

## EDUKASI DAN SIMULASI PHISHING UNTUK MENINGKATKAN LITERASI KEAMANAN SIBER SISWA SMA SEJAHTERA 1 DEPOK

Sapta Nugraha<sup>1</sup>, Ferry Setefanus<sup>2</sup>, Indriyani Astuti<sup>3</sup>, Muhammad Al-Farisy<sup>4</sup>, Ferdiansyah Winardi<sup>5</sup>, Agung Sutopo<sup>6</sup>, Abdul Haris<sup>7</sup>, dan Arya Adhyaksa Waskita<sup>8</sup>

<sup>1</sup>Program Studi Teknik Informatika S-2, Program Pascasarjana, Universitas Pamulang, Jl. Raya Puspipetek, Buaran, Kota Tangerang Selatan, Banten, Indonesia, 15310

e-mail: [saptasakuragi@gmail.com](mailto:saptasakuragi@gmail.com), [ferrysetefanus@gmail.com](mailto:ferrysetefanus@gmail.com), [indrie.edu@gmail.com](mailto:indrie.edu@gmail.com), [m.alfarisy797@gmail.com](mailto:m.alfarisy797@gmail.com), [winardiferdiansyah@gmail.com](mailto:winardiferdiansyah@gmail.com), [agunkmars@gmail.com](mailto:agunkmars@gmail.com), [abdulharis.net.dev@gmail.com](mailto:abdulharis.net.dev@gmail.com)

### Abstract

*High school students are active users of digital services, yet their ability to recognize phishing and social engineering attacks has not kept pace with that use. The partner school, SMA Sejahtera 1 Depok, did not yet have a structured, practice-based cybersecurity education program. This community service activity aimed to improve students' cybersecurity literacy and their ability to recognize and resist phishing and social engineering attacks. It was carried out as a one-day intensive workshop on 25 September 2026 for about 50 grade X students. The methods combined interactive lectures, case demonstrations, controlled simulations, role-play, and group discussions across four pillars: cybersecurity concepts, the anatomy of phishing, social engineering patterns, and account security practices. The case demonstration used a fake free food-and-drink e-voucher claim email impersonating a look-alike brand of a well-known coffee shop near the school. Evaluation used a pre-test and post-test, simulation worksheets, a phishing email simulation, and a satisfaction questionnaire. Of the 35 phishing emails delivered, 17 students (48.6%) opened the fake link and entered data into the imitation form without verification. The mean score rose from 90.67 on the pre-test (30 students) to 97.92 on the post-test (24 students), and correct identification of a safe address rose from 46.7% to 100%. These findings show that students remain vulnerable to familiar instant offers even when their knowledge is high, underlining the importance of experience-based education. All simulations were controlled, and the data entered by students were used only to count responses and were not published.*

### Abstrak

Siswa sekolah menengah atas (SMA) merupakan pengguna aktif layanan digital, tetapi kemampuan mereka dalam mengenali serangan *phishing* dan *social engineering* belum berkembang sejalan dengan intensitas penggunaan tersebut. SMA Sejahtera 1 Depok sebagai mitra belum memiliki program edukasi keamanan siber yang terstruktur dan berbasis praktik. Kegiatan pengabdian kepada masyarakat ini bertujuan meningkatkan literasi keamanan siber siswa serta kemampuan mengenali dan menolak serangan *phishing* dan *social engineering*. Kegiatan dilaksanakan dalam bentuk *workshop* intensif satu hari pada 25 September 2026 dan diikuti sekitar 50 siswa kelas X. Metode yang digunakan memadukan ceramah interaktif, demonstrasi kasus, simulasi terkendali, permainan peran, dan diskusi kelompok dengan materi yang disusun ke dalam empat pilar, yaitu konsep keamanan siber, anatomi *phishing*, pola *social engineering*, dan praktik pengamanan akun. Demonstrasi kasus menggunakan skenario surel klaim *e-voucher* makanan dan minuman gratis palsu yang mengatasnamakan merek tiruan dari kedai kopi ternama di dekat sekolah. Evaluasi dilakukan melalui *pre-test* dan *post-test*, lembar kerja simulasi, simulasi surel jebakan, dan kuesioner kepuasan. Dari 35 surel jebakan yang berhasil terkirim, 17 siswa (48,6%) membuka tautan palsu dan mengisi data pada formulir tiruan tanpa verifikasi. Rata-rata skor meningkat dari 90,67 pada *pre-test* (30 siswa) menjadi 97,92 pada *post-test* (24 siswa), dan ketepatan memilih alamat yang aman

naik dari 46,7% menjadi 100%. Temuan ini menunjukkan bahwa siswa tetap rentan terhadap tawaran instan yang terasa familiar meskipun pengetahuannya sudah tinggi sehingga edukasi berbasis pengalaman langsung menjadi penting. Seluruh simulasi dijalankan secara terkendali, dan data isian siswa hanya digunakan untuk rekapitulasi jumlah serta tidak dipublikasikan.

Keywords: Phishing; Social Engineering; Cybersecurity Literacy; Simulation; High School Students

## 1. PENDAHULUAN

Transformasi digital telah menjadikan internet dan perangkat bergerak sebagai bagian dari keseharian remaja Indonesia. Siswa sekolah menengah atas (SMA) kini mengelola surel, media sosial, dompet digital, dan layanan pembelajaran daring yang terhubung pada identitas digital mereka. Kemudahan tersebut sekaligus memperluas permukaan serangan, terutama serangan yang menyasar sisi manusia alih-alih sisi teknologi. Salah satu bentuk yang paling umum adalah *phishing*, yaitu upaya memperoleh informasi sensitif dengan menyamar sebagai pihak tepercaya melalui surel, pesan singkat, atau situs tiruan [1]. *Phishing* merupakan bagian dari *social engineering*, yakni manipulasi psikologis yang mendorong korban melakukan tindakan atau mengungkapkan informasi yang seharusnya dirahasiakan [2], [3]. Karena memanfaatkan kepercayaan dan kelengahan, manusia kerap disebut sebagai mata rantai terlemah dalam sistem keamanan informasi [4].

Remaja termasuk kelompok yang rentan terhadap serangan tersebut. Kajian demografis tentang kerentanan terhadap *phishing* menemukan bahwa kelompok usia muda lebih mudah terkecoh dibandingkan kelompok usia lainnya [5]. Pengguna juga cenderung menilai keaslian sebuah situs dari tampilan isinya, bukan dari indikator keamanan seperti alamat URL [6], sementara sifat impulsif berkaitan dengan perilaku keamanan siber yang berisiko [7]. Pada konteks pelajar Indonesia, remaja cenderung merespons pesan bernada mendesak atau menjanjikan hadiah tanpa verifikasi sehingga membutuhkan pendampingan yang kontekstual [8].

Berbagai kajian menunjukkan bahwa kewaspadaan terhadap *phishing* lebih efektif dibangun melalui pelatihan yang melibatkan pengalaman langsung daripada imbauan satu arah. Pelatihan yang disisipkan pada konteks nyata membantu pengguna mempertahankan pengetahuan tentang *phishing* [9], dan pelatihan berbasis kesadaran penuh (*mindfulness*) saat menilai pesan efektif menekan respons terhadap surel *phishing* [10]. Sejumlah kegiatan pengabdian kepada masyarakat juga melaporkan hasil yang sejalan. Sosialisasi pencegahan *social engineering*

meningkatkan kesadaran masyarakat tentang keamanan informasi [11], pelatihan perlindungan data pribadi membekali siswa SMK menghadapi risiko di dunia digital [12], edukasi yang memadukan materi interaktif dan praktik meningkatkan rata-rata skor pemahaman siswa SMA dari 60 menjadi 88 [13], serta simulasi serangan dalam lingkungan virtual meningkatkan kesadaran keamanan siber siswa SMK [14].

SMA Sejahtera 1 Depok yang berlokasi di Jl. Anyelir Raya No. 68, Depok Jaya, Kecamatan Pancoran Mas, Kota Depok, merupakan sekolah swasta yang aktivitas akademik dan administrasinya semakin bertumpu pada layanan digital. Hasil identifikasi bersama mitra menunjukkan bahwa sekolah belum memiliki program edukasi keamanan siber yang terstruktur dan berbasis praktik. Sebagian besar siswa belum pernah dilatih mengenali tautan dan situs palsu, membedakan surel resmi dari surel penipuan, maupun merespons permintaan data pribadi yang mencurigakan. Materi keamanan digital yang diterima siswa umumnya berhenti pada imbauan normatif sehingga belum terbentuk menjadi kewaspadaan perilaku.

