

Edukasi Keamanan Digital untuk Meningkatkan Pemahaman Guru SMK Negeri 6 Makassar dalam Mencegah Penipuan Online

¹Erick Irawadi Alwi, ²Jasmaniar

^{1,2}Universitas Muslim Indonesia, Indonesia

¹erick.alwi@umi.ac.id, ²jasmaniar.jasmaniar@umi.ac.id

*Correspondence Email: erick.alwi@umi.ac.id

Abstrak: Transformasi digital dalam lingkungan pendidikan meningkatkan intensitas penggunaan internet, telepon pintar, aplikasi komunikasi, dan berbagai platform digital oleh guru, sekaligus memperbesar risiko penipuan online yang dapat mengancam keamanan data dan akun. Kegiatan Pengabdian kepada Masyarakat ini bertujuan meningkatkan pemahaman guru SMK Negeri 6 Makassar mengenai keamanan digital serta kemampuan mengenali dan mencegah berbagai modus penipuan online. Kegiatan dilaksanakan dengan pendekatan edukatif, partisipatif, dan berbasis pengalaman melalui penyampaian materi, diskusi, berbagi pengalaman, simulasi kasus, serta evaluasi menggunakan pre-test dan post-test. Peserta kegiatan berjumlah 22 orang guru. Materi meliputi konsep keamanan digital, perlindungan data pribadi, keamanan akun, identifikasi penipuan online, phishing, social engineering, tautan berbahaya, aplikasi palsu, dan praktik penggunaan perangkat digital secara aman. Hasil evaluasi menunjukkan bahwa rata-rata nilai pre-test peserta sebesar 60,68, sedangkan rata-rata nilai post-test meningkat menjadi 85,23. Selisih kedua nilai tersebut mencapai 24,55 poin atau peningkatan sebesar 40,45% dibandingkan nilai awal. Hasil tersebut menunjukkan bahwa kegiatan edukasi memberikan perubahan positif terhadap pemahaman guru dalam mengenali ancaman dan menentukan tindakan pencegahan yang tepat. Pemberian buku literasi digital juga menjadi luaran pendukung untuk memperkuat keberlanjutan pembelajaran. Kegiatan ini menunjukkan bahwa edukasi, diskusi, simulasi, dan evaluasi dapat menjadi strategi penguatan kapasitas guru sebagai pengguna teknologi sekaligus agen literasi digital di lingkungan sekolah.

Kata kunci: Keamanan Digital, Literasi Digital, Penipuan Online, Edukasi, Guru.

PENDAHULUAN

Transformasi digital telah menjadi bagian integral dari penyelenggaraan pendidikan karena internet, telepon pintar, aplikasi komunikasi, dan berbagai platform digital semakin terintegrasi dalam aktivitas sekolah di lingkungan pendidikan. Perubahan tersebut terlihat melalui penggunaan internet untuk mengakses sumber pembelajaran, smartphone untuk komunikasi, aplikasi pesan untuk koordinasi, serta berbagai layanan digital untuk mendukung aktivitas akademik dan administratif. Teknologi digital juga memungkinkan guru mengembangkan pembelajaran yang lebih fleksibel melalui pemanfaatan sumber belajar daring, media interaktif, dan aplikasi pendukung pembelajaran. Pemanfaatan tersebut memperluas ruang interaksi antara guru dan peserta didik, sekaligus mempercepat pertukaran informasi dalam lingkungan sekolah.

Perkembangan kompetensi digital guru menjadi kebutuhan penting karena kemampuan menggunakan teknologi tidak hanya berkaitan dengan aspek teknis, tetapi juga kemampuan mengelola informasi, memahami risiko, serta menerapkan penggunaan teknologi secara bertanggung jawab (Tzafilkou et al., 2023; Wohlfart & Wagner, 2023).

Pemanfaatan teknologi digital dalam pendidikan memperluas akses terhadap sumber belajar, mempercepat komunikasi, serta mendukung pengelolaan pembelajaran dan administrasi sekolah secara lebih fleksibel yang semakin dinamis. Internet dan perangkat digital memungkinkan guru memperoleh informasi secara cepat, berkomunikasi dengan peserta didik dan rekan kerja, menyimpan dokumen, serta menggunakan berbagai aplikasi untuk mendukung pekerjaan profesional. Kompetensi digital guru menjadi bagian penting dari transformasi tersebut karena penggunaan teknologi dalam pendidikan tidak berhenti pada kemampuan mengoperasikan perangkat. Kajian sistematis terhadap kompetensi digital guru menunjukkan bahwa kemampuan tersebut mencakup penggunaan teknologi untuk perencanaan pembelajaran, praktik pengajaran, aktivitas peserta didik, pengembangan keterampilan abad ke-21, dan penguatan kompetensi digital peserta didik (Claro et al., 2024). Kondisi tersebut menunjukkan bahwa pengembangan kompetensi guru perlu ditempatkan dalam konteks penggunaan teknologi yang aman, kritis, dan bertanggung jawab.

Perluasan penggunaan teknologi digital membawa konsekuensi berupa meningkatnya paparan pengguna terhadap ancaman keamanan informasi yang dapat mengganggu privasi, kerahasiaan data, dan keselamatan aktivitas digital dalam ruang pendidikan. Penggunaan internet dan perangkat digital dapat membuka peluang terjadinya penipuan online, pencurian identitas, penyalahgunaan data pribadi, phishing, social engineering, smishing, tautan berbahaya, serta aplikasi palsu. Phishing secara khusus memanfaatkan teknik manipulasi untuk memperoleh informasi sensitif melalui pesan, tautan, atau halaman digital yang menyerupai layanan resmi. Kajian mengenai kompetensi keamanan digital menunjukkan bahwa perlindungan data pribadi, pengelolaan identitas digital, keamanan perangkat, dan penggunaan teknologi secara etis merupakan bagian penting dari kompetensi keamanan digital (Torres-Hernández & Gallego-Arrufat, 2022). Ancaman tersebut memperlihatkan bahwa kemampuan menggunakan teknologi

perlu disertai kemampuan mengenali risiko dan menentukan respons yang tepat ketika menghadapi situasi mencurigakan.

Guru menempati posisi strategis dalam membangun ekosistem digital sekolah karena kompetensi mereka menentukan cara teknologi digunakan, dipahami, diajarkan, dan diterapkan secara aman oleh peserta didik. Guru merupakan pengguna teknologi sekaligus figur yang dapat membentuk kebiasaan digital peserta didik melalui praktik pembelajaran dan komunikasi sehari-hari. Literatur mengenai digitalisasi pendidikan menempatkan guru sebagai aktor sentral dalam proses integrasi teknologi di sekolah, sementara pengembangan literasi digital membutuhkan dukungan pengembangan profesional yang sesuai dengan konteks pekerjaan guru (Wohlfart & Wagner, 2023). Kompetensi keamanan digital juga perlu mendapat perhatian karena penelitian menunjukkan bahwa aspek keamanan, perlindungan data, privasi, dan penggunaan teknologi secara bertanggung jawab merupakan komponen penting dalam kompetensi digital pendidik (Torres-Hernández & Gallego-Arrufat, 2022). Guru yang memiliki pemahaman keamanan digital lebih baik memiliki landasan yang lebih kuat untuk membangun perilaku penggunaan teknologi yang aman di lingkungan sekolah.

