahan tersebut, kegiatan pengabdian kepada masyarakat ini dilaksanakan dalam bentuk edukasi pencegahan *phishing* melalui peningkatan literasi keamanan siber kepada siswa SMP Negeri 61 Palembang. Kegiatan ini bertujuan meningkatkan pengetahuan, kesadaran, dan keterampilan siswa dalam mengenali serta mencegah serangan *phishing* sehingga mereka dapat menggunakan teknologi digital secara lebih aman, bijak, dan bertanggung jawab.

METODE PELAKSANAAN

Kegiatan pengabdian kepada masyarakat ini dilaksanakan di SMP Negeri 61 Palembang pada tanggal 29 April 2026 dengan melibatkan 26 siswa sebagai peserta kegiatan. Sasaran kegiatan dipilih secara *purposive* karena

pelajar tingkat SMP merupakan pengguna aktif internet dan media sosial yang rentan terhadap ancaman *phishing* dan penyalahgunaan data pribadi.

Metode pelaksanaan kegiatan menggunakan kombinasi metode Pendidikan Masyarakat, Pelatihan, dan Simulasi Ipteks. Metode Pendidikan Masyarakat dilakukan melalui penyampaian materi mengenai keamanan siber dan *phishing*. Metode Pelatihan dilakukan melalui demonstrasi identifikasi tautan mencurigakan dan perlindungan akun digital. Sementara itu, metode Simulasi Ipteks dilakukan dengan memberikan studi kasus *phishing* kepada peserta untuk melatih kemampuan identifikasi ancaman digital. Materi edukasi yang diberikan kepada peserta disajikan pada Tabel 1.

Tabel 1. Metode Edukasi Kegiatan Pengabdian

No	Materi Edukasi	Metode Penyampaian
1	Pengertian dan jenis *phishing*	Presentasi interaktif
2	Ciri-ciri tautan *phishing*	Demonstrasi
3	Perlindungan data pribadi	Diskusi
4	Pencegahan *phishing*	Simulasi kasus
5	Penggunaan *password* aman	Praktik sederhana

Sumber : Tim pelaksana, 2026

Metode Pelatihan dilakukan melalui demonstrasi cara mengenali tautan mencurigakan, identifikasi situs palsu, penggunaan *password* yang aman, serta langkah-langkah pencegahan *phishing* pada media sosial dan aplikasi komunikasi digital. Pendekatan ini dipilih agar siswa tidak hanya memahami teori secara konseptual, tetapi juga menguasai keterampilan teknis yang relevan dengan aktivitas digital mereka sehari-hari. Selain itu, penggunaan alat peraga visual dalam demonstrasi membantu siswa dalam memvisualisasikan bentuk ancaman siber yang sebenarnya terjadi di internet.

Peserta diberikan contoh kasus sederhana untuk meningkatkan pemahaman praktis terkait ancaman *phishing*. Melalui kasus nyata tersebut, siswa diajak untuk berpikir kritis dalam menganalisis pesan yang mencurigakan sehingga mereka mampu mengambil tindakan pencegahan yang tepat sebelum menjadi korban kejahatan siber.

Selanjutnya, metode Simulasi Ipteks dilakukan dengan memberikan simulasi studi kasus *phishing* kepada peserta. Dalam simulasi tersebut, peserta diminta mengidentifikasi ciri-ciri pesan atau tautan *phishing* dan menentukan tindakan yang tepat untuk menghindari ancaman penipuan digital. Simulasi ini bertujuan meningkatkan keterampilan peserta dalam menerapkan pengetahuan keamanan siber pada situasi nyata.

Alat dan bahan yang digunakan dalam kegiatan meliputi laptop, proyektor, jaringan internet, media presentasi berbentuk *slide*, materi edukasi keamanan siber, serta contoh studi kasus *phishing*. Tahapan pelaksanaan kegiatan terdiri atas tahap persiapan, pelaksanaan edukasi, simulasi kasus, diskusi interaktif, dan evaluasi kegiatan. Teknik pengumpulan data dilakukan melalui observasi langsung terhadap partisipasi peserta, sesi tanya jawab, dan evaluasi pemahaman peserta selama kegiatan berlangsung. Data yang diperoleh dianalisis menggunakan teknik analisis deskriptif berdasarkan tingkat keaktifan, pemahaman peserta terhadap materi, serta kemampuan peserta dalam mengenali dan mencegah serangan *phishing*.

HASIL DAN PEMBAHASAN

Kegiatan edukasi pencegahan *phishing* melalui peningkatan literasi keamanan siber di SMP Negeri 61 Palembang telah dilaksanakan dengan melibatkan 26 siswa sebagai peserta. Kegiatan dilakukan melalui penyampaian materi, diskusi interaktif, dan simulasi kasus *phishing* untuk meningkatkan pemahaman peserta mengenai keamanan digital. Kegiatan ini difokuskan pada pengenalan ancaman siber yang sering terjadi di kalangan pelajar agar mereka lebih waspada terhadap modus penipuan daring.

Proses penyampaian materi dan diskusi interaktif selama kegiatan berlangsung dapat dilihat pada Gambar 1 dan 2. Dokumentasi tersebut menunjukkan tingginya antusiasme serta keaktifan peserta dalam merespons materi yang diberikan selama sesi berlangsung. Hal ini menunjukkan bahwa metode edukasi yang diterapkan sangat efektif dalam membangun kesadaran para peserta akan pentingnya praktik keamanan siber di kehidupan sehari-hari.

