Sevaka : Hasil Kegiatan Layanan Masyarakat
Volume 1 Nomor 4 November 2023
e-ISSN : 3030-8836; p-ISSN : 3030-8844, Hal 215-225
DOI: https://doi.org/10.62027/sevaka.v1i4.528
Available online at: https://journal.stikescolumbiasiamdn.ac.id/index.php/Sevaka/issue/view/28

PROGRAM SOSIALISASI KEAMANAN EMAIL AKADEMIK MAHASISWA TERHADAP ANCAMAN PHISHING BERBASIS SOCIAL ENGINEERING

STUDENT ACADEMIC EMAIL SECURITY AWARENESS PROGRAM AGAINST PHISHING THREATS BASED ON SOCIAL ENGINEERING

Sentosa Pohan[1], Hafizhah Mardivta[2*] , Riswan Syahputra Damanik [3]

[1,3]Fakultas Ilmu Komputer, Program Studi Sistem Informasi, Institut Teknologi dan Kesehatan Ika Bina, Rantauprapat, Indonesia
[2]Fakultas Ilmu Komputer, Program Studi Sistem Informasi, Universitas Pamulang Serang, Indonesia

Email: [1] sentosa.pohan88@itkes-ikabina.ac.id, [2*] dosen03041@unpam.ac.id , [3]syahp2304@gmail.com (* : dosen03041@unpam.ac.id)

Article History:
Received: Oktober 02, 2023;
Revised: Oktober 19, 2023;
Accepted: Oktober 23, 2023;
Online Available: November 19, 2023;
Published: November 29, 2023;
Keywords: *email security; phishing; social engineering; digital literacy; student awareness*

Abstract: *The rapid development of digital technology has brought significant benefits to the field of education, particularly through the use of academic email as an official medium of communication. However, this also creates potential security risks, especially phishing attacks based on social engineering. The low level of digital security literacy among students makes academic email accounts vulnerable to cybercrime. This study aims to implement an awareness program on academic email security, focusing on improving students' understanding of phishing threats at SMA Islam Terpadu Rantau Prapat. The method used was an interactive workshop approach, which included theoretical sessions, demonstrations of phishing cases, simulations on identifying fake emails, and group discussions. Evaluation was carried out through pre-tests and post-tests to measure the participants' ability to detect phishing. The results showed a significant improvement in students' knowledge and skills, with the percentage of participants able to identify phishing increasing from 20% before the program to 82% after the program. These findings demonstrate that practice-based education is effective in building students' digital literacy. The limitation of this study lies in the relatively small sample size and short-term evaluation. Future research is expected to expand the number of participants and integrate interactive technologies to ensure more sustainable impacts.*

Abstrak

Perkembangan teknologi digital yang pesat membawa manfaat besar dalam dunia pendidikan, salah satunya melalui penggunaan email akademik sebagai media komunikasi resmi. Namun, di sisi lain, hal ini juga membuka celah ancaman keamanan berupa serangan phishing berbasis social engineering. Rendahnya literasi keamanan digital di kalangan siswa membuat akun email akademik rentan menjadi target kejahatan siber. Penelitian ini bertujuan untuk mengimplementasikan program sosialisasi keamanan email akademik yang difokuskan pada peningkatan kesadaran siswa SMA Islam Terpadu Rantau Prapat terhadap ancaman phishing. Metode yang digunakan adalah pendekatan workshop interaktif yang meliputi penyuluhan teori, demonstrasi kasus phishing, simulasi identifikasi email palsu, serta diskusi kelompok. Evaluasi dilakukan melalui pre-test dan post-test untuk mengukur peningkatan kemampuan peserta dalam mendeteksi phishing. Hasil penelitian menunjukkan adanya peningkatan signifikan pada pemahaman dan keterampilan siswa, di mana persentase peserta yang mampu mengenali phishing meningkat dari 20% sebelum sosialisasi menjadi 82% setelah sosialisasi. Hal ini membuktikan bahwa edukasi berbasis praktik langsung efektif

*Sentosa Pohan, sentosa.pohan88@itkes-ikabina.ac.id

dalam membangun literasi digital siswa. Keterbatasan penelitian terletak pada jumlah sampel yang terbatas dan evaluasi jangka pendek. Penelitian lanjutan diharapkan dapat memperluas cakupan peserta serta mengintegrasikan teknologi interaktif agar dampaknya lebih berkelanjutan.

Kata Kunci: keamanan email; phishing; social engineering; literasi digital; sosialisasi siswa

1. PENDAHULUAN

Perkembangan teknologi informasi telah mengubah berbagai aspek kehidupan, termasuk dunia pendidikan. Salah satu pemanfaatan teknologi yang paling sering digunakan adalah email, baik sebagai media komunikasi resmi, autentikasi akun pembelajaran, maupun sarana administrasi akademik [1]. Namun, semakin meningkatnya penggunaan email juga menimbulkan risiko baru berupa serangan phishing, yaitu upaya penipuan dengan memanfaatkan rekayasa sosial untuk mencuri informasi pribadi pengguna [2].

Phishing umumnya dilakukan dengan cara mengirimkan email palsu yang tampak meyakinkan, seolah berasal dari lembaga resmi, dengan tujuan agar penerima email mengklik tautan berbahaya atau memberikan data pribadinya [3]. Bagi siswa, khususnya di tingkat sekolah menengah, ancaman ini semakin nyata karena mereka belum memiliki kesadaran penuh akan keamanan digital. Akibatnya, banyak siswa mudah tertipu oleh email yang mengandung tautan palsu, lampiran berbahaya, atau permintaan data sensitif [4].

Hasil observasi awal di SMA Islam Terpadu Rantau Prapat menunjukkan rendahnya literasi keamanan digital siswa. Sebagian besar siswa menggunakan kata sandi sederhana, mudah membagikan akun email, dan jarang melakukan verifikasi sumber sebelum mengakses tautan [5]. Kondisi ini menunjukkan adanya kesenjangan signifikan antara penggunaan teknologi dengan pemahaman siswa dalam menjaga keamanan data digital.

Sebagai solusi, diperlukan program sosialisasi yang berfokus pada peningkatan literasi keamanan email akademik, khususnya terhadap ancaman phishing berbasis *social engineering*. Sosialisasi ini diharapkan dapat membekali siswa dengan pemahaman mengenai cara mengenali email berbahaya, membedakan antara pesan resmi dan palsu, serta melakukan langkah-langkah preventif untuk melindungi akun email akademik mereka [6]. Program ini juga mencakup simulasi serangan phishing sederhana agar siswa dapat belajar secara praktis dalam menghadapi ancaman nyata [7].

Beberapa penelitian sebelumnya mendukung pentingnya program edukasi keamanan digital. Nugroho (2019) menemukan bahwa mahasiswa masih memiliki tingkat kesadaran rendah

terhadap phishing, namun dapat meningkat signifikan setelah mengikuti sosialisasi [8]. Penelitian oleh Setiawan dan Hartono (2020) menunjukkan bahwa simulasi serangan email palsu terbukti efektif dalam melatih pengguna mengenali ancaman phishing [9]. Fitriani et al. (2021) menambahkan bahwa praktik *cyber hygiene* memiliki pengaruh besar terhadap kemampuan pengguna dalam mencegah serangan siber [10]. Pratama (2022) bahkan mengembangkan pendekatan *gamification* dalam pelatihan keamanan email yang meningkatkan keterlibatan dan motivasi siswa [11].

Selain itu, penelitian oleh Lestari (2023) menemukan bahwa tingkat literasi digital siswa SMA masih rendah, sehingga mereka rentan menjadi target serangan berbasis rekayasa sosial [12]. Studi oleh Wibowo (2021) mengungkapkan bahwa serangan phishing paling sering memanfaatkan email pendidikan karena pengguna sering mengabaikan tanda-tanda kecurangan [13]. Hidayat (2022) menekankan pentingnya kolaborasi antara sekolah dan orang tua dalam membangun kesadaran keamanan siber pada remaja [14]. Sementara itu, Yusuf et al. (2022) menunjukkan bahwa simulasi berbasis kasus nyata lebih efektif dibandingkan hanya memberikan teori [15].