Kondisi tersebut relevan dengan situasi SMK Negeri 6 Makassar yang telah memanfaatkan smartphone dan internet dalam aktivitas guru, pembelajaran, administrasi, serta komunikasi sekolah sehari-hari. Berdasarkan observasi awal dan komunikasi dengan pihak sekolah, penggunaan teknologi digital telah menjadi bagian dari aktivitas para guru, tetapi pemanfaatan tersebut belum sepenuhnya disertai pemahaman yang memadai mengenai keamanan digital dan pencegahan penipuan online. erick+JPKM+revisi Kondisi tersebut memperlihatkan adanya kebutuhan penguatan kapasitas guru agar penggunaan teknologi tidak hanya efektif untuk mendukung pekerjaan, tetapi juga aman dari berbagai bentuk ancaman digital. Kebutuhan tersebut menjadi semakin relevan ketika guru berinteraksi secara intensif dengan peserta didik yang memiliki tingkat penggunaan teknologi tinggi. Penguatan kompetensi keamanan digital guru dapat mendukung terbentuknya kebiasaan digital yang lebih aman serta memperkuat fungsi guru sebagai agen literasi digital di lingkungan sekolah.



Kegiatan edukasi keamanan digital perlu diarahkan pada kebutuhan praktis pengguna agar pemahaman mengenai ancaman siber dapat diterjemahkan menjadi kemampuan mengenali risiko dan mengambil tindakan pencegahan. Program pengabdian sebelumnya telah memberikan perhatian terhadap literasi digital, penggunaan media sosial secara bijak, perlindungan privasi, dan pengenalan ancaman siber. Draft kegiatan ini menunjukkan bahwa kebutuhan mitra lebih spesifik pada kemampuan mengenali modus penipuan online melalui contoh nyata, termasuk pesan phishing, tautan berbahaya, aplikasi palsu, dan teknik social engineering. erick+JPKM+revisi Pendekatan edukasi yang mengintegrasikan penyampaian materi dengan diskusi, simulasi kasus, dan latihan praktis memiliki relevansi kuat karena kajian tentang phishing education, training, and awareness menunjukkan pentingnya memperhatikan kesenjangan pengetahuan pengguna, faktor manusia, serta pendekatan pembelajaran yang sesuai dengan karakteristik peserta (Sarker et al., 2024).

Berdasarkan kondisi tersebut, kegiatan Pengabdian kepada Masyarakat ini bertujuan meningkatkan literasi keamanan digital guru SMK Negeri 6 Makassar dalam mengenali dan mencegah penipuan online secara kontekstual. Kegiatan diarahkan untuk memperkuat pemahaman mengenai konsep keamanan digital, perlindungan data pribadi, keamanan akun, identifikasi modus penipuan online, phishing, social engineering, tautan berbahaya, dan aplikasi palsu. erick+JPKM+revisi Kontribusi kegiatan tidak hanya diarahkan pada peningkatan pemahaman peserta, tetapi juga pada penguatan kesadaran guru sebagai pengguna teknologi dan agen literasi digital di sekolah. Pelaksanaan kegiatan melalui edukasi, diskusi, simulasi kasus, dan evaluasi diharapkan dapat memberikan pengalaman belajar yang aplikatif serta membantu guru menerapkan pengetahuan keamanan digital dalam aktivitas sehari-hari. Pendekatan tersebut juga memberikan dasar bagi terbentuknya budaya penggunaan teknologi yang lebih aman dan bertanggung jawab dalam lingkungan pendidikan. Dengan demikian, kegiatan ini menempatkan edukasi keamanan digital sebagai bagian dari penguatan kapasitas guru menghadapi risiko penipuan online di lingkungan sekolah.

METODE

Desain dan Pendekatan Kegiatan

Kegiatan pengabdian kepada masyarakat ini dirancang menggunakan pendekatan edukatif, partisipatif, dan berbasis pengalaman untuk membangun pemahaman keamanan digital melalui interaksi aktif seluruh peserta kegiatan secara terstruktur. Pendekatan tersebut dipilih karena kegiatan tidak diarahkan sebagai penyampaian materi satu arah, melainkan sebagai proses pembelajaran yang memberikan ruang kepada peserta untuk berdiskusi, berbagi pengalaman, mengidentifikasi permasalahan, serta melakukan latihan praktis. Peserta terlibat secara langsung dalam pembahasan kasus penipuan daring yang relevan dengan penggunaan teknologi dalam lingkungan sekolah. Kegiatan juga dilengkapi simulasi dan pendampingan agar peserta memperoleh pengalaman dalam mengenali karakteristik ancaman digital serta menentukan tindakan yang tepat. Pendekatan pembelajaran aktif melalui latihan dan pengalaman praktis relevan untuk meningkatkan kemampuan peserta dalam mengenali phishing dan ancaman rekayasa sosial (Marshall et al., 2024; Yasin et al., 2024).

Lokasi dan Peserta Kegiatan

Kegiatan dilaksanakan di SMK Negeri 6 Makassar dengan melibatkan 22 orang guru yang dipilih berdasarkan peran strategisnya sebagai pengguna teknologi digital sekaligus agen literasi digital. Guru menjadi sasaran kegiatan karena penggunaan perangkat digital dalam aktivitas pendidikan membutuhkan kompetensi keamanan yang memadai, terutama berkaitan dengan perlindungan informasi, pengelolaan akun, serta kemampuan mengenali ancaman digital. Kompetensi tersebut juga penting karena guru memiliki posisi strategis dalam membangun kebiasaan penggunaan teknologi yang aman bagi peserta didik. Penelitian mengenai kompetensi keamanan siber guru menunjukkan pentingnya penguasaan kemampuan untuk mengenali ancaman digital, melindungi informasi pribadi, menggunakan perangkat secara aman, serta memahami mekanisme autentikasi dan keamanan digital (de la Flor-Bancalero & Guillen-Gamez, 2026).

Tahapan Pelaksanaan Kegiatan

Pelaksanaan program disusun secara sistematis melalui tahapan identifikasi kebutuhan mitra, penyusunan materi, edukasi keamanan digital, diskusi, simulasi, post-test, serta analisis hasil

kegiatan secara menyeluruh dan terukur. Tahap identifikasi kebutuhan dilakukan untuk memperoleh gambaran awal mengenai pemahaman peserta terhadap keamanan digital dan potensi penipuan online yang dihadapi dalam penggunaan teknologi. Hasil identifikasi menjadi dasar penyusunan materi kegiatan agar sesuai dengan kebutuhan peserta. Tahap berikutnya berupa edukasi keamanan digital melalui penyampaian materi dan interaksi dengan peserta. Proses tersebut dilanjutkan dengan diskusi serta berbagi pengalaman mengenai permasalahan keamanan digital yang pernah ditemui. Simulasi kasus digunakan untuk memberikan pengalaman praktis dalam mengidentifikasi pesan mencurigakan, tautan berbahaya, serta pola komunikasi yang mengarah pada penipuan. Setelah seluruh sesi selesai, peserta mengikuti post-test untuk mengetahui perubahan pemahaman.

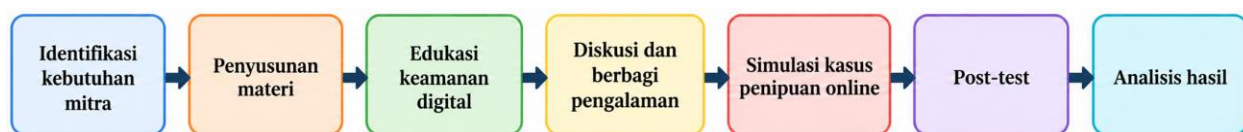


Figure 1. Alur pelaksanaan kegiatan

Materi Kegiatan

Materi kegiatan disusun berdasarkan kebutuhan penguatan kompetensi keamanan digital guru yang mencakup perlindungan data pribadi, keamanan akun, pencegahan penipuan, dan penggunaan perangkat digital secara aman. Materi mencakup konsep dasar keamanan digital, perlindungan data pribadi, keamanan akun, identifikasi modus penipuan online, phishing, *social engineering*, tautan berbahaya, aplikasi palsu, serta praktik penggunaan perangkat digital secara aman. Penyusunan materi diarahkan pada kemampuan praktis peserta dalam mengenali indikator ancaman dan menentukan respons yang tepat ketika menerima komunikasi atau informasi mencurigakan. Materi phishing diberikan melalui contoh kasus dan simulasi sehingga peserta dapat memahami pola manipulasi yang digunakan pelaku. Pendekatan edukasi phishing berbasis keterlibatan aktif dan latihan praktik dinilai dapat membantu meningkatkan kemampuan pengguna dalam mengenali ancaman digital (Marshall et al., 2024; Sarker et al., 2024).

Instrumen dan Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui observasi awal, dokumentasi kegiatan, serta pengukuran pemahaman peserta menggunakan pre-test sebelum kegiatan dan post-test setelah

seluruh sesi pembelajaran selesai dilaksanakan secara keseluruhan. Observasi awal digunakan untuk memperoleh gambaran kondisi dan kebutuhan peserta sebelum intervensi diberikan. Dokumentasi digunakan untuk merekam proses pelaksanaan kegiatan, termasuk aktivitas edukasi, diskusi, simulasi, dan pendampingan. Pre-test diberikan sebelum penyampaian materi untuk memperoleh gambaran tingkat pemahaman awal guru mengenai keamanan digital dan pencegahan penipuan online. Post-test diberikan setelah seluruh materi, diskusi, dan simulasi selesai untuk mengetahui perubahan pemahaman peserta. Data tersebut selanjutnya digunakan sebagai dasar evaluasi pencapaian kegiatan.

Teknik Analisis Data

Data hasil evaluasi dianalisis secara deskriptif kuantitatif dengan menghitung rata-rata skor, selisih nilai, dan persentase peningkatan pemahaman peserta setelah mengikuti keseluruhan program kegiatan secara lengkap. Rata-rata skor pre-test digunakan untuk menggambarkan kondisi pemahaman awal peserta, sedangkan rata-rata skor post-test digunakan untuk menunjukkan kondisi pemahaman setelah kegiatan. Selisih skor dihitung dengan membandingkan nilai rata-rata post-test dan pre-test. Persentase peningkatan digunakan untuk menunjukkan besarnya perubahan pemahaman peserta secara relatif terhadap skor awal. Analisis tersebut digunakan untuk memberikan gambaran objektif mengenai perubahan kemampuan peserta setelah memperoleh edukasi dan mengikuti simulasi keamanan digital. Prosedur analisis mengikuti rancangan evaluasi dalam kegiatan yang menggunakan perbandingan hasil sebelum dan sesudah pelaksanaan program.

HASIL DAN PEMBAHASAN

Pelaksanaan Kegiatan Edukasi

Kegiatan edukasi keamanan digital melibatkan 22 guru SMK Negeri 6 Makassar melalui penyampaian materi, diskusi, simulasi kasus penipuan online, dan evaluasi pemahaman peserta secara terstruktur selama kegiatan. Pelaksanaan kegiatan diarahkan untuk memperkuat kemampuan guru dalam mengenali berbagai bentuk ancaman digital yang berpotensi muncul dalam penggunaan perangkat, media sosial, aplikasi komunikasi, serta layanan internet. Materi

diberikan melalui pendekatan yang menggabungkan penjelasan konseptual dengan pengalaman praktis sehingga peserta memperoleh kesempatan untuk menghubungkan pengetahuan dengan persoalan yang mereka hadapi dalam aktivitas digital. Materi mencakup konsep keamanan digital, perlindungan data pribadi, keamanan akun, identifikasi modus penipuan online, *phishing*, *social engineering*, tautan berbahaya, aplikasi palsu, serta praktik penggunaan perangkat digital secara aman. Rangkaian tersebut sesuai dengan kebutuhan kegiatan karena keamanan digital tidak hanya berkaitan dengan kemampuan teknis, tetapi juga kemampuan pengguna dalam mengambil keputusan ketika berhadapan dengan informasi atau komunikasi yang mencurigakan.

Pelaksanaan kegiatan memperlihatkan keterlibatan peserta dalam proses pembelajaran melalui diskusi, tanggapan terhadap contoh kasus, dan penyampaian pengalaman mengenai penggunaan teknologi digital. Peserta diberikan berbagai contoh pesan mencurigakan, tautan palsu, serta modus penipuan yang dapat ditemukan melalui media sosial dan aplikasi komunikasi. Contoh tersebut digunakan untuk mengidentifikasi karakteristik komunikasi yang berpotensi mengandung unsur penipuan. Peserta diarahkan untuk memperhatikan isi pesan, sumber pengirim, bentuk tautan, permintaan informasi pribadi, serta tekanan waktu yang sering digunakan untuk mendorong korban segera mengambil keputusan. Pembahasan tersebut menjadi penting karena penelitian Butavicius et al. (2022) menunjukkan bahwa tekanan waktu dapat menurunkan akurasi seseorang dalam membedakan pesan *phishing* dari pesan yang sah. Temuan tersebut memperkuat relevansi penggunaan kasus yang menampilkan unsur urgensi dalam kegiatan edukasi keamanan digital.

Peserta juga dilibatkan dalam pembahasan mengenai *social engineering* yang menempatkan faktor manusia sebagai bagian penting dalam keberhasilan penipuan digital. Pelaku tidak selalu mengandalkan kelemahan teknis, tetapi dapat memanfaatkan kepercayaan, rasa takut, rasa ingin tahu, atau dorongan untuk segera merespons suatu informasi. Pemahaman mengenai pola manipulasi tersebut membantu peserta melihat bahwa keamanan digital membutuhkan kewaspadaan terhadap proses komunikasi, bukan hanya penggunaan perangkat lunak keamanan. Bullee dan Junger (2020), melalui meta-analisis terhadap 19 studi dengan 37 ukuran efek dan total 23.146 peserta, menemukan bahwa efektivitas intervensi terhadap kerentanan *social engineering*

berbeda-beda menurut karakteristik intervensinya. Intervensi dengan intensitas lebih tinggi dan fokus yang lebih sempit menunjukkan efektivitas yang lebih baik.



Gambar 2. Proses penyampaian materi edukasi penipuan online

Gambar 2 menunjukkan proses penyampaian materi yang dikombinasikan dengan diskusi dan pembahasan kasus. Interaksi tersebut memberikan ruang kepada peserta untuk mengklarifikasi konsep, menyampaikan pengalaman, dan menilai risiko berdasarkan contoh yang disediakan fasilitator. Proses pembelajaran menjadi lebih kontekstual karena peserta tidak hanya memperoleh definisi mengenai *phishing* atau *social engineering*, tetapi juga berlatih mengidentifikasi indikator ancaman. Pendekatan semacam ini sejalan dengan hasil penelitian Naqvi et al. (2023) yang menunjukkan bahwa strategi mitigasi *phishing* perlu mempertimbangkan kemampuan manusia sebagai bagian dari sistem pertahanan. Kajian tersebut juga menunjukkan bahwa pendekatan yang hanya mengandalkan solusi teknis tidak cukup untuk menghadapi persoalan *phishing* karena keputusan pengguna tetap menjadi bagian penting dalam proses perlindungan.

Hasil Evaluasi Pemahaman Peserta

Hasil evaluasi memperlihatkan perubahan pemahaman peserta setelah mengikuti rangkaian edukasi yang mencakup perlindungan data pribadi, keamanan akun, *phishing*, *social engineering*, tautan berbahaya, dan aplikasi palsu. Evaluasi dilakukan menggunakan *pre-test* sebelum kegiatan dan *post-test* setelah seluruh sesi edukasi, diskusi, serta simulasi selesai dilaksanakan. Sebanyak 22 guru mengikuti kedua tahap evaluasi sehingga data dapat dibandingkan berdasarkan jumlah peserta yang sama. Evaluasi tersebut digunakan untuk memperoleh gambaran perubahan pengetahuan peserta secara deskriptif. Data hasil evaluasi menjadi indikator utama pencapaian

kegiatan karena tujuan program diarahkan pada peningkatan pemahaman guru mengenai keamanan digital dan pencegahan penipuan online.

Tabel 1. Hasil Evaluasi Pemahaman Peserta Sebelum dan Sesudah Kegiatan

No.	Evaluasi	Jumlah Peserta	Nilai Rata-rata
1	Pre-test sebelum kegiatan	22 orang	60,68
2	Post-test setelah kegiatan	22 orang	85,23
3	Peningkatan pemahaman	22 orang	24,55

Tabel 1 menunjukkan bahwa nilai rata-rata *pre-test* peserta adalah 60,68, sedangkan nilai rata-rata *post-test* meningkat menjadi 85,23. Selisih kedua nilai tersebut mencapai 24,55 poin. Berdasarkan nilai awal, peningkatan tersebut setara dengan 40,45%. Hasil tersebut menunjukkan perubahan capaian pemahaman peserta setelah mengikuti kegiatan. Angka tersebut merupakan temuan utama program karena menunjukkan perbedaan yang cukup jelas antara kondisi pengetahuan sebelum dan sesudah intervensi edukatif.

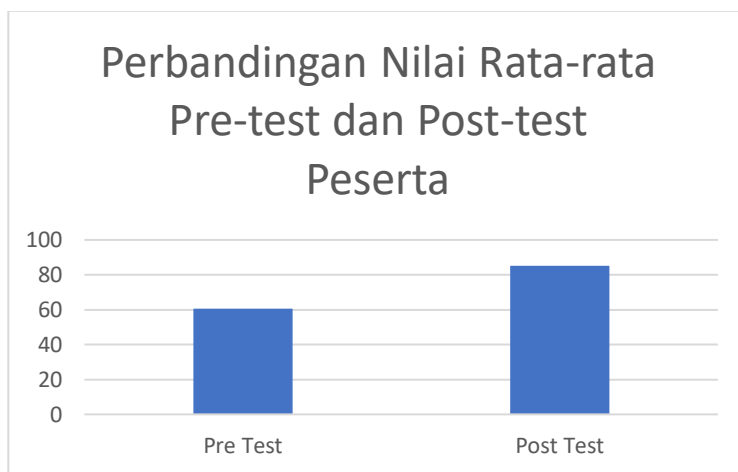
Hasil tersebut dapat dipahami dalam kerangka evaluasi pembelajaran keamanan siber yang menempatkan perubahan pengetahuan sebagai salah satu indikator penting keberhasilan intervensi. Khan et al. (2023) menunjukkan melalui evaluasi berbasis *Protection Motivation Theory* bahwa pelatihan keamanan siber dapat meningkatkan pengetahuan mengenai ancaman dan strategi penanggulangannya. Penelitian tersebut menggunakan desain *pre-test* dan *post-test* serta menunjukkan peningkatan pengetahuan peserta setelah pelatihan. Kesamaan pola tersebut memberikan dukungan konseptual terhadap hasil kegiatan di SMK Negeri 6 Makassar, meskipun karakteristik peserta dan konteks pelaksanaan kedua kegiatan berbeda.

Nilai *pre-test* sebesar 60,68 menunjukkan bahwa peserta telah memiliki pengetahuan awal mengenai penggunaan teknologi digital, tetapi pemahaman spesifik mengenai keamanan dan pencegahan penipuan masih membutuhkan penguatan. Kondisi tersebut menunjukkan bahwa kemampuan menggunakan teknologi tidak selalu identik dengan kemampuan melindungi diri dari ancaman digital. Pengguna dapat terbiasa menggunakan media sosial, aplikasi komunikasi, dan layanan internet tanpa secara konsisten melakukan pemeriksaan keamanan terhadap informasi yang diterima. Kajian Alsharida et al. (2023) memperlihatkan bahwa penelitian mengenai perilaku keamanan siber banyak menempatkan pengguna sebagai elemen penting dalam memahami

perilaku perlindungan digital. Kajian tersebut juga menemukan bahwa media sosial dan perangkat bergerak menjadi teknologi yang sering diteliti dalam konteks perilaku keamanan siber.