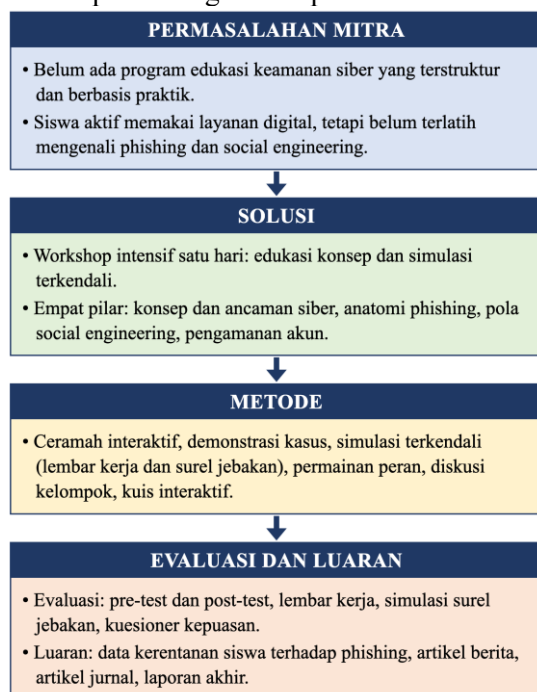
Berdasarkan permasalahan tersebut, kegiatan pengabdian kepada masyarakat ini bertujuan (1) meningkatkan pemahaman siswa terhadap konsep dasar keamanan siber, karakteristik *phishing*, dan pola *social engineering*; (2) melatih siswa mengenali indikator serangan secara mandiri melalui simulasi terkendali; dan (3) mendorong kebiasaan digital yang aman, seperti penggunaan kata sandi yang kuat dan autentikasi dua faktor. Berbeda dari kegiatan sebelumnya, kegiatan ini memadukan edukasi konsep, lembar kerja simulasi, permainan peran, dan simulasi surel jebakan dengan skenario yang dekat dengan keseharian siswa sehingga siswa dapat merasakan langsung bagaimana tawaran instan dapat mengalahkan kewaspadaan.

## 2. METODE

Kegiatan ini merupakan pengabdian kepada masyarakat berbentuk *workshop* edukasi dan simulasi. Kegiatan dilaksanakan pada Jumat, 25 September 2026, mulai pukul 08.00 WIB di SMA Sejahtera 1 Depok, Jl. Anyelir Raya No. 68, Depok Jaya, Kecamatan Pancoran Mas, Kota

Depok, Jawa Barat. Sasaran kegiatan adalah siswa kelas X SMA Sejahtera 1 Depok dengan jumlah peserta sekitar 50 siswa. Kegiatan dilaksanakan oleh tujuh mahasiswa Program Studi Teknik Informatika S-2 Universitas Pamulang dengan pendampingan dosen.

Kerangka pemecahan masalah disusun berdasarkan permasalahan prioritas mitra sebagaimana ditunjukkan pada Gbr. 1. Solusi yang ditawarkan adalah *workshop* intensif satu hari dengan materi yang dibagi ke dalam empat pilar, yaitu (1) konsep keamanan siber dan lanskap ancaman, (2) anatomi serangan *phishing* dan teknik verifikasi, (3) pola *social engineering* melalui permainan peran, serta (4) praktik pengamanan akun dan perlindungan data pribadi.



Gbr 1. Kerangka pemecahan masalah

Kegiatan direalisasikan melalui tiga tahap. Tahap persiapan meliputi koordinasi perizinan dengan sekolah, pengecekan sarana seperti ruang kelas, proyektor, dan akses internet, penyusunan materi dan lembar kerja simulasi, serta penyiapan instrumen evaluasi. Tahap pelaksanaan dibagi ke dalam beberapa sesi sebagaimana dirinci pada Tabel I. Tahap evaluasi meliputi pengolahan instrumen, rekapitulasi hasil simulasi surel jebakan, serta penyusunan laporan dan publikasi kegiatan.

Tabel I. Rincian sesi kegiatan

| Sesi      | Kegiatan                                                                           |
|-----------|------------------------------------------------------------------------------------|
| Pembukaan | Sosialisasi program dan urgensi literasi keamanan siber; pengisian <i>pre-test</i> |

| Sesi                            | Kegiatan                                                                                                                                                         |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sesi I: Pengenalan konsep       | Konsep dasar keamanan siber, jenis ancaman yang menasar pelajar, ciri pesan <i>phishing</i> , dan pola <i>social engineering</i>                                 |
| Sesi I: Anatomi <i>phishing</i> | Pembedahan skenario surel klaim <i>e-voucher</i> makanan dan minuman gratis palsu: pemicu emosi, formulir klaim palsu, dan pendataan isian formulir              |
| Sesi II: Simulasi terkendali    | Penilaian keaslian surel, pesan, dan tautan melalui lembar kerja; permainan peran <i>social engineering</i> ; praktik kata sandi kuat dan autentikasi dua faktor |
| Evaluasi                        | Pemaparan hasil simulasi surel jebakan, kuis interaktif, <i>post-test</i> , dan kuesioner kepuasan                                                               |

Pendekatan yang digunakan adalah pembelajaran aktif dengan metode ceramah interaktif, demonstrasi kasus, simulasi terkendali, permainan peran, serta praktik dan diskusi kelompok. Demonstrasi kasus menggunakan skenario surel klaim *e-voucher* makanan dan minuman gratis palsu yang mengatasnamakan merek kopi tiruan yang menyerupai kedai kopi ternama dengan gerai yang letaknya sangat dekat dari sekolah. Skenario ini dipilih agar terasa familiar bagi siswa dan proses klaim *voucher* terkesan mudah, sesuai dengan pola persuasi yang lazim dimanfaatkan pelaku rekayasa sosial [15]. Materi pengamanan akun mengacu pada pedoman identitas digital NIST yang menekankan kata sandi yang panjang dan unik serta autentikasi multifaktor [16].

Data dikumpulkan melalui empat instrumen, yaitu *pre-test* dan *post-test*, lembar kerja simulasi, simulasi surel jebakan, dan kuesioner kepuasan. Simulasi surel jebakan dilakukan dengan mengirimkan surel berisi tautan menuju formulir klaim *e-voucher* makanan dan minuman gratis tiruan yang dibuat menggunakan Google Formulir. Isian formulir direkap untuk menghitung jumlah siswa yang membuka tautan dan mengisi data, kemudian dianalisis secara deskriptif dalam bentuk frekuensi dan persentase menggunakan persamaan (1).

$$P = (n / N) \times 100\% \quad (1)$$

dengan  $P$  adalah persentase siswa yang mengisi data,  $n$  adalah jumlah siswa yang mengisi data pada formulir tiruan, dan  $N$  adalah jumlah surel yang berhasil terkirim. Seluruh bahan simulasi disiapkan oleh tim dan dijalankan secara terkendali. Data yang dimasukkan siswa pada formulir tiruan hanya digunakan untuk merekap jumlah siswa yang mengisi, tidak dipublikasikan, dan dihapus setelah rekapitulasi selesai.

*Pre-test* dan *post-test* menggunakan sepuluh soal pilihan ganda yang sama dan disajikan melalui Google Formulir. Setiap soal bernilai 10 poin sehingga skor maksimum adalah 100. Soal mencakup pengertian dan tujuan keamanan siber, pengertian *phishing*, data yang menjadi sasaran *phishing*, modus penipuan, perlakuan terhadap kode OTP, fungsi autentikasi multifaktor (MFA), pemeriksaan URL, pemilihan alamat yang aman, dan respons terhadap pesan hadiah. Satu pertanyaan tambahan tanpa skor mengukur keyakinan siswa dalam membedakan surel atau situs asli dan *phishing*. Hasil kedua tes dianalisis secara deskriptif melalui rata-rata, median, rentang skor, dan persentase jawaban benar per soal. Persentase jawaban benar dihitung dengan persamaan (1), dengan  $n$  sebagai jumlah siswa yang menjawab benar dan  $N$  sebagai jumlah responden.

### 3. HASIL

*Workshop* diikuti sekitar 50 siswa kelas X dan diawali dengan pembukaan serta pengisian *pre-test*. Pada sesi pertama, narasumber memaparkan konsep dasar keamanan siber, jenis ancaman yang kerap menyasar pelajar, serta ciri pesan *phishing*, mulai dari alamat pengirim, nada pesan, hingga tautan tujuan. Siswa juga dikenalkan pada pola manipulasi *social engineering*, seperti urgensi palsu, iming-iming hadiah, dan penyamaran sebagai pihak berwenang.

Materi dilanjutkan dengan pembedahan anatomi *phishing* melalui skenario surel klaim *e-voucher* makanan dan minuman gratis palsu. Tiga tahap serangan diuraikan, yaitu memancing emosi korban dengan iming-iming hadiah instan, mengarahkan korban ke situs palsu berupa formulir klaim *e-voucher* yang harus diisi, dan mendata kredensial seperti alamat surel yang dimasukkan korban pada halaman hasil pengisian formulir yang dikelola tim pelaksana. Pada sesi kedua, siswa menilai keaslian sejumlah contoh surel, pesan singkat, dan tautan melalui lembar kerja simulasi, mengikuti permainan peran skenario *social engineering*, berlatih menyusun kata sandi yang kuat, mempraktikkan pengaktifan autentikasi dua faktor, dan mendiskusikan langkah yang perlu diambil apabila terlanjur menjadi korban. Dokumentasi setiap sesi disajikan pada bagian Dokumentasi Kegiatan.

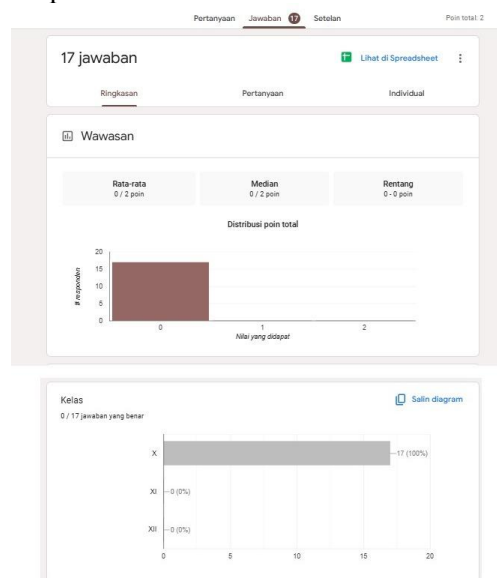
Hasil simulasi surel jebakan disajikan pada Tabel II. Dari 35 surel yang berhasil terkirim, 17 siswa (48,6%) membuka tautan palsu dan mengisikan data pada formulir tiruan tanpa memeriksa keasliannya terlebih dahulu, sedangkan 18 siswa (51,4%) tidak mengisikan data. Dengan

kata lain, hampir separuh siswa penerima surel terpancing oleh tawaran instan yang terasa familiar.

Tabel II. Hasil simulasi surel jebakan

| Keterangan                                          | Jumlah | Persentase |
|-----------------------------------------------------|--------|------------|
| Surel jebakan yang berhasil terkirim                | 35     | 100%       |
| Siswa yang membuka tautan palsu dan mengisikan data | 17     | 48,6%      |
| Siswa yang tidak mengisikan data                    | 18     | 51,4%      |

Formulir jebakan berupa klaim *e-voucher* makanan dan minuman gratis mencatat 17 respons yang seluruhnya berasal dari siswa kelas X (Gbr. 2). Jumlah ini sama dengan jumlah siswa yang terjebak pada Tabel II. Alamat surel yang tercatat pada formulir tidak dicantumkan untuk menjaga privasi peserta.



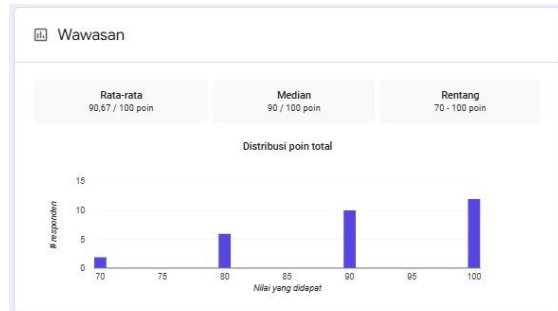
Gbr 2. Rekap respons formulir jebakan klaim *e-voucher* makanan dan minuman gratis

Hasil tersebut dipaparkan langsung di hadapan peserta pada akhir kegiatan sebagai bahan refleksi bersama, kemudian dilanjutkan dengan kuis interaktif, *post-test*, dan kuesioner kepuasan. Rekapitulasi lembar kerja dan kuesioner kepuasan didokumentasikan oleh tim sebagai bahan tindak lanjut bersama sekolah mitra, sedangkan analisis kuantitatif dalam artikel ini difokuskan pada hasil simulasi surel jebakan serta hasil *pre-test* dan *post-test*.

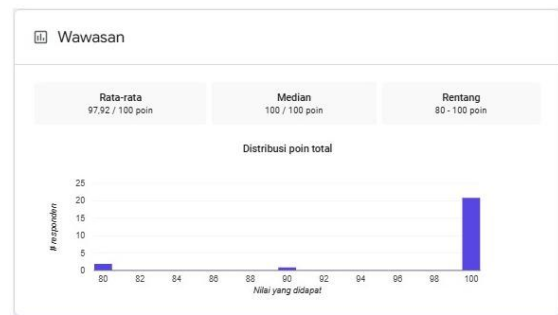
*Pre-test* dikerjakan oleh 30 siswa sebelum materi disampaikan, sedangkan *post-test* dikerjakan oleh 24 siswa setelah seluruh sesi selesai. Seluruh responden kedua tes merupakan siswa kelas X. Ringkasan hasil kedua tes disajikan pada Tabel III, sedangkan distribusi skornya ditunjukkan pada Gbr. 3.

Tabel III. Ringkasan hasil pre-test dan post-test

| Indikator           | Pre-test   | Post-test  |
|---------------------|------------|------------|
| Jumlah responden    | 30         | 24         |
| Rata-rata skor      | 90,67      | 97,92      |
| Median              | 90         | 100        |
| Rentang skor        | 70–100     | 80–100     |
| Skor sempurna (100) | 12 (40,0%) | 21 (87,5%) |
| Skor di bawah 80    | 2 (6,7%)   | 0 (0,0%)   |



(a) Pre-test



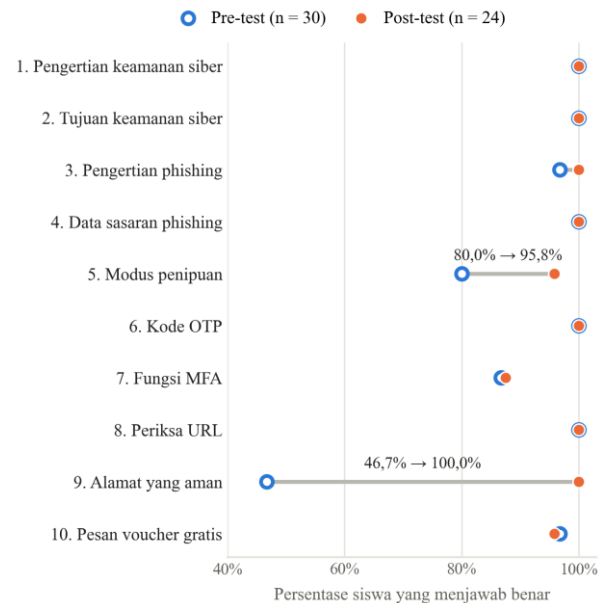
(b) Post-test

Gbr 3. Ringkasan skor pada Google Formulir: (a) pre-test dan (b) post-test

Rata-rata skor meningkat dari 90,67 menjadi 97,92 atau naik 7,25 poin (8,0%). Median naik dari 90 menjadi 100, skor terendah naik dari 70 menjadi 80, dan proporsi siswa dengan skor sempurna naik dari 40,0% menjadi 87,5%. Persentase jawaban benar per soal disajikan pada Tabel IV dan Gbr. 4.

Tabel IV. Persentase jawaban benar per soal (%)

| No | Materi soal                  | Pre          | Post         | Selisih      |
|----|------------------------------|--------------|--------------|--------------|
| 1  | Pengertian keamanan siber    | 100,0        | 100,0        | 0,0          |
| 2  | Tujuan keamanan siber        | 100,0        | 100,0        | 0,0          |
| 3  | Pengertian <i>phishing</i>   | 96,7         | 100,0        | +3,3         |
| 4  | Data sasaran <i>phishing</i> | 100,0        | 100,0        | 0,0          |
| 5  | Modus penipuan               | 80,0         | 95,8         | +15,8        |
| 6  | Perlakuan kode OTP           | 100,0        | 100,0        | 0,0          |
| 7  | Fungsi MFA                   | 86,7         | 87,5         | +0,8         |
| 8  | Pemeriksaan URL              | 100,0        | 100,0        | 0,0          |
| 9  | Pemilihan alamat aman        | 46,7         | 100,0        | +53,3        |
| 10 | Respons pesan <i>voucher</i> | 96,7         | 95,8         | -0,9         |
|    | <b>Rata-rata skor</b>        | <b>90,67</b> | <b>97,92</b> | <b>+7,25</b> |



Gbr 4. Perbandingan persentase jawaban benar per soal pada pre-test dan post-test

Peningkatan terbesar terjadi pada soal nomor 9 tentang pemilihan alamat yang lebih aman, yaitu dari 46,7% menjadi 100%. Pada *pre-test*, 15 siswa (50,0%) justru memilih <https://instagram.login-update.com> sebagai alamat yang aman. Soal nomor 5 tentang modus penipuan naik dari 80,0% menjadi 95,8%, soal nomor 7 tentang fungsi MFA relatif tetap (86,7% menjadi 87,5%), dan soal nomor 10 sedikit turun karena satu siswa memilih langsung mengklik tautan. Selain itu, siswa yang menyatakan sangat yakin atau yakin dapat membedakan surel atau situs asli dan *phishing* naik dari 76,7% menjadi 91,7%, sedangkan siswa yang kurang yakin turun dari 23,3% menjadi 8,3%.

#### 4. PEMBAHASAN

Persentase siswa yang mengisikan data sebesar 48,6% menunjukkan bahwa tawaran instan masih efektif mengalahkan kewaspadaan siswa. Temuan ini konsisten dengan kajian yang menunjukkan bahwa kelompok usia muda lebih rentan terhadap *phishing* [5] dan bahwa remaja cenderung merespons pesan yang menjanjikan hadiah tanpa verifikasi [8]. Skenario klaim *e-voucher* makanan dan minuman gratis memanfaatkan dua daya tarik sekaligus, yaitu hadiah dan rasa familiar terhadap merek yang dekat dengan keseharian siswa, yang merupakan pola persuasi khas rekayasa sosial [3], [15]. Kecenderungan pengguna menilai keaslian dari tampilan halaman, bukan dari alamat tautan [6], menjelaskan mengapa formulir tiruan yang tampak meyakinkan cukup untuk mendorong siswa mengisikan data.

Temuan tersebut juga menegaskan bahwa imbauan normatif saja tidak cukup. Pengetahuan tentang keamanan informasi perlu diterjemahkan menjadi sikap dan perilaku [17], sementara sifat impulsif dalam merespons pesan berkaitan dengan perilaku keamanan siber yang berisiko [7]. Pemaparan hasil simulasi secara langsung memberi siswa pengalaman nyata tentang titik kelengahan mereka sendiri. Pendekatan ini sejalan dengan pelatihan yang disisipkan pada konteks nyata [9] dan pelatihan berbasis *mindfulness* yang mendorong pengguna berhenti sejenak sebelum merespons pesan [10]. Hasil kegiatan ini juga sejalan dengan kegiatan pengabdian berbasis simulasi dan praktik yang dilaporkan meningkatkan kesadaran keamanan siber siswa [13], [14].

Hasil *pre-test* dan simulasi surel jebakan juga menunjukkan adanya kesenjangan antara pengetahuan dan perilaku. Skor awal siswa sudah tinggi dan seluruh responden mengetahui bahwa URL perlu diperiksa sebelum tautan diklik, tetapi hampir separuh penerima surel tetap mengisi formulir klaim *e-voucher*. Pengetahuan tersebut belum otomatis menjadi kebiasaan memverifikasi ketika siswa dihadapkan langsung pada tawaran yang menarik sehingga latihan berbasis simulasi tetap diperlukan. Kesalahan dominan pada soal pemilihan alamat yang aman menguatkan temuan bahwa pengguna cenderung menilai keaslian dari tampilan dan nama merek yang dikenal, bukan dari domain sebenarnya [6], dan kesalahan tersebut tidak muncul lagi pada *post-test* setelah anatomi *phishing* dibahas. Kenaikan rata-rata skor dalam kegiatan ini lebih kecil daripada kegiatan serupa [13] karena skor awal siswa sudah mendekati maksimum, tetapi peningkatan pada indikator yang paling lemah menunjukkan bahwa materi yang diberikan tepat sasaran.

Penguatan perilaku juga dilakukan melalui praktik pengamanan akun. Autentikasi dua faktor tetap melindungi akun meskipun kredensial telah bocor melalui *phishing* karena pelaku masih membutuhkan faktor kedua yang dimiliki korban [16]. Dari sisi etika, simulasi dirancang sepenuhnya edukatif: bahan disiapkan oleh tim dan data isian siswa hanya digunakan untuk rekapitulasi jumlah, tidak dipublikasikan, dan dihapus setelah rekapitulasi selesai. Keterbatasan kegiatan ini adalah pengukuran yang dilakukan pada satu waktu sehingga perubahan perilaku jangka panjang belum dapat diamati. Selain itu, jumlah responden *post-test* lebih sedikit daripada *pre-test* dan kedua tes tidak dipasangkan per individu sehingga

perbandingan hanya dapat dilakukan pada tingkat kelompok.

## 5. KESIMPULAN

Berdasarkan pelaksanaan dan hasil kegiatan, dapat disimpulkan hal-hal berikut.

1. *Workshop* literasi keamanan siber telah terlaksana pada 25 September 2026 di SMA Sejahtera 1 Depok dengan sekitar 50 siswa kelas X sebagai peserta melalui sesi edukasi konsep dan sesi simulasi terkendali.
2. Simulasi surel jebakan menunjukkan bahwa 17 dari 35 siswa (48,6%) membuka tautan palsu dan mengisikan data tanpa verifikasi. Hasil ini menunjukkan kerentanan siswa terhadap *phishing* berbasis tawaran instan yang terasa familiar, sekaligus menjadi bahan refleksi yang menyadarkan siswa akan kerentanan tersebut.
3. Pemahaman siswa meningkat setelah kegiatan, ditunjukkan oleh kenaikan rata-rata skor dari 90,67 pada *pre-test* menjadi 97,92 pada *post-test* serta kenaikan ketepatan memilih alamat yang aman dari 46,7% menjadi 100%. Meski demikian, tingginya skor *pre-test* yang disertai banyaknya siswa yang terjebak menunjukkan bahwa pengetahuan perlu diperkuat dengan latihan berbasis simulasi.
4. Siswa telah dibekali praktik pengamanan akun yang mendasar, meliputi penyusunan kata sandi yang kuat, pengaktifan autentikasi dua faktor, dan langkah yang perlu diambil apabila menjadi korban.

Pengembangan selanjutnya disarankan mencakup pengukuran lanjutan beberapa waktu setelah kegiatan untuk melihat perubahan perilaku jangka panjang, pelibatan guru dan orang tua, integrasi materi literasi keamanan siber ke dalam pembelajaran Informatika atau layanan Bimbingan Konseling, serta penyusunan prosedur persetujuan tertulis dari sekolah sebelum menjalankan simulasi surel jebakan.

## UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada SMA Sejahtera 1 Depok atas kesempatan dan dukungan selama pelaksanaan kegiatan, kepada seluruh siswa yang telah berpartisipasi aktif, serta kepada Ketua Program Studi Teknik Informatika S-2 Universitas Pamulang, Dr. Sajarwo Anggai, S.ST., M.T., atas dukungan terhadap kegiatan ini.

## DOKUMENTASI KEGIATAN

Pada sesi pemaparan, tim menyampaikan materi konsep keamanan siber dan menjawab pertanyaan siswa (Gbr. 5).



Gbr 5. Tim PKM menyampaikan materi dan menjawab pertanyaan siswa

Anatomi serangan dibedah melalui materi “Membedah Anatomi Simulasi Phishing” dengan skenario surel klaim *e-voucher* makanan dan minuman gratis palsu (Gbr. 6).