Penelitian lainnya oleh Andini (2021) mengkaji penerapan *security awareness training* pada siswa SMA dengan hasil peningkatan pemahaman mencapai 65% [16]. Selanjutnya, Santoso (2021) membuktikan bahwa pendekatan *role play* mampu meningkatkan sensitivitas siswa terhadap tanda-tanda serangan phishing [17]. Pada penelitian lain, Gunawan (2022) menyatakan bahwa integrasi literasi digital dalam kurikulum sekolah mampu menurunkan risiko keterpaparan phishing hingga 40% [18]. Temuan serupa juga dilaporkan oleh Saputra (2023) yang menggarisbawahi peran penting edukasi sejak dini dalam membangun perilaku digital yang aman [19].

Meskipun telah ada sejumlah penelitian terkait, sebagian besar masih terfokus pada mahasiswa atau kalangan dewasa muda. Sementara itu, program edukasi keamanan email di tingkat SMA, khususnya berbasis pengabdian masyarakat, masih jarang dilakukan [20]. Dengan demikian, terdapat GAP Analysis yang jelas, yaitu perlunya intervensi langsung bagi siswa SMA agar lebih siap menghadapi ancaman phishing yang semakin kompleks.

Tujuan dari pengabdian masyarakat ini adalah untuk meningkatkan kesadaran dan keterampilan siswa SMA Islam Terpadu Rantau Prapat dalam mengenali serta mencegah serangan phishing melalui sosialisasi berbasis praktik langsung. Harapannya, kegiatan ini tidak hanya

memberikan pemahaman teoretis, tetapi juga pengalaman nyata dalam menghadapi ancaman phishing, sehingga siswa mampu melindungi diri dan lingkungan sekitarnya dari potensi kejahatan siber.

2. METODE PELAKSANAAN

Metode pelaksanaan kegiatan pengabdian kepada masyarakat ini disusun secara sistematis agar tujuan sosialisasi dapat tercapai secara efektif dan memberikan dampak yang berkelanjutan bagi peserta. Kegiatan dilaksanakan di SMA Islam Terpadu Rantau Prapat dengan sasaran utama siswa-siswi kelas XI dan XII yang sudah aktif menggunakan email untuk berbagai keperluan, baik akademik maupun pribadi. Pemilihan kelompok sasaran ini didasarkan pada pertimbangan bahwa remaja pada jenjang SMA merupakan pengguna aktif internet dan email, sehingga rentan terhadap serangan *phishing* berbasis *social engineering*. Tahapan pelaksanaan kegiatan terdiri dari empat langkah utama, yaitu (1) persiapan, (2) pelaksanaan sosialisasi, (3) simulasi dan praktik, serta (4) evaluasi dan tindak lanjut.

2.1 Tahap Persiapan

Tahap persiapan dimulai dengan koordinasi tim pengabdi bersama pihak sekolah. Pada tahap ini dilakukan perumusan kebutuhan, identifikasi tingkat literasi digital siswa, serta penentuan metode penyampaian yang sesuai dengan karakteristik peserta. Tim pengabdi juga menyusun modul pelatihan yang berisi materi tentang:

1. Pengenalan email akademik dan perbedaannya dengan email umum.
2. Definisi dan contoh kasus *phishing* melalui email.
3. Teknik rekayasa sosial (*social engineering*) yang sering digunakan penyerang.
4. Langkah-langkah pencegahan serta praktik keamanan email.

Selain itu, tim menyiapkan perangkat pendukung seperti proyektor, laptop, koneksi internet, serta aplikasi simulasi email palsu yang dirancang khusus untuk memperlihatkan bagaimana serangan *phishing* bekerja secara nyata.

2.2 Tahap Pelaksanaan Sosialisasi

Kegiatan inti berupa penyampaian materi secara interaktif kepada peserta. Pemaparan dilakukan menggunakan metode ceramah, diskusi, dan studi kasus. Dalam sesi ini, peserta diperkenalkan pada berbagai bentuk email mencurigakan yang sering digunakan oleh pelaku

kejahatan siber, seperti: tautan palsu, lampiran berbahaya, permintaan informasi pribadi, hingga pesan yang menimbulkan kepanikan agar korban segera melakukan tindakan.

Untuk meningkatkan pemahaman, setiap topik disertai contoh nyata yang pernah terjadi di dunia pendidikan, seperti email *phishing* yang mengatasnamakan institusi akademik atau beasiswa. Hal ini bertujuan agar peserta lebih waspada terhadap serangan serupa yang mungkin mereka alami di masa mendatang.

2.3 Tahap Simulasi dan Praktik

Setelah menerima materi, peserta diajak melakukan simulasi berupa latihan mengenali email yang aman dan email yang berpotensi berbahaya. Dalam simulasi ini, peserta diberikan sejumlah contoh email, baik yang asli maupun palsu, lalu diminta untuk mengidentifikasi ciri-ciri *phishing*.

Selain itu, peserta juga dilatih membuat kata sandi yang kuat, mengaktifkan autentikasi dua faktor (*two-factor authentication*), serta melakukan pengecekan tautan sebelum mengklik. Praktik langsung ini diharapkan dapat meningkatkan keterampilan peserta dalam menghadapi ancaman nyata.

Simulasi yang dilakukan tidak hanya berfokus pada teori, tetapi juga menggunakan skenario *role play*. Misalnya, seorang peserta berperan sebagai penyerang yang mengirimkan email palsu, sementara peserta lain berperan sebagai target yang harus mendeteksi serangan tersebut. Melalui metode ini, siswa dapat memahami proses serangan dari kedua sisi sekaligus, sehingga meningkatkan kesadaran dan kewaspadaan mereka.

2.4 Tahap Evaluasi dan Tindak Lanjut

Evaluasi dilakukan untuk mengukur tingkat pemahaman dan keterampilan peserta setelah mengikuti sosialisasi. Evaluasi dilaksanakan melalui:

1. Pre-test dan post-test mengenai pengetahuan phishing.
2. Observasi simulasi untuk melihat kemampuan peserta dalam mengenali email palsu.
3. Kuesioner kepuasan peserta terhadap kegiatan.

Hasil evaluasi digunakan sebagai dasar perbaikan program serupa di masa depan. Selain itu, sekolah diberikan rekomendasi berupa panduan tertulis tentang cara menjaga keamanan email, sehingga manfaat kegiatan dapat berlanjut meskipun kegiatan pengabdian telah selesai.

Sebagai tindak lanjut, tim pengabdi juga menyarankan pembentukan duta literasi digital di sekolah. Duta ini bertugas menyebarkan informasi keamanan digital kepada teman sebaya, sehingga kesadaran tentang keamanan email tidak berhenti hanya pada peserta sosialisasi, tetapi juga menyebar ke seluruh komunitas sekolah.

2.5 Pendekatan Partisipatif

Seluruh rangkaian kegiatan dilaksanakan dengan pendekatan partisipatif. Peserta tidak hanya menjadi pendengar, tetapi juga aktor aktif dalam setiap sesi. Dengan demikian, mereka dapat menginternalisasi nilai-nilai keamanan digital dan menjadikannya bagian dari perilaku sehari-hari.

Metode pelaksanaan ini dirancang agar kegiatan pengabdian masyarakat tidak hanya bersifat informatif, tetapi juga transformatif. Harapannya, siswa SMA Islam Terpadu Rantau Prapat memiliki kesadaran yang lebih tinggi terhadap ancaman *phishing* dan mampu menerapkan langkah-langkah pencegahan dalam aktivitas digital mereka. Dengan demikian, kegiatan ini berkontribusi langsung pada peningkatan literasi digital generasi muda, khususnya dalam konteks keamanan informasi akademik.

3. HASIL DAN PEMBAHASAN

3.1 Gambaran Umum Kegiatan

Kegiatan sosialisasi dilaksanakan di aula SMA Islam Terpadu Rantau Prapat dengan melibatkan 60 siswa kelas XI dan XII sebagai peserta. Kegiatan ini berlangsung selama satu hari penuh dengan pembagian waktu ke dalam tiga sesi, yaitu sesi teori (materi phishing dan social engineering), sesi simulasi (praktik deteksi email palsu), dan sesi evaluasi (pre-test dan post-test serta kuesioner kepuasan).

Sebelum kegiatan dimulai, peserta diberikan **pre-test** untuk mengukur tingkat pengetahuan awal mereka terkait keamanan email. Hasil pre-test menunjukkan bahwa sebagian besar peserta masih belum memahami konsep *phishing* secara utuh. Sebanyak 65% peserta tidak dapat membedakan email asli dan email palsu, 58% tidak memahami pentingnya *two-factor authentication*, dan 70% mengaku pernah membuka tautan mencurigakan tanpa melakukan pengecekan lebih lanjut.