Peningkatan Pemahaman Guru

Perbandingan skor pre-test dan post-test menunjukkan peningkatan rata-rata pemahaman peserta setelah memperoleh materi, mengikuti diskusi, menyelesaikan simulasi, serta mendapatkan umpan balik dari fasilitator kegiatan. Rata-rata skor meningkat dari 60,68 menjadi 85,23 dengan selisih 24,55 poin. Perubahan tersebut menghasilkan persentase peningkatan sebesar 40,45% berdasarkan nilai awal. Peningkatan tersebut dapat dipandang sebagai indikator keberhasilan program pada tingkat pengetahuan karena peserta menunjukkan capaian evaluasi yang lebih tinggi setelah memperoleh intervensi edukatif. Hasil ini sekaligus memperlihatkan bahwa kegiatan yang menggabungkan materi konseptual dengan pengalaman praktis dapat memberikan perubahan positif terhadap pemahaman peserta.



Gambar 1. Perbandingan Nilai Rata-rata Pre-test dan Post-test Peserta

Gambar 1 memperlihatkan perbedaan nilai rata-rata melalui grafik batang. Nilai *post-test* berada pada posisi lebih tinggi dibandingkan nilai *pre-test*, sehingga arah perubahan pemahaman dapat diamati secara visual. Grafik tersebut memperkuat informasi yang disajikan pada Tabel 1 mengenai perubahan nilai peserta. Interpretasi terhadap peningkatan tersebut tetap ditempatkan dalam kerangka deskriptif karena data yang tersedia hanya mencakup nilai rata-rata, selisih, dan persentase perubahan. Tidak dilakukan pengujian statistik inferensial sehingga hasil tidak

digunakan untuk menyatakan hubungan kausal atau generalisasi terhadap populasi guru yang lebih luas.

Peningkatan pengetahuan juga relevan dengan kajian Sikolia et al. (2023) mengenai program *Security Education, Training, and Awareness* atau SETA. Penelitian tersebut menemukan bahwa program pelatihan dapat menurunkan kerentanan terhadap *phishing* dan meningkatkan pengetahuan keamanan siber, tetapi sebagian pengetahuan dapat mengalami penurunan dalam periode tertentu setelah pelatihan. Temuan tersebut memberikan implikasi bahwa peningkatan yang terlihat segera setelah kegiatan merupakan capaian penting, tetapi belum cukup untuk menyimpulkan bahwa perubahan tersebut akan bertahan dalam jangka panjang. Program penguatan dan pengulangan materi tetap diperlukan agar pengetahuan dapat dipertahankan.

Kondisi tersebut memberikan alasan akademik untuk menempatkan hasil kegiatan bukan hanya sebagai peningkatan nilai evaluasi, tetapi sebagai dasar pengembangan program keamanan digital berkelanjutan. Peserta perlu memperoleh kesempatan untuk mengulang pengetahuan, menghadapi variasi kasus, serta memperoleh umpan balik ketika melakukan kesalahan. Siklus pembelajaran tersebut dapat membantu mengubah pengetahuan menjadi kemampuan yang lebih stabil. Singh et al. (2023) menunjukkan bahwa desain pelatihan *anti-phishing* perlu memperhatikan proses belajar dan pengambilan keputusan manusia. Penelitian tersebut menemukan bahwa frekuensi paparan terhadap contoh *phishing* dan pemberian umpan balik yang lebih rinci dapat memengaruhi kemampuan peserta membedakan pesan phishing dan pesan yang sah.

Analisis Efektivitas Edukasi Keamanan Digital

Peningkatan pemahaman peserta memperlihatkan bahwa edukasi keamanan digital memberikan kontribusi positif terhadap kemampuan guru memahami ancaman dan menentukan tindakan pencegahan dalam penggunaan teknologi sehari-hari secara lebih aman. Efektivitas kegiatan dalam konteks pengabdian ini dapat dilihat melalui keterkaitan antara kebutuhan peserta, materi yang diberikan, metode pembelajaran, serta perubahan hasil evaluasi. Materi disusun berdasarkan persoalan yang dekat dengan penggunaan teknologi sehari-hari, sedangkan metode pelaksanaan memberikan kesempatan kepada peserta untuk mendiskusikan dan mempraktikkan

pengetahuan tersebut. Kombinasi tersebut menghasilkan proses pembelajaran yang lebih aplikatif dibandingkan penyampaian informasi keamanan digital secara abstrak.

Kajian Naqvi et al. (2023) terhadap 248 artikel mengenai mitigasi *phishing* menunjukkan bahwa strategi perlindungan dapat dikelompokkan ke dalam pendekatan berbasis sistem, model atau kerangka kerja, serta strategi yang berpusat pada manusia. Kajian tersebut juga menekankan bahwa kemampuan pengguna perlu dipertimbangkan dalam pengembangan strategi mitigasi. Temuan tersebut relevan dengan kegiatan karena guru ditempatkan sebagai aktor utama yang perlu mampu mengenali ancaman sebelum menentukan tindakan. Edukasi tidak dimaksudkan menggantikan sistem keamanan teknis, tetapi melengkapi perlindungan teknis melalui peningkatan kapasitas pengguna.

Aspek pembelajaran berbasis pengalaman menjadi penting karena ancaman *phishing* tidak selalu memiliki ciri visual yang mudah dikenali. Safi dan Singh (2023) menunjukkan bahwa penelitian mengenai deteksi situs *phishing* telah berkembang melalui pendekatan berbasis daftar, kesamaan visual, heuristik, *machine learning*, dan *deep learning*. Perkembangan tersebut memperlihatkan bahwa deteksi teknis semakin kompleks. Pengguna tetap membutuhkan pengetahuan dasar agar tidak mengambil keputusan berisiko ketika menerima tautan atau mengakses halaman tertentu. Kegiatan edukasi memberikan dasar bagi guru untuk memahami bahwa pemeriksaan terhadap tautan, sumber informasi, dan permintaan data merupakan bagian dari perilaku digital yang aman.

Efektivitas kegiatan juga dapat dilihat dari relevansi materi dengan karakteristik perilaku pengguna. Alsharida et al. (2023) menunjukkan bahwa penelitian perilaku keamanan siber banyak menggunakan kerangka seperti *Protection Motivation Theory* dan *Theory of Planned Behavior*. Kerangka tersebut menunjukkan bahwa perilaku keamanan dipengaruhi oleh faktor kognitif dan motivasional, bukan semata-mata kemampuan teknis. Dalam kegiatan ini, peserta diberikan pengetahuan mengenai ancaman sekaligus kesempatan untuk mempertimbangkan konsekuensi tindakan ketika menerima pesan mencurigakan. Pemahaman mengenai risiko diharapkan dapat memperkuat kecenderungan peserta untuk memeriksa informasi sebelum mengambil keputusan.

Peran Simulasi dan Pembelajaran Berbasis Kasus

Simulasi kasus memberikan pengalaman pembelajaran yang memungkinkan peserta menguji pengetahuan keamanan digital melalui situasi yang menyerupai ancaman penipuan online dalam komunikasi sehari-hari di lingkungan kerja. Simulasi digunakan untuk menghadirkan kondisi yang lebih konkret daripada penjelasan teoritis mengenai *phishing*, *social engineering*, dan tautan berbahaya. Peserta diminta mengamati contoh, mengenali unsur yang mencurigakan, serta mempertimbangkan respons yang paling aman. Proses tersebut memberikan pengalaman pengambilan keputusan yang relevan dengan situasi penggunaan teknologi sehari-hari.

Singh et al. (2023) memberikan dukungan terhadap pentingnya desain pengalaman dalam pelatihan *anti-phishing*. Hasil eksperimen mereka menunjukkan bahwa frekuensi paparan terhadap contoh *phishing* dapat membentuk sensitivitas peserta, sementara umpan balik terperinci membantu peserta membedakan pesan *phishing* dan pesan yang sah secara lebih baik. Temuan tersebut memberikan dasar bahwa simulasi sebaiknya tidak berhenti pada aktivitas identifikasi benar atau salah. Peserta juga perlu memperoleh penjelasan mengenai alasan suatu pesan dianggap berbahaya sehingga terbentuk proses belajar yang lebih mendalam.

Diskusi setelah simulasi memberikan ruang bagi peserta untuk menjelaskan alasan sebuah pesan dianggap mencurigakan, membandingkan pendapat, dan memperoleh klarifikasi mengenai tindakan pencegahan yang tepat. Diskusi memungkinkan fasilitator mengetahui bagian materi yang masih menimbulkan keraguan. Peserta dapat menyampaikan pengalaman yang tidak selalu sama sehingga muncul variasi contoh ancaman yang dapat dibahas bersama. Interaksi tersebut juga membantu membangun kesadaran bahwa keamanan digital merupakan persoalan bersama dalam lingkungan sekolah.

Bullee dan Junger (2020) menemukan bahwa intervensi untuk mengurangi kerentanan terhadap *social engineering* menunjukkan variasi efektivitas berdasarkan karakteristik program. Intervensi yang lebih intensif dan memiliki fokus lebih sempit cenderung memberikan efek lebih kuat. Temuan tersebut relevan dengan rancangan kegiatan yang memusatkan materi pada penipuan online, *phishing*, *social engineering*, tautan berbahaya, dan aplikasi palsu. Fokus tersebut membuat peserta tidak dibebani terlalu banyak topik keamanan siber yang tidak berhubungan langsung dengan kebutuhan kegiatan.

Luaran Pendukung dan Keberlanjutan Program

Luaran berupa buku literasi digital memberikan dukungan terhadap keberlanjutan program karena peserta memperoleh sumber belajar yang dapat digunakan kembali setelah kegiatan pengabdian selesai dilaksanakan. Buku “Literasi Digital: Panduan Aman dan Cerdas di Era Digital” diberikan kepada seluruh peserta sebagai sumber bacaan lanjutan mengenai penggunaan teknologi secara aman. Pemberian buku tersebut memperluas manfaat kegiatan karena proses belajar tidak berhenti ketika sesi edukasi berakhir. Peserta dapat menggunakan buku untuk mengingat kembali materi, memperdalam pemahaman, dan mendiskusikan informasi keamanan digital dengan rekan kerja.



Gambar 3. Pemberian buku literasi digital kepada peserta

Gambar 3 menunjukkan pemberian buku kepada peserta sebagai bagian dari luaran kegiatan. Bahan bacaan tersebut dapat digunakan sebagai sumber belajar mandiri dan referensi dalam pengembangan literasi digital di lingkungan sekolah. Keberadaan bahan belajar juga memberikan peluang untuk mengembangkan kegiatan lanjutan tanpa harus memulai materi dari awal. Guru dapat menggunakan buku sebagai sumber diskusi dalam komunitas belajar atau kegiatan pengembangan kompetensi internal.

Keberlanjutan tersebut penting karena kesadaran keamanan informasi merupakan konstruk yang bersifat multidimensional. Rohan et al. (2023), melalui tinjauan terhadap 24 penelitian mengenai pengukuran *information security awareness*, menunjukkan bahwa kesadaran keamanan

informasi mencakup berbagai dimensi dan membutuhkan instrumen pengukuran yang memiliki kualitas konseptual dan metodologis memadai. Temuan tersebut memperlihatkan bahwa penguatan keamanan digital sebaiknya tidak direduksi menjadi satu kemampuan saja. Pengguna perlu memahami berbagai aspek yang berkaitan dengan ancaman, perlindungan informasi, perilaku, serta pengambilan keputusan.

Peran Guru sebagai Agen Literasi Keamanan Digital

Peran guru sebagai penerima manfaat sekaligus agen literasi digital memberikan peluang perluasan dampak program melalui penerapan pengetahuan dan penyebaran praktik keamanan kepada peserta didik di sekolah. Guru berada pada posisi strategis karena aktivitas profesional mereka berkaitan dengan penggunaan perangkat digital, pengelolaan informasi, komunikasi dengan peserta didik dan orang tua, serta pemanfaatan berbagai platform pembelajaran. Pengetahuan yang diperoleh melalui kegiatan dapat diterapkan dalam praktik sehari-hari dan dikembangkan menjadi kebiasaan keamanan digital dalam lingkungan sekolah.

Khan et al. (2022) menunjukkan bahwa penelitian perilaku keamanan siber berkembang secara signifikan, tetapi masih terdapat kebutuhan untuk memperkuat pengembangan teori dan konsistensi metodologis dalam penelitian mengenai aspek manusia. Temuan tersebut menegaskan bahwa keamanan siber tidak dapat dipahami hanya melalui teknologi. Perilaku pengguna menjadi bagian penting yang perlu mendapat perhatian. Dalam konteks sekolah, guru dapat menjadi aktor yang menghubungkan kebijakan keamanan digital dengan praktik penggunaan teknologi sehari-hari.

Penerapan pengetahuan guru kepada peserta didik dapat dilakukan melalui pembiasaan sederhana, seperti tidak membagikan kata sandi, memeriksa sumber pesan, menghindari tautan mencurigakan, menjaga informasi pribadi, serta melaporkan aktivitas digital yang tidak wajar. Penguatan tersebut dapat dilakukan melalui integrasi dalam pembelajaran maupun melalui aturan penggunaan perangkat digital. Guru juga dapat menggunakan kasus penipuan online sebagai bahan diskusi literasi digital sehingga peserta didik tidak hanya belajar menggunakan teknologi, tetapi juga memahami risiko penggunaannya.

Implikasi, Keterbatasan, dan Pengembangan Program

Hasil kegiatan perlu ditafsirkan secara proporsional karena evaluasi hanya menggunakan perbandingan rata-rata pre-test dan post-test tanpa kelompok pembanding serta pengukuran perilaku jangka panjang peserta. Nilai peningkatan sebesar 24,55 poin atau 40,45% menunjukkan perubahan capaian pemahaman peserta setelah kegiatan, tetapi belum dapat digunakan untuk membuktikan perubahan perilaku secara permanen. Desain evaluasi yang tersedia belum menyediakan data mengenai retensi pengetahuan setelah beberapa minggu atau bulan. Kondisi tersebut menjadi batas interpretasi hasil program.

Keterbatasan tersebut juga konsisten dengan persoalan yang ditemukan dalam penelitian keamanan siber berbasis pelatihan. Sikolia et al. (2023) menunjukkan bahwa pengetahuan yang diperoleh melalui program kesadaran keamanan dapat mengalami penurunan setelah periode tertentu. Temuan tersebut memberikan alasan bahwa pelatihan satu kali perlu dilanjutkan dengan penguatan berkala. Program lanjutan dapat dilakukan melalui *refresher training*, simulasi berkala, kuis keamanan digital, pembaruan kasus, dan evaluasi perilaku. Strategi tersebut dapat membantu mempertahankan pengetahuan dan meningkatkan kesiapan peserta menghadapi variasi ancaman.

Pengembangan program lanjutan dapat diarahkan pada penguatan retensi pengetahuan, evaluasi perilaku, pembaruan kasus, serta perluasan sasaran kepada tenaga kependidikan dan peserta didik secara bertahap. Evaluasi dapat dikembangkan menggunakan asesmen berbasis skenario sehingga peserta tidak hanya menjawab pertanyaan pengetahuan, tetapi juga menunjukkan kemampuan mengambil keputusan ketika menghadapi kasus keamanan digital. Pengukuran perilaku aktual juga dapat dilakukan melalui observasi atau simulasi terkontrol. Pendekatan tersebut akan memberikan informasi yang lebih kuat mengenai keberlanjutan dampak kegiatan.

Kajian Rohan et al. (2023) memberikan implikasi bahwa pengukuran kesadaran keamanan informasi perlu dilakukan dengan instrumen yang memiliki dasar konseptual dan validitas yang memadai. Pengembangan evaluasi kegiatan berikutnya dapat mempertimbangkan indikator yang lebih beragam, seperti kemampuan mengenali ancaman, persepsi risiko, kepercayaan diri, niat berperilaku aman, dan kemampuan mengambil keputusan. Perluasan indikator tersebut dapat

membantu menjelaskan apakah peningkatan pengetahuan juga diikuti dengan perubahan sikap dan perilaku keamanan.

Program juga dapat dikembangkan menjadi kegiatan literasi keamanan digital pada tingkat kelembagaan. Sekolah dapat membentuk kebijakan sederhana mengenai perlindungan data, penggunaan akun, pengelolaan dokumen digital, penggunaan perangkat pribadi, serta mekanisme pelaporan ketika terjadi insiden. Guru dapat menjadi penggerak penerapan kebijakan tersebut melalui praktik sehari-hari. Pengembangan kebijakan akan memperkuat keberlanjutan program karena keamanan digital tidak hanya bergantung pada kesadaran individu, tetapi juga dipengaruhi lingkungan organisasi.

Sintesis Hasil Kegiatan

Secara keseluruhan, kegiatan menunjukkan bahwa edukasi keamanan digital berbasis pengalaman mampu memperkuat pemahaman guru mengenai pencegahan penipuan online melalui pembelajaran yang kontekstual dan partisipatif di sekolah. Peningkatan nilai rata-rata dari 60,68 pada *pre-test* menjadi 85,23 pada *post-test* menunjukkan selisih sebesar 24,55 poin, sedangkan persentase peningkatan mencapai 40,45%. Hasil tersebut menjadi indikator capaian utama kegiatan. Materi yang berfokus pada keamanan digital, perlindungan data, keamanan akun, *phishing*, *social engineering*, tautan berbahaya, dan aplikasi palsu memberikan dasar pengetahuan yang relevan dengan kebutuhan peserta.

Temuan tersebut memperoleh penguatan dari berbagai penelitian yang menempatkan manusia sebagai komponen penting dalam keamanan siber. Naqvi et al. (2023) menunjukkan pentingnya pendekatan yang mempertimbangkan kemampuan manusia dalam mitigasi *phishing*. Singh et al. (2023) menegaskan pentingnya pengalaman dan umpan balik dalam pembelajaran *anti-phishing*. Bullee dan Junger (2020) menunjukkan bahwa karakteristik intervensi memengaruhi efektivitas pengurangan kerentanan terhadap *social engineering*. Khan et al. (2023) menunjukkan bahwa pelatihan dapat meningkatkan pengetahuan dan niat perilaku keamanan. Sikolia et al. (2023) memberikan pengingat bahwa keberlanjutan pengetahuan membutuhkan penguatan setelah pelatihan.

Hasil tersebut menunjukkan bahwa program pengabdian tidak hanya menghasilkan peningkatan skor evaluasi, tetapi juga menyediakan dasar bagi pengembangan budaya keamanan digital di lingkungan sekolah. Pemberian buku literasi digital memperkuat peluang pembelajaran lanjutan, sedangkan posisi guru sebagai agen literasi memberikan kemungkinan perluasan manfaat kepada peserta didik. erick+JPKM+revisi Dengan demikian, kegiatan edukasi keamanan digital dapat ditempatkan sebagai strategi peningkatan kapasitas yang menghubungkan pengetahuan, pengalaman, kesadaran, dan praktik penggunaan teknologi secara aman.

KESIMPULAN

Kegiatan edukasi keamanan digital di SMK Negeri 6 Makassar melibatkan 22 orang guru sebagai peserta dengan fokus pada peningkatan pemahaman mengenai keamanan digital dan pencegahan penipuan online. Hasil evaluasi menunjukkan adanya peningkatan nilai rata-rata pemahaman peserta dari 60,68 pada pre-test menjadi 85,23 pada post-test, dengan selisih sebesar 24,55 poin. Berdasarkan nilai awal tersebut, peningkatan pemahaman mencapai 40,45%. Hasil tersebut menunjukkan bahwa kegiatan edukasi memberikan perubahan positif terhadap pemahaman peserta mengenai perlindungan data pribadi, keamanan akun, pengenalan modus penipuan online, *phishing*, *social engineering*, tautan berbahaya, dan aplikasi palsu.