Gambar 1. Kegiatan Penyampaian Materi
Sumber : Tim pelaksana, 2026

Gambar 2. Kegiatan Diskusi
Sumber : Tim pelaksana, 2026

Hasil kegiatan menunjukkan bahwa peserta memiliki antusiasme yang tinggi selama kegiatan berlangsung. Hal ini terlihat dari keaktifan peserta dalam sesi diskusi dan tanya jawab mengenai bentuk-bentuk *phishing*, keamanan data pribadi, serta cara mengenali tautan mencurigakan. Sebagian besar peserta juga mampu memahami materi yang disampaikan dan dapat menjelaskan kembali ciri-ciri *phishing* setelah sesi edukasi berlangsung. Antusiasme peserta dapat dilihat pada Gambar 3.

Gambar 3. Antusiasme Peserta Menjawab Pertanyaan
Sumber : Tim pelaksana, 2026

Melalui simulasi studi kasus, peserta mulai mampu membedakan antara tautan asli dan tautan *phishing* serta memahami risiko membagikan data pribadi secara sembarangan. Selain itu, peserta juga memahami pentingnya penggunaan *password* yang kuat dan fitur keamanan tambahan seperti verifikasi dua langkah dalam melindungi akun digital.

Akhir dari pengabdian ini dilakukan apresiasi kepada peserta yang berhasil menjawab pertanyaan diberikan beserta dokumentasi bersama dengan peserta pengabdian yang dapat dilihat pada Gambar 4 dan 5. Pemberian apresiasi ini bertujuan untuk memotivasi siswa agar tetap antusias dan mengingat kembali poin-poin utama materi yang telah disampaikan.

Gambar 4. Dokumentasi Pemberian Hadiah Apresiasi
Sumber : Tim pelaksana, 2026

Gambar 5. Dokumentasi Bersama Peserta
Sumber : Tim pelaksana, 2026

Peningkatan pemahaman peserta menunjukkan bahwa metode edukasi berbasis interaktif efektif dalam meningkatkan literasi keamanan siber pada pelajar. Hasil ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa pendekatan edukasi melalui simulasi dan praktik langsung dapat meningkatkan kesadaran pengguna terhadap ancaman *phishing* dan keamanan digital. Selain itu, keterlibatan aktif siswa dalam setiap sesi diskusi terbukti mampu meminimalisir kekeliruan dalam mengidentifikasi tautan berbahaya yang sering ditemui di media sosial.

Selain memberikan dampak positif kepada peserta, kegiatan ini juga meningkatkan kemampuan komunikasi dan penerapan ilmu pengetahuan bagi tim pelaksana dalam melakukan edukasi kepada masyarakat. Pengalaman ini memberikan wawasan berharga bagi tim pelaksana mengenai tantangan nyata di lapangan dalam menyampaikan materi teknis yang kompleks menjadi bahasa yang lebih mudah dipahami oleh kalangan remaja.

SIMPULAN

Kegiatan pengabdian kepada masyarakat mengenai edukasi pencegahan *phishing* di SMP Negeri 61 Palembang berhasil meningkatkan pemahaman dan kesadaran peserta terhadap ancaman kejahatan siber, khususnya *phishing*. Melalui metode penyampaian materi, diskusi interaktif, dan simulasi kasus, peserta mampu mengenali ciri-ciri *phishing* serta memahami langkah-langkah pencegahan yang tepat dalam menjaga keamanan data pribadi.

Kegiatan ini menunjukkan bahwa pendekatan edukasi berbasis interaktif efektif dalam meningkatkan literasi keamanan siber pada pelajar. Selain memberikan pengetahuan teoritis, kegiatan ini juga membentuk sikap kritis dan perilaku digital yang lebih aman dalam penggunaan internet dan media sosial. Namun, kegiatan ini masih terbatas pada satu sekolah dan jumlah peserta yang relatif sedikit sehingga diperlukan pengembangan kegiatan serupa dengan cakupan yang lebih luas di masa mendatang.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada SMP Negeri 61 Palembang yang telah memberikan izin dan dukungan dalam pelaksanaan kegiatan pengabdian kepada masyarakat ini. Ucapan terima kasih juga disampaikan kepada Universitas Multi Data Palembang, dosen pembimbing, serta seluruh mahasiswa pelaksana yang telah berkontribusi dalam menyukseskan kegiatan edukasi pencegahan *phishing* melalui peningkatan literasi keamanan siber.

DAFTAR PUSTAKA

APJII. (2022). Profil Internet Indonesia 2022. *SRA Consulting.*, *June*.

BSSN. (2024). *LANSKAP KEAMANAN SIBER INDONESIA*.

Diaz, A., Sherman, A. T., & Joshi, A. (2018). Phishing in an Academic Community: A Study of User Susceptibility and Behavior. *Cryptologia*, *44*(1), 53–67. https://doi.org/10.1080/01611194.2019.1623343

Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security*, *94*, 101862. https://doi.org/10.1016/J.COSE.2020.101862

Heartfield, R., & Loukas, G. (2016). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, *48*(3). https://doi.org/10.1145/2835375

Kavvadias, A., & Kotsilieris, T. (2025). Understanding the Role of Demographic and Psychological Factors in Users' Susceptibility to Phishing Emails: A Review. *Applied Sciences 2025, Vol. 15, Page 2236*, *15*(4), 2236. https://doi.org/10.3390/APP15042236

Kominfo. (2023). *STATUS LITERASI DIGITAL DI INDONESIA*.

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology*, *12*, 561011. https://doi.org/10.3389/FPSYG.2021.561011/TEXT

Riandari, F., Tasril, V., & Ritonga, R. P. (2024). *Increasing cybersecurity awareness among teenagers through digital education and simulation*.

Shahbazi, Z., Jalali, R., & Molaeevand, M. (2025). AI-Based Phishing Detection and Student Cybersecurity Awareness in the Digital Age. *Big Data and Cognitive Computing*, *9*(8), 210. https://doi.org/10.3390/BDCC9080210

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