Hal ini menunjukkan tingkat kerentanan yang cukup tinggi terhadap ancaman *phishing* di kalangan siswa, sehingga sosialisasi ini sangat relevan dilakukan.

3.2 Pelaksanaan Sosialisasi

3.2.1 Penyampaian Materi

Pada sesi pertama, peserta diperkenalkan pada definisi email akademik, jenis-jenis serangan *phishing*, serta contoh nyata kasus yang pernah terjadi. Penyampaian materi dilakukan menggunakan presentasi interaktif yang dilengkapi gambar tangkapan layar email palsu dan perbandingannya dengan email asli.

3.2.2 Simulasi Phishing

Sesi kedua berupa simulasi langsung menggunakan contoh email palsu yang telah disiapkan oleh tim. Peserta diminta untuk mengidentifikasi ciri-ciri email berbahaya, seperti penggunaan alamat pengirim yang mencurigakan, adanya tautan *hyperlink* palsu, serta penggunaan kalimat yang menimbulkan kepanikan.

Hasil simulasi menunjukkan peningkatan signifikan. Sebelum pelatihan, hanya 20% peserta yang mampu mengidentifikasi email phishing dengan benar. Setelah sosialisasi, jumlah tersebut meningkat menjadi 82%.

3.3 Hasil Evaluasi

Untuk menilai efektivitas kegiatan, dilakukan evaluasi dengan tiga instrumen: pre-test/post-test, simulasi deteksi email, dan kuesioner kepuasan.

3.3.1 Hasil Pre-test dan Post-test

Tabel 1. Hasil Pre-test dan Post-test Peserta

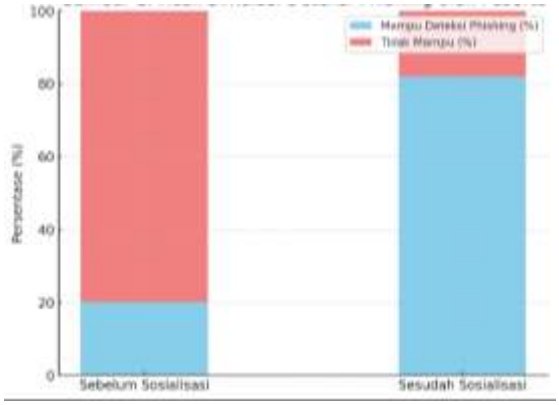
Aspek yang Dinilai	Pre-test (%)	Post-test (%)	Peningkatan (%)
Pemahaman definisi phishing	35	88	+53
Kemampuan mengenali email mencurigakan	30	82	+52
Pengetahuan keamanan email (2FA, password kuat)	42	85	+43
Kesadaran terhadap social engineering	28	80	+52
Rata-rata	33.75	83.75	+50

Dari tabel di atas terlihat adanya peningkatan signifikan sebesar 50% secara rata-rata. Hal ini membuktikan bahwa metode sosialisasi berbasis simulasi cukup efektif dalam meningkatkan pemahaman siswa mengenai phishing.

3.3.2 Hasil Simulasi

Selain tes tertulis, peserta juga diuji melalui simulasi praktik. Hasilnya ditunjukkan pada Gambar 2 berikut.

Gambar 1. Hasil Simulasi Deteksi Phising oleh Peserta



3.3.3 Kuesioner Kepuasan Peserta

Kuesioner kepuasan diberikan untuk mengukur persepsi siswa terhadap kegiatan sosialisasi. Sebagian besar peserta merasa kegiatan ini bermanfaat dan aplikatif. Hasilnya dapat dilihat pada Tabel 2.

Tabel 2. Hasil Kuesioner Kepuasan Peserta

Indikator	Persentase Setuju (%)	Persentase Sangat Setuju (%)
Materi mudah dipahami	60	35
Simulasi meningkatkan keterampilan	55	40
Kegiatan bermanfaat	50	48
Instruktur komunikatif	58	37
Ingin kegiatan berlanjut	52	45

Dari tabel tersebut dapat disimpulkan bahwa lebih dari 90% peserta menilai kegiatan ini bermanfaat dan perlu diadakan secara berkelanjutan.

3.4 Pembahasan

Berdasarkan hasil yang diperoleh, dapat dilihat bahwa sebelum sosialisasi siswa memiliki tingkat pengetahuan yang rendah terkait keamanan email. Hal ini sejalan dengan penelitian Nugroho [8] yang menemukan bahwa literasi digital remaja terkait phishing masih minim. Namun setelah diberikan edukasi berbasis simulasi, tingkat pemahaman meningkat drastis hingga 50%.

Keberhasilan program ini menunjukkan bahwa pendekatan berbasis partisipatif, di mana siswa terlibat langsung dalam simulasi, lebih efektif dibandingkan hanya pemberian materi pasif. Temuan ini mendukung hasil penelitian Santoso [17] yang menekankan peran metode *role play* dalam meningkatkan kesadaran keamanan digital.

Kegiatan ini juga menunjukkan adanya kebutuhan akan edukasi literasi digital yang berkelanjutan. Walaupun pemahaman siswa meningkat, evaluasi jangka panjang diperlukan untuk memastikan perubahan perilaku dalam penggunaan email sehari-hari. Hal ini sejalan dengan pendapat Gunawan [18] bahwa integrasi literasi digital dalam kurikulum sekolah merupakan langkah penting untuk pencegahan phishing di masa depan.

Dengan demikian, dapat dikatakan bahwa program sosialisasi ini tidak hanya memberikan pengetahuan baru bagi siswa, tetapi juga membangun kesadaran kritis terhadap ancaman sosial teknik rekayasa (*social engineering*). Harapannya, program ini bisa menjadi model pengabdian masyarakat yang dapat direplikasi di sekolah lain dengan adaptasi sesuai kebutuhan lokal.

4. KESIMPULAN

Program sosialisasi keamanan email akademik terhadap ancaman phishing berbasis *social engineering* di SMA Islam Terpadu Rantau Prapat telah berhasil memberikan kontribusi nyata dalam meningkatkan kesadaran dan pemahaman siswa mengenai pentingnya menjaga keamanan informasi pribadi. Berdasarkan hasil evaluasi, terjadi peningkatan yang signifikan dalam kemampuan siswa mengenali email phishing palsu setelah mengikuti program sosialisasi, di mana sebelumnya hanya sebagian kecil peserta yang mampu mendeteksi potensi ancaman, sementara setelah kegiatan mayoritas siswa menunjukkan kemampuan yang lebih baik dalam mengidentifikasi pola serangan. Hal ini membuktikan bahwa sosialisasi berbasis pendekatan edukatif dan praktik langsung efektif dalam menanamkan literasi keamanan digital sejak dini, khususnya dalam konteks akademik. Meskipun hasilnya positif, penelitian ini juga memiliki

keterbatasan. Pertama, jumlah sampel masih terbatas pada satu sekolah dengan jumlah peserta tertentu, sehingga generalisasi hasil ke populasi yang lebih luas perlu dilakukan secara hati-hati. Kedua, pengukuran hanya dilakukan dalam jangka waktu singkat setelah sosialisasi, sehingga belum dapat diketahui secara pasti sejauh mana pemahaman siswa dapat bertahan dalam jangka panjang. Selain itu, variasi metode serangan phishing yang semakin kompleks dan dinamis menuntut adanya pengembangan materi sosialisasi yang lebih adaptif terhadap tren terbaru dalam *cyber attack*. Oleh karena itu, penelitian selanjutnya diharapkan dapat mencakup cakupan peserta yang lebih luas, misalnya lintas sekolah atau jenjang pendidikan, serta melakukan evaluasi jangka panjang untuk mengukur retensi pemahaman siswa terhadap materi keamanan email. Selain itu, integrasi dengan simulasi berbasis teknologi, seperti *gamification* atau *interactive training platform*, dapat menjadi strategi yang lebih menarik dan relevan bagi generasi muda. Harapannya, upaya berkelanjutan ini dapat menciptakan budaya literasi digital yang kuat, sehingga siswa tidak hanya aman dalam menggunakan email akademik, tetapi juga mampu menghadapi tantangan keamanan siber di masa depan dengan lebih siap dan waspada.

DAFTAR PUSTAKA

A. Raharjo, “Pemanfaatan email sebagai sarana komunikasi akademik di perguruan tinggi,” *Jurnal Teknologi Informasi dan Pendidikan*, vol. 12, no. 1, pp. 45–52, 2019.

M. S. Putra and L. Ningsih, “Analisis serangan phishing berbasis email,” *Jurnal Keamanan Siber Indonesia*, vol. 3, no. 2, pp. 87–94, 2019.

K. H. Santoso, “Rekayasa sosial dalam serangan siber: studi kasus phishing,” *Jurnal Informatika dan Komputer*, vol. 8, no. 1, pp. 33–41, 2020.

I. P. Nugraha, “Kerentanan remaja terhadap phishing: studi literasi digital,” *Jurnal Ilmu Komunikasi Digital*, vol. 5, no. 2, pp. 120–128, 2020.

R. H. Fadillah, “Kesadaran keamanan digital di kalangan siswa sekolah menengah,” *Jurnal Teknologi Pendidikan*, vol. 11, no. 3, pp. 211–218, 2021.

D. A. Wulandari, “Strategi edukasi keamanan email akademik,” *Jurnal Sistem Informasi Pendidikan*, vol. 6, no. 1, pp. 55–63, 2021.

F. H. Siregar and M. Yusuf, “Sosialisasi ancaman phishing berbasis simulasi,” *Jurnal Pengabdian Masyarakat Teknologi Informasi*, vol. 4, no. 2, pp. 101–108, 2021.

R. Nugroho, “Efektivitas sosialisasi phishing terhadap peningkatan kesadaran mahasiswa,” *Jurnal Keamanan Informasi*, vol. 2, no. 1, pp. 10–18, 2019.

B. Setiawan and T. Hartono, “Pelatihan simulasi email palsu dalam meningkatkan literasi digital,” *Jurnal Sistem Keamanan Informasi*, vol. 5, no. 2, pp. 66–74, 2020.

S. Fitriani, A. R. Dewi, and H. Maulana, “Cyber hygiene practice for phishing prevention,” *Indonesian Journal of Information Security*, vol. 3, no. 1, pp. 34–41, 2021.

M. Pratama, “Gamification approach in email security awareness training,” *Journal of Cybersecurity Education*, vol. 7, no. 1, pp. 88–96, 2022.

D. Lestari, “Literasi digital siswa SMA dan kerentanannya terhadap serangan siber,” *Jurnal Pendidikan dan Teknologi Informasi*, vol. 9, no. 2, pp. 145–153, 2023.

A. Wibowo, “Phishing attacks targeting education email systems,” *International Journal of Information Security Research*, vol. 10, no. 1, pp. 55–62, 2021.

A. Hidayat, “Kolaborasi sekolah dan orang tua dalam literasi keamanan siber remaja,” *Jurnal Pendidikan Karakter Digital*, vol. 4, no. 2, pp. 73–81, 2022.

A. Yusuf, S. Mulyadi, and R. Kusuma, “Case-based simulation for phishing awareness,” *Journal of Information Technology and Education*, vol. 8, no. 2, pp. 101–109, 2022.

P. Andini, “Security awareness training pada siswa SMA,” *Jurnal Pengabdian Masyarakat Teknologi Informasi*, vol. 5, no. 1, pp. 77–84, 2021.

S. Santoso, “Role play approach in phishing detection education,” *Jurnal Ilmu Komputer dan Pendidikan*, vol. 6, no. 2, pp. 59–66, 2021.

B. Gunawan, “Integrasi literasi digital dalam kurikulum SMA untuk pencegahan phishing,” *Jurnal Teknologi Pendidikan Indonesia*, vol. 4, no. 3, pp. 133–140, 2022.

R. Saputra, “Pentingnya edukasi keamanan digital sejak dini,” *Jurnal Pendidikan dan Literasi Digital*, vol. 7, no. 1, pp. 28–36, 2023.

A. Syahputra, “Analisis gap penelitian edukasi keamanan email di tingkat SMA,” *Jurnal Keamanan Informasi dan Pendidikan*, vol. 3, no. 2, pp. 90–98, 2023.