Peningkatan pemahaman tersebut menunjukkan bahwa kombinasi edukasi, diskusi, simulasi kasus, dan evaluasi dapat membantu peserta memahami ancaman digital secara lebih kontekstual dan aplikatif. Peserta memperoleh kesempatan untuk mengenali karakteristik pesan mencurigakan, tautan palsu, serta berbagai modus penipuan yang dapat ditemukan melalui media sosial dan aplikasi komunikasi. Pengalaman tersebut diharapkan meningkatkan kesiapan guru dalam mengenali potensi ancaman serta menentukan tindakan pencegahan yang lebih aman dalam aktivitas digital. Posisi guru sebagai pengguna teknologi sekaligus bagian dari lingkungan pendidikan juga memberikan peluang bagi pengetahuan yang diperoleh untuk dikembangkan menjadi praktik literasi digital yang dapat diterapkan kepada peserta didik.

Keberlanjutan manfaat kegiatan didukung melalui pemberian buku “Literasi Digital: Panduan Aman dan Cerdas di Era Digital” kepada seluruh peserta sebagai sumber belajar lanjutan.

Buku tersebut diharapkan dapat digunakan guru untuk memperkuat kembali pemahaman mengenai penggunaan teknologi secara aman setelah kegiatan selesai. Pengetahuan yang diperoleh juga diharapkan dapat diterapkan dalam aktivitas digital sehari-hari serta disampaikan kepada peserta didik sehingga manfaat kegiatan tidak berhenti pada peserta, tetapi dapat berkontribusi terhadap terbentuknya budaya penggunaan teknologi yang lebih aman dan bertanggung jawab di lingkungan sekolah.

Pernyataan Konflik Kepentingan

Penulis menyatakan bahwa tidak terdapat konflik kepentingan dalam pelaksanaan kegiatan, penyusunan, maupun publikasi artikel ini. Seluruh proses dilaksanakan secara independen tanpa adanya kepentingan pribadi, kelembagaan, maupun finansial yang dapat memengaruhi hasil dan penyajian artikel.

Pernyataan Penggunaan Kecerdasan Buatan Generatif

Penulis menyatakan bahwa tidak menggunakan kecerdasan buatan generatif (Generative AI) dalam proses penyusunan, pengolahan data, analisis, maupun penulisan artikel ini. Seluruh isi artikel disusun dan dikembangkan oleh penulis berdasarkan pelaksanaan kegiatan, data, analisis, dan sumber referensi yang digunakan.

REFERENSI

- Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, 73, 102258. <https://doi.org/10.1016/j.techsoc.2023.102258> IDEAS/RePEc
- Bullee, J.-W., & Junger, M. (2020). How effective are social engineering interventions? A meta-analysis. *Information & Computer Security*, 28(5), 801–830. <https://doi.org/10.1108/ICS-07-2019-0078> UT Research Info
- Butavicius, M., Taib, R., & Han, S. J. (2022). Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security*, 123, 102937. <https://doi.org/10.1016/j.cose.2022.102937> ScienceDirect

- Claro, M., Castro-Grau, C., Ochoa, J. M., Hinostroza, J. E., & Cabello, P. (2024). Systematic review of quantitative research on digital competences of in-service school teachers. *Computers & Education*, 215, 105030. <https://doi.org/10.1016/j.compedu.2024.105030> [ScienceDirect](#)
- de la Flor-Bancalero, P., & Guillen-Gamez, F. D. (2026). What digital competencies should teachers possess to teach educational cybersecurity to students in schools? Design and validation of a teacher competency scale. *Technology, Knowledge and Learning*. <https://doi.org/10.1007/s10758-026-09954-x> [Springer Nature Link](#)
- Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Computers & Security*, 125, 103049. <https://doi.org/10.1016/j.cose.2022.103049> [DOI](#)
- Khan, N. F., Yaqoob, A., Khan, M. S., & Ikram, N. (2022). The cybersecurity behavioral research: A tertiary study. *Computers & Security*, 120, 102826. <https://doi.org/10.1016/j.cose.2022.102826> [DBLP](#)
- Marshall, N., Sturman, D., & Auton, J. C. (2024). Exploring the evidence for email phishing training: A scoping review. *Computers & Security*, 139, 103695. <https://doi.org/10.1016/j.cose.2023.103695> [ScienceDirect](#)
- Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyediji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security*, 132, 103387. <https://doi.org/10.1016/j.cose.2023.103387> [DOI](#)
- Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*, 9(3), e14234. <https://doi.org/10.1016/j.heliyon.2023.e14234> [DOI](#)
- Safi, A., & Singh, S. (2023). A systematic literature review on phishing website detection techniques. *Journal of King Saud University—Computer and Information Sciences*, 35(2), 590–611. <https://doi.org/10.1016/j.jksuci.2023.01.004> [DOI](#)
- Sarker, O., Jayatilaka, A., Haggag, S., Liu, C., & Babar, M. A. (2024). A multi-vocal literature review on challenges and critical success factors of phishing education, training and



awareness. *The Journal of Systems & Software*, 208, 111899.

<https://doi.org/10.1016/j.jss.2023.111899>

Sikolia, D., Biros, D., & Zhang, T. (2023). How effective are SETA programs anyway: Learning and forgetting in security awareness training. *Journal of Cybersecurity Education, Research and Practice*, 2023(1). <https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss1/4/> [Digital Commons Kennesaw](#)

Singh, K., Aggarwal, P., Rajivan, P., & Gonzalez, C. (2023). Cognitive elements of learning and discriminability in anti-phishing training. *Computers & Security*, 127, 103105. <https://doi.org/10.1016/j.cose.2023.103105>

Torres-Hernández, N., & Gallego-Arrufat, M.-J. (2022). Indicators to assess preservice teachers' digital competence in security: A systematic review. *Education and Information Technologies*, 27(6), 8583–8602. <https://doi.org/10.1007/s10639-022-10978-w> [Springer Nature Link](#)

Tzafilkou, K., Perifanou, M., & Economides, A. A. (2023). Assessing teachers' digital competence in primary and secondary education: Applying a new instrument to integrate pedagogical and professional elements for digital education. *Education and Information Technologies*, 28, 16017–16040. <https://doi.org/10.1007/s10639-023-11848-9> [Springer Nature Link](#)

Wohlfart, O., & Wagner, I. (2023). Teachers' role in digitalizing education: An umbrella review. *Educational Technology Research and Development*, 71(2), 339–365. <https://doi.org/10.1007/s11423-022-10166-0>

Yasin, A., Fatima, R., JiangBin, Z., Afzal, W., & Raza, S. (2024). Can serious gaming tactics bolster spear-phishing and phishing resilience? Securing the human hacking in information security. *Information and Software Technology*, 170, 107426. <https://doi.org/10.1016/j.infsof.2024.107426>