Gbr 6. Pemaparan anatomi simulasi phishing dengan skenario surel klaim *e-voucher* makanan dan minuman gratis palsu

Pada sesi simulasi terkendali, siswa menganalisis contoh pesan *phishing* yang meminta “verifikasi akun” (Gbr. 7).



Gbr 7. Siswa menganalisis contoh pesan phishing yang meminta “verifikasi akun”

Hasil simulasi surel jebakan dipaparkan kepada peserta sebagai bahan refleksi bersama (Gbr. 8).



Gbr 8. Pemaparan hasil evaluasi simulasi phishing kepada peserta

Kegiatan ditutup dengan foto bersama tim pelaksana dan siswa SMA Sejahtera 1 Depok (Gbr. 9).



Gbr 9. Tim PKM berfoto bersama siswa SMA Sejahtera 1 Depok usai kegiatan

## DAFTAR PUSTAKA

- [1] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing attacks: A recent comprehensive study and a new anatomy,” *Front. Comput. Sci.*, vol. 3, Art. no. 563060, 2021, doi: 10.3389/fcomp.2021.563060.
- [2] F. Salahdine and N. Kaabouch, “Social engineering attacks: A survey,” *Future Internet*, vol. 11, no. 4, Art. no. 89, 2019, doi: 10.3390/fi11040089.
- [3] C. Hadnagy, *Social Engineering: The Science of Human Hacking*, 2nd ed. Indianapolis, IN, USA: Wiley, 2018.
- [4] K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, IN, USA: Wiley, 2002.
- [5] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, “Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions,” in *Proc. SIGCHI Conf. Human Factors Comput. Syst. (CHI '10)*, Atlanta, GA, USA, 2010, pp. 373–382, doi: 10.1145/1753326.1753383.

- [6] M. Alsharnouby, F. Alaca, and S. Chiasson, "Why phishing still works: User strategies for combating phishing attacks," *Int. J. Hum.-Comput. Stud.*, vol. 82, pp. 69–82, 2015, doi: 10.1016/j.ijhcs.2015.05.005.
- [7] L. Hadlington, "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours," *Heliyon*, vol. 3, no. 7, Art. no. e00346, 2017, doi: 10.1016/j.heliyon.2017.e00346.
- [8] A. A. J. Arsyad, U. Tamrin, J. P. Lande, and N. Umar, "Meningkatkan kesadaran remaja terhadap phishing melalui literasi digital: Studi kasus di SMK Darussalam Makassar," *Jurnal Pengabdian Literasi Digital Indonesia*, vol. 3, no. 2, pp. 60–71, 2024, doi: 10.57119/abdimas.v3i2.122.
- [9] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching Johnny not to fall for phish," *ACM Trans. Internet Technol.*, vol. 10, no. 2, pp. 1–31, 2010, doi: 10.1145/1754393.1754396.
- [10] M. L. Jensen, M. Dinger, R. T. Wright, and J. B. Thatcher, "Training to mitigate phishing attacks using mindfulness techniques," *J. Manage. Inf. Syst.*, vol. 34, no. 2, pp. 597–626, 2017, doi: 10.1080/07421222.2017.1334499.
- [11] E. W. Tyas Darmaningrat et al., "Sosialisasi bahaya dan upaya pencegahan social engineering untuk meningkatkan kesadaran masyarakat tentang keamanan informasi," *Sewagati*, vol. 6, no. 2, pp. 159–168, 2022, doi: 10.12962/j26139960.v6i2.92.
- [12] J. Maulindar and D. Hartanti, "Pelatihan perlindungan data pribadi dan keamanan siber untuk siswa SMK Negeri 2 Surakarta," *Madaniya*, vol. 4, no. 4, pp. 1851–1856, 2023. [Online]. Available: <https://madaniya.pustaka.my.id/journals/contents/article/view/652>
- [13] M. Patria et al., "Edukasi keamanan siber sebagai upaya preventif terhadap ancaman phishing pada siswa SMA Islam Tambora Jakarta Barat," *Al Hayat: Jurnal Pengabdian Masyarakat*, vol. 4, no. 1, pp. 65–74, 2026, doi: 10.62588/ahjpm.2026.v4i1.274.
- [14] A. Wijayanto et al., "Peningkatan kesadaran keamanan siber siswa SMK melalui pelatihan dan simulasi serangan dalam lingkungan virtual," *BERBAKTI: Jurnal Pengabdian kepada Masyarakat*, vol. 3, no. 3, pp. 278–285, 2026, doi: 10.30822/hj4rr981.
- [15] R. B. Cialdini, *Influence: The Psychology of Persuasion*, rev. ed. New York, NY, USA: Harper Business, 2006.
- [16] P. A. Grassi et al., "Digital identity guidelines: Authentication and lifecycle management," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Spec. Publ. 800-63B, 2017, doi: 10.6028/NIST.SP.800-63b.
- [17] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, 2017, doi: 10.1016/j.cose.2017.01.004.