Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 4 No. 4 (2026) pp: 11877-11886
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Pengembangan Modul Edukasi Interaktif Berbasis Web Untuk Deteksi Phishing Di Ma Raudlatul Hidayah

Fat Khudin[1], Dimas Rahma Samudra[2], Muhammad Fauzan[3], Indriani Utama[4], Sarman[5]
[1,2,3,4,5]Fakultas Ilmu Komputer, Prodi Teknik Informatika, Universitas Pamulang, Kota Tangerang Selatan, Indonesia
[1]fatkhudinudin47434@gmail.com , [2]dimassamudraa1122@gmail.com, [3]mhmdfauzan86@gmail.com,
[4]indriautama85@gmail.com , [5]dosen02966@unpam.ac.id

Abstrak

Transformasi digital dalam dunia pendidikan telah mengubah pola pembelajaran secara signifikan, terutama melalui pemanfaatan internet sebagai sumber utama informasi dan media pembelajaran. Di satu sisi, perkembangan ini memberikan kemudahan akses pengetahuan dan memperluas ruang belajar siswa. Namun, di sisi lain, peningkatan aktivitas digital juga diiringi oleh meningkatnya risiko keamanan siber, khususnya bagi pelajar yang termasuk kelompok pengguna internet paling aktif. Penelitian ini bertujuan mengimplementasikan program literasi keamanan digital melalui pengembangan modul edukasi interaktif berbasis web bernama PHISH-CHECK yang dirancang khusus untuk siswa MA Raudlatul Hidayah, Kabupaten Tangerang. Meskipun sebagian siswa telah mengenal penipuan digital secara umum, kemampuan mereka dalam melakukan analisis teknis serta merespons ancaman phishing secara sistematis masih tergolong terbatas. Program ini mengintegrasikan pembelajaran konseptual mengenai phishing, simulasi interaktif dengan tiga skenario autentik yaitu login palsu, undian hadiah, dan formulir beasiswa, serta panduan praktis perlindungan data pribadi. Kegiatan dilaksanakan melalui workshop intensif yang melibatkan 25 siswa selama satu hari penuh di laboratorium komputer sekolah. Hasil kegiatan menunjukkan adanya peningkatan pemahaman terhadap indikator teknis phishing, seperti analisis struktur URL, verifikasi domain, dan identifikasi inkonsistensi visual. Siswa yang sebelumnya mengandalkan intuisi mulai menerapkan pendekatan evaluasi yang lebih terstruktur dan sistematis. Evaluasi pasca-workshop menunjukkan peningkatan kemampuan deteksi teknis secara signifikan, menandakan pergeseran dari penilaian intuitif menuju analisis berbasis indikator konkret. Platform PHISH-CHECK juga berfungsi sebagai media pembelajaran mandiri yang mendukung penguatan literasi keamanan digital secara berkelanjutan dan berpotensi direplikasi sebagai model intervensi edukatif keamanan siber berbasis sekolah. Pendekatan ini diharapkan mampu meningkatkan kewaspadaan siswa terhadap ancaman digital masa depan yang semakin kompleks.

***Kata kunci**: Deteksi Phishing, Platform Edukasi Interaktif, Literasi Keamanan Digital, Simulasi Pembelajaran, Madrasah Aliyah*

1. Latar Belakang

Intensitas penggunaan internet oleh pelajar memberikan kontribusi signifikan terhadap proses pembelajaran digital, terutama dalam mendukung akses informasi, komunikasi akademik, serta pemanfaatan berbagai layanan pendidikan berbasis daring. Internet tidak hanya digunakan untuk mengakses materi pembelajaran, tetapi juga untuk berinteraksi melalui media sosial, mengikuti kegiatan ekstrakurikuler daring, serta mengisi berbagai formulir digital yang sering kali meminta data pribadi. Kondisi ini menjadikan pelajar sebagai bagian dari ekosistem digital yang aktif dan sekaligus rentan terhadap ancaman keamanan siber.

Salah satu bentuk ancaman keamanan siber yang paling sering ditemui adalah phishing. Phishing merupakan bentuk serangan siber yang menargetkan aspek perilaku pengguna dengan memanfaatkan manipulasi psikologis, sehingga tidak bergantung pada eksploitasi celah teknis sistem. Pelaku phishing biasanya menyamar sebagai pihak terpercaya dengan tampilan visual dan bahasa yang meyakinkan, sehingga korban terdorong untuk memberikan informasi sensitif tanpa melakukan verifikasi mendalam. Pola serangan ini menjadikan pelajar sebagai target potensial karena tingkat kewaspadaan digital yang masih berkembang.

Hasil observasi awal yang dilakukan secara langsung di MA Raudlatul Hidayah menunjukkan bahwa sebagian siswa telah mengenal konsep penipuan daring, baik melalui pengalaman pribadi maupun informasi dari lingkungan sekitar. Namun demikian, pemahaman tersebut masih bersifat umum dan belum disertai kemampuan analisis teknis yang memadai. Penilaian terhadap keamanan suatu konten digital umumnya didasarkan pada intuisi atau rasa curiga semata, tanpa mempertimbangkan indikator teknis seperti struktur URL, kesesuaian domain, maupun konsistensi elemen visual.

Kondisi ini menimbulkan risiko kesalahan penilaian, terutama ketika serangan phishing dirancang dengan tingkat kemiripan tinggi terhadap layanan resmi. Kesadaran tanpa keterampilan analitis yang memadai dapat menciptakan rasa aman semu yang justru meningkatkan potensi menjadi korban. Oleh karena itu, literasi keamanan digital perlu diarahkan tidak hanya pada peningkatan kesadaran, tetapi juga pada pembentukan keterampilan analitis dan kebiasaan verifikasi yang sistematis.

Berbagai kajian terdahulu menunjukkan bahwa pendekatan edukasi keamanan siber yang efektif perlu mengintegrasikan pemahaman konseptual dengan pengalaman praktik secara langsung. Pembelajaran berbasis pengalaman memungkinkan siswa berinteraksi langsung dengan simulasi ancaman dalam lingkungan yang aman, sehingga proses pembelajaran menjadi lebih bermakna dan kontekstual. Pendekatan ini dinilai lebih efektif dibandingkan metode ceramah semata dalam membentuk pemahaman jangka panjang.

Berdasarkan latar belakang tersebut, penelitian ini mengembangkan modul edukasi interaktif berbasis web melalui platform PHISH-CHECK. Platform ini dirancang sebagai media pembelajaran yang mampu menjembatani kesenjangan antara pengetahuan konseptual dan penerapan teknis, dengan tujuan meningkatkan literasi keamanan digital siswa secara komprehensif.

1. Metode Pelaksanaan

Program ini dirancang menggunakan pendekatan pembelajaran partisipatif berbasis pengalaman, dengan menempatkan siswa sebagai subjek aktif dalam setiap tahapan kegiatan. Pendekatan ini dipilih untuk mendorong keterlibatan langsung siswa dalam proses pembelajaran serta membangun pemahaman yang diperoleh melalui pengalaman nyata.

Metode pelaksanaan terdiri atas beberapa tahap utama, yaitu asesmen kebutuhan, pengembangan platform, implementasi workshop, dan evaluasi hasil kegiatan. Tahap asesmen kebutuhan dilakukan melalui koordinasi dengan pihak sekolah serta diskusi awal dengan siswa untuk mengidentifikasi tingkat pemahaman keamanan digital dan kesiapan sarana pendukung. Asesmen ini juga bertujuan memastikan bahwa materi dan metode yang digunakan sesuai dengan konteks dan kebutuhan peserta.

Pengembangan platform PHISH-CHECK dilakukan dengan pendekatan kontekstual dan responsif. Platform ini dirancang agar dapat diakses melalui berbagai perangkat dan memuat tiga modul utama. Modul pembelajaran konseptual menyajikan materi dasar mengenai phishing, karakteristik serangan, serta dampak yang ditimbulkan. Modul simulasi interaktif menghadirkan tiga skenario autentik yang sering dijumpai oleh pelajar, yaitu login palsu, undian hadiah, dan formulir beasiswa. Modul panduan proteksi berisi praktik keamanan digital, termasuk pengelolaan kata sandi, autentikasi dua faktor, dan langkah respons ketika menghadapi potensi insiden keamanan.

Kegiatan workshop dilaksanakan secara tatap muka selama satu hari di laboratorium komputer sekolah dengan melibatkan 25 siswa peserta. Workshop mencakup sesi pengenalan konsep, eksplorasi simulasi secara terpandu, diskusi reflektif, dan asesmen penutup. Fasilitator berperan sebagai pendamping analisis untuk membantu siswa memahami indikator teknis dan mendorong diskusi kritis.

Evaluasi kegiatan dilakukan secara kualitatif melalui observasi langsung terhadap interaksi siswa, diskusi pasca-simulasi, serta analisis respons siswa terhadap setiap skenario yang diberikan. Pendekatan evaluasi ini digunakan untuk menangkap perubahan pola berpikir dan perilaku siswa secara lebih mendalam.

3. Hasil dan Pembahasan

Hasil Seluruh aktivitas pembelajaran dan interaksi peserta selama kegiatan berlangsung diamati dan dicatat secara langsung oleh tim pelaksana untuk mendokumentasikan perubahan pola berpikir dan perilaku siswa dalam menghadapi konten digital mencurigakan.

3.1 Pemahaman Dasar dan Kesenjangan Pengetahuan

Temuan awal dari asesmen informal mengungkapkan lanskap yang lebih bernuansa dibandingkan asumsi awal. Berlawanan dengan ekspektasi bahwa siswa memiliki pengetahuan minimal tentang ancaman siber, ternyata 72% dari peserta sudah familiar dengan konsep phishing, dengan 48% melaporkan paparan langsung atau tidak langsung terhadap upaya phishing. Angka ini signifikan lebih tinggi dari estimasi awal dan mengindikasikan bahwa kampanye kesadaran dan liputan media tentang penipuan siber sudah mencapai demografi ini.

DOI: https://doi.org/10.31004/riggs.v4i4.5304

Hasil kegiatan menunjukkan bahwa sebelum mengikuti program, sebagian besar siswa telah memiliki kesadaran awal terhadap keberadaan penipuan daring. Namun, kesadaran tersebut belum disertai kemampuan untuk mengidentifikasi indikator teknis phishing secara spesifik. Banyak siswa masih mengandalkan perasaan atau pengalaman pribadi dalam menilai keamanan suatu konten digital.

Ketika ditanya "Bagaimana kalian tahu itu phishing?", respons tipikal adalah "rasanya aneh", "terlalu mencurigakan", atau "teman bilang itu penipuan" yang semuanya mengindikasikan ketergantungan pada intuisi atau informasi pihak kedua ketimbang analisis sistematis. Penyelidikan lebih dalam mengungkapkan kesenjangan kritis dimana meskipun siswa dapat mengidentifikasi istilah dan secara umum sadar bahwa terdapat penipuan di internet, kemampuan mereka untuk mengartikulasikan mekanisme spesifik atau mengidentifikasi indikator konkret sangat terbatas.

Lebih mengkhawatirkan adalah penemuan bahwa beberapa siswa yang mengklaim pernah menghindari upaya phishing sebenarnya melakukannya secara tidak sengaja atau karena alasan yang tidak terkait dengan kesadaran keamanan. Seorang siswa mengaku tidak mengisi formulir undian bukan karena mengenalinya sebagai penipuan, tetapi karena merasa malas mengisi data yang banyak. Siswa lain tidak mengklik tautan mencurigakan karena sinyal internet sedang lambat sehingga membatalkan. Ini mengungkapkan bahwa penghindaran yang berhasil tidak selalu sama dengan kesadaran keamanan dimana terdapat elemen keberuntungan yang terlibat.

Analisis lebih lanjut mengidentifikasi tiga kelompok berbeda dalam populasi peserta. Kelompok pertama adalah Kelompok Pemula sebesar 28% dengan pemahaman terbatas tentang ancaman digital, jarang menghadapi konten mencurigakan, atau ketika menghadapi tidak mengenalinya sebagai ancaman. Kelompok kedua adalah Kelompok Sadar Namun Tidak Terampil sebesar 56% yang mengetahui phishing ada dan bisa mengidentifikasi penipuan yang jelas, namun kurang kemampuan teknis untuk menganalisis kasus yang ambigu. Kelompok ketiga adalah Kelompok Berpengalaman sebesar 16% yang pernah menjadi korban aktual atau pengalaman nyaris terjebak yang membuat mereka mengembangkan kesadaran yang meningkat, namun masih kurang kerangka kerja sistematis.

Segmentasi ini penting karena menginformasikan pendekatan yang berbeda dalam penyampaian konten dengan mengakui bahwa penjelasan satu ukuran untuk semua tidak optimal untuk kemampuan dasar yang beragam. Temuan ini sejalan dengan penelitian Permadi dan Ramli (2024) yang menekankan pentingnya mengukur tingkat kesadaran keamanan informasi sebagai langkah awal dalam merancang program edukasi yang efektif.

3.2 Transformasi Pembelajaran Melalui Simulasi Interaktif

Dampak dari komponen simulasi langsung terbukti menjadi aspek paling transformatif dari program. Transisi dari pembelajaran pasif ke eksperimentasi aktif menciptakan beberapa momen pembelajaran kritis yang mengubah cara siswa memandang dan menganalisis konten digital.

Setelah mengikuti simulasi interaktif pada platform PHISH-CHECK, siswa mulai menunjukkan peningkatan kemampuan analisis teknis. Momen disonansi kognitif terjadi ketika banyak siswa yang awalnya percaya diri dengan kemampuan mereka untuk mendeteksi phishing terkejut ketika benar-benar dihadapkan dengan halaman login palsu yang relatif canggih dalam simulasi. Seorang siswa mengakui bahwa "Saya kira saya bisa langsung tahu, tapi ternyata waktu lihat halamannya, hampir saja saya kira itu asli." Momen keraguan diri ini berharga karena menciptakan keterbukaan untuk pembelajaran dimana pengakuan bahwa pengetahuan saat ini tidak memadai memotivasi keterlibatan lebih dalam dengan materi.

Pengembangan pengenalan pola terjadi ketika siswa bekerja melalui berbagai skenario. Awalnya, kecenderungan adalah untuk pandangan cepat dan penilaian segera. Namun demikian, dengan bimbingan dan paparan berulang, siswa mulai mengembangkan proses pemeriksaan yang lebih metodis. Komentar bergeser dari "ini kayaknya phishing deh" menjadi "URL-nya menggunakan domain titik xyz, terus logonya agak buram, sama tata bahasanya ada yang salah di sini" yang mendemonstrasikan transisi dari pemikiran intuitif ke analitis.

Momen pencerahan muncul ketika siswa menemukan petunjuk halus yang memerlukan observasi cermat. Ketika siswa menemukan petunjuk ini, kegembiraan dan kepuasan yang terlihat jelas. Momen penemuan ini menciptakan penguatan positif yang mendorong pemeriksaan cermat berkelanjutan dalam pertemuan masa depan. Temuan ini memvalidasi penelitian Sheng et al. (2007) yang menunjukkan bahwa pembelajaran berbasis game dan simulasi interaktif lebih efektif dalam mengajarkan deteksi phishing dibandingkan metode instruksi tradisional.

DOI: https://doi.org/10.31004/riggs.v4i4.5304

3.3 Analisis Mendalam Skenario Simulasi

3.3.1 Skenario Login Palsu

Pada skenario login palsu, siswa mampu mengidentifikasi perbedaan struktur URL, domain yang tidak sesuai, serta inkonsistensi elemen visual. Tingkat kelulusan awal atau siswa yang awalnya berpikir halaman tersebut sah adalah 64%, memvalidasi kekhawatiran bahwa kemiripan visual sangat menipu. Namun demikian, setelah analisis terpandu dan diskusi indikator teknis, percobaan selanjutnya dengan skenario yang dimodifikasi menunjukkan peningkatan dramatis dengan hanya 12% yang awalnya tertipu.

Proses diskusi pasca-simulasi membantu siswa memahami alasan teknis di balik setiap indikator yang ditemukan. Poin pembelajaran kunci yang muncul meliputi:

Keterampilan Inspeksi Domain: Siswa belajar untuk tidak hanya melirik bilah URL tetapi benar-benar membaca karakter demi karakter, mencari substitusi halus seperti angka nol untuk huruf O (facebo0k.com), vvw untuk www, kata tambahan atau subdomain yang mencurigakan (facebook-login.xyz). Fasilitator mendemonstrasikan bahwa domain seperti ini adalah indikator jelas pemalsuan meskipun tampilan visualnya sangat mirip dengan situs asli.

Koreksi Kesalahpahaman HTTPS: Banyak siswa beroperasi di bawah asumsi bahwa adanya gembok atau HTTPS sama dengan aman. Simulasi mendemonstrasikan bahwa situs phishing dapat memiliki sertifikat keamanan yang valid, menggeser fokus dari evaluasi biner aman atau tidak aman ke evaluasi komprehensif yang mempertimbangkan berbagai indikator. Siswa belajar bahwa HTTPS hanya mengenkripsi komunikasi antara browser dan server, tetapi tidak menjamin bahwa server tersebut adalah pihak yang diklaim. Temuan ini sejalan dengan penelitian Alkhalil et al. (2021) yang mengidentifikasi bahwa pelaku phishing kini menggunakan HTTPS untuk meningkatkan kredibilitas serangan mereka.

Perhatian Detail Visual: Melalui perbandingan dengan halaman login asli, siswa dilatih untuk memperhatikan perbedaan kualitas seperti logo resolusi rendah, font tidak konsisten, elemen tidak sejajar, atau fitur yang hilang. Beberapa siswa mencatat bahwa tombol login pada halaman palsu memiliki warna yang sedikit berbeda, atau tata letak footer tidak sempurna seperti versi asli. Kemampuan untuk mendeteksi inkonsistensi visual halus ini menandakan peningkatan signifikan dalam keterampilan observasi kritis.

3.3.2 Skenario Undian Hadiah

Skenario undian hadiah beresonansi kuat dengan peserta karena banyak yang mengakui pernah melihat atau bahkan awalnya bersemangat tentang tawaran serupa. Efektivitas skenario terletak pada progresi dimana dimulai dengan tawaran menarik yang memicu minat, secara bertahap meminta informasi yang semakin sensitif, dengan setiap langkah disertai dengan rasionalisasi seperti "untuk verifikasi identitas" atau "supaya hadiah bisa dikirim".

Diskusi setelah simulasi ini sangat kaya dimana siswa merefleksikan teknik psikologis yang digunakan:

Kelangkaan Artifisial: Pesan seperti "hanya untuk 100 orang pertama" atau "tawaran terbatas hari ini" menciptakan tekanan waktu yang mendorong keputusan cepat tanpa evaluasi menyeluruh. Siswa menyadari bahwa taktik urgensi ini dirancang untuk melewati pemikiran kritis mereka. Vishwanath et al. (2011) mengidentifikasi bahwa tekanan waktu adalah salah satu faktor kunci yang meningkatkan kerentanan terhadap phishing.

Bukti Sosial Palsu: Testimoni "ribuan orang sudah menang" atau counter yang menampilkan jumlah pemenang yang terus bertambah menciptakan ilusi legitimasi. Siswa belajar untuk mempertanyakan keaslian bukti sosial semacam ini dan mencari verifikasi independen.

Eksploitasi Otoritas: Mengklaim kerjasama dengan merek terkenal atau menggunakan logo perusahaan besar tanpa izin untuk meminjam kredibilitas. Siswa dilatih untuk memverifikasi klaim kemitraan melalui saluran resmi perusahaan yang disebutkan.

Permintaan Informasi Berlebihan: Meminta informasi yang tidak wajar untuk klaim hadiah sederhana seperti meminta nomor kartu kredit, password, atau data pribadi sensitif lainnya. Siswa mengembangkan pemahaman tentang prinsip minimalisasi data dimana organisasi yang sah hanya meminta informasi yang benar-benar diperlukan untuk tujuan spesifik.

Pengakuan bahwa ini adalah taktik manipulasi yang disengaja ketimbang hanya pesan yang mencurigakan mewakili kecanggihan signifikan dalam pemahaman. Siswa mulai memahami bahwa phishing bukan hanya tentang teknologi tetapi juga tentang rekayasa sosial yang mengeksploitasi psikologi manusia, sesuai dengan

DOI: https://doi.org/10.31004/riggs.v4i4.5304

temuan Aleroud dan Zhou (2017) mengenai evolusi teknik phishing dari eksploitasi teknis ke manipulasi psikologis.

3.3.3 Skenario Formulir Beasiswa

Skenario formulir beasiswa menciptakan jenis pembelajaran yang berbeda karena menargetkan aspirasi yang sah dan konteks yang biasanya dapat dipercaya. Beberapa siswa mencatat bahwa mereka pernah mendaftar untuk beasiswa aktual dan memang diminta berbagai informasi, membuat lebih sulit untuk membedakan permintaan yang sah dari yang menipu.

Keterampilan diferensiasi kritis yang dikembangkan meliputi:

Protokol Verifikasi: Siswa belajar untuk secara independen memverifikasi keberadaan beasiswa melalui saluran resmi sebelum melanjutkan dengan aplikasi. Mereka dilatih untuk mencari informasi beasiswa di situs web resmi institusi pemberi, bukan hanya mengandalkan email atau iklan yang diterima.

Pengenalan Tanda Bahaya: Mengidentifikasi permintaan mencurigakan seperti pembayaran di muka untuk "biaya administrasi" atau "jaminan", meminta password atau PIN, atau detail personal berlebihan yang tidak relevan untuk evaluasi beasiswa seperti nomor kartu kredit orang tua atau informasi rekening bank. Siswa mengembangkan pemahaman bahwa beasiswa yang sah tidak pernah meminta pembayaran dari pelamar.

Autentikasi Sumber: Memeriksa apakah tautan aplikasi berasal dari domain institusional resmi, apakah ada informasi kontak yang dapat diverifikasi, dan apakah format komunikasi konsisten dengan standar profesional institusi pendidikan. Siswa belajar untuk waspada terhadap formulir yang dihosting di platform pihak ketiga tanpa afiliasi jelas dengan institusi yang diklaim.

Evaluasi Konteks Komunikasi: Siswa dilatih untuk mempertimbangkan apakah mereka pernah mendaftar atau menunjukkan minat pada beasiswa tersebut sebelumnya, atau apakah ini adalah tawaran yang tidak diminta yang datang tiba-tiba. Komunikasi yang tidak diminta yang mengklaim siswa telah dipilih untuk beasiswa tanpa aplikasi sebelumnya adalah tanda bahaya utama.

3.4 Pergeseran dari Pendekatan Intuitif ke Sistematis

Hasil paling signifikan adalah pergeseran yang dapat diamati dalam bagaimana siswa mendekati evaluasi keamanan digital. Sebelum program, pendekatan dominan adalah intuitif dengan mengandalkan perasaan naluri atau kesan tingkat permukaan untuk membuat keputusan kepercayaan. Setelah program, siswa mulai mengadopsi kerangka kerja sistematis yang menandakan transformasi fundamental dalam pemikiran kritis mereka.

Pengembangan Mentalitas Daftar Periksa: Beberapa siswa menyebutkan secara spontan membuat daftar periksa mental atau aktual untuk mengevaluasi konten mencurigakan. Elemen umum yang muncul meliputi: memeriksa pengirim atau domain dengan teliti, memverifikasi struktur URL karakter demi karakter, mencari kesalahan tata bahasa atau ejaan, menilai kewajaran permintaan informasi dalam konteks, mencari konfirmasi independen melalui saluran resmi, dan mempertimbangkan apakah komunikasi diminta atau tidak diminta.

Pembentukan Kebiasaan Mempertanyakan: Alih-alih penerimaan pasif, siswa mulai default ke skeptisisme sehat. Bukan skeptisisme paranoid yang menolak segalanya, tetapi skeptisisme konstruktif yang mendorong verifikasi sebelum kepercayaan. Pergeseran terlihat dalam komentar seperti "Sekarang kalau ada tautan, saya langsung cek dulu alamatnya" atau "Saya jadi berpikir untuk mencari di mesin pencari dulu sebelum mengisi formulir daring".

Perubahan perilaku ini menunjukkan internalisasi prinsip keamanan digital dimana verifikasi menjadi kebiasaan alami bukan tugas tambahan yang memberatkan. Wright dan Marett (2010) menemukan bahwa pengalaman langsung dengan phishing, bahkan dalam konteks simulasi, secara signifikan meningkatkan kemampuan individu untuk mendeteksi upaya phishing di masa depan.

Inisiasi Edukasi Sebaya: Beberapa siswa melaporkan berbagi pembelajaran dengan teman sekelas yang tidak berpartisipasi, saudara kandung, atau bahkan orang tua. Seorang siswa bersemangat menceritakan bagaimana dia menyelamatkan temannya yang hampir mengirimkan informasi ke formulir beasiswa mencurigakan, kini dilengkapi dengan kemampuan untuk menunjukkan tanda bahaya spesifik seperti domain yang tidak cocok dan permintaan pembayaran di muka. Fenomena pendidikan sebaya ini memperluas dampak program melampaui 25 peserta langsung, menciptakan efek pengganda dalam komunitas sekolah.

DOI: https://doi.org/10.31004/riggs.v4i4.5304

3.5 Adopsi Platform dan Keterlibatan Berkelanjutan

Data akses pasca-workshop mengindikasikan keterlibatan berkelanjutan yang menjanjikan. Dalam minggu pertama setelah workshop, platform mencatat 47 sesi akses unik dari 19 pengguna berbeda yang mengindikasikan bahwa 76% peserta kembali ke platform melampaui sesi workshop wajib. Rata-rata waktu yang dihabiskan per sesi adalah 18 menit, menunjukkan keterlibatan substansif ketimbang pemeriksaan sekilas.

Analisis pola penggunaan mengungkapkan wawasan menarik:

Popularitas Modul: Skenario simulasi paling sering dikunjungi kembali, dengan skenario login palsu memiliki tingkat pengulangan tertinggi. Ini selaras dengan umpan balik bahwa siswa menemukan nilai dalam praktik berulang untuk mempertajam keterampilan deteksi mereka. Jampen et al. (2020) dalam kajian literatur mereka menemukan bahwa pelatihan anti-phishing yang efektif memerlukan paparan berulang dan praktik berkelanjutan untuk membangun keterampilan yang bertahan lama.

Penggunaan Bagian Sumber Daya: Panduan tentang pembuatan kata sandi yang kuat dan pengaturan autentikasi dua faktor mengalami akses yang stabil dan konsisten. Hal ini menunjukkan siswa tidak hanya tertarik pada deteksi phishing tetapi juga mengambil langkah proaktif untuk menerapkan praktik keamanan yang direkomendasikan.

Pola Temporal: Lonjakan akses diamati selama jam awal malam (19.00-21.00) dan akhir pekan, mengindikasikan pembelajaran sukarela di luar waktu pendidikan terjadwal. Pola ini mengkonfirmasi bahwa platform berhasil memfasilitasi pembelajaran mandiri yang didorong oleh minat intrinsik ketimbang kewajiban akademik.

Beberapa siswa melampaui konsumsi pasif dan secara aktif menyarankan skenario tambahan seperti situs web belanja palsu, notifikasi pengiriman palsu, portal layanan pemerintah palsu, dan aplikasi pinjaman online mencurigakan. Usulan-usulan ini mendemonstrasikan bahwa siswa menginternalisasi pembelajaran dan berpikir kritis tentang aplikasi konsep keamanan ke konteks lain yang mereka hadapi.

3.6 Perubahan Indikator Perilaku

Melampaui perolehan pengetahuan kognitif, observasi dan laporan diri siswa mengindikasikan perubahan perilaku nyata yang mendemonstrasikan transfer pembelajaran ke praktik aktual.

Peningkatan Perilaku Verifikasi: Siswa melaporkan secara aktif menerapkan langkah verifikasi seperti mengetik URL situs web secara manual alih-alih mengklik tautan langsung dari email, memeriksa alamat email pengirim dengan cermat sebelum merespons, menggunakan mesin pencari untuk mengonfirmasi legitimasi tawaran sebelum mengambil tindakan, memverifikasi identitas pengirim melalui saluran komunikasi alternatif ketika menerima permintaan yang tidak biasa, dan memeriksa ulasan tentang platform atau layanan baru sebelum mendaftar.

Adopsi Fitur Keamanan: Survei informal pasca-workshop mengindikasikan 42% peserta telah mengaktifkan autentikasi dua faktor pada setidaknya satu akun digital mereka, dengan mayoritas memilih email atau akun media sosial utama. Angka ini mewakili peningkatan signifikan mengingat baseline diperkirakan di bawah 10% sebelum workshop. Siswa juga melaporkan telah mengubah kata sandi mereka menjadi lebih kuat dan unik untuk setiap layanan.

Berbagi Informasi yang Lebih Hati-hati: Kesadaran yang meningkat tentang privasi data mengarah ke perilaku berbagi informasi yang lebih selektif. Siswa melaporkan lebih kritis tentang formulir yang mereka isi, lebih mempertanyakan mengapa informasi tertentu diminta dan apakah permintaan tersebut wajar, lebih sadar akan izin yang mereka berikan kepada aplikasi mobile terutama terkait akses ke kontak atau lokasi, dan lebih berhati-hati dalam membagikan informasi pribadi di media sosial.

Perilaku Pelaporan: Peningkatan kesediaan siswa untuk melaporkan konten mencurigakan dan mencari konfirmasi ketika ragu. Beberapa siswa menghubungi fasilitator untuk mengonfirmasi apakah pesan atau situs web tertentu sah, mendemonstrasikan baik ketidakpastian yang sehat maupun kepercayaan dalam sistem dukungan yang dibentuk.

3.7 Perspektif Pemangku Kepentingan dan Dampak Institusional

Umpan balik dari guru teknologi informasi dan administrasi sekolah memberikan validasi eksternal terhadap efektivitas program. Guru TIK khususnya mengapresiasi ketersediaan sumber daya terstruktur yang dapat diintegrasikan ke dalam pengajaran reguler. Komentar bahwa "ini memudahkan saya karena sekarang ada platform

DOI: https://doi.org/10.31004/riggs.v4i4.5304

konkret untuk demonstrasi, bukan hanya ceramah teoritis" menyoroti proposisi nilai platform sebagai alat pedagogis yang dapat digunakan berulang.

Administrasi sekolah mengekspresikan minat kuat dalam memperluas program ke seluruh badan siswa dan potensial melibatkan orang tua dalam workshop terpisah. Pengakuan dari kepala sekolah bahwa literasi keamanan siber adalah keterampilan hidup yang penting mewakili pergeseran pola pikir institusional yang signifikan.

Diskusi dimulai tentang menggabungkan platform PHISH-CHECK sebagai komponen wajib dalam program orientasi untuk siswa baru setiap tahun akademik. Beberapa guru mata pelajaran lain juga menunjukkan minat untuk mengintegrasikan elemen keamanan digital ke dalam kurikulum mereka, seperti guru Bahasa Indonesia yang tertarik menggunakan contoh phishing untuk analisis teks persuasif, atau guru PKN yang ingin mendiskusikan hak privasi digital dan tanggung jawab kewargaan digital.

Komitmen institusional ini penting untuk keberlanjutan dampak program karena memastikan bahwa literasi keamanan digital tidak diperlakukan sebagai intervensi sekali jalan tetapi menjadi bagian integral dari ekosistem pembelajaran sekolah. Kalnoor dan Gowrishankar (2020) menekankan bahwa pendidikan keamanan siber yang berkelanjutan dan terintegrasi dalam kurikulum menghasilkan dampak jangka panjang yang lebih signifikan dibandingkan pelatihan satu kali.

3.8 Analisis Perubahan Kognitif Peserta Setelah Intervensi

Selain perubahan perilaku yang dapat diamati secara langsung, program PHISH-CHECK juga menunjukkan dampak signifikan pada aspek kognitif peserta, khususnya dalam cara mereka memproses dan mengevaluasi informasi digital. Sebelum intervensi, proses kognitif siswa cenderung bersifat heuristik, yaitu mengandalkan penilaian cepat berbasis kesan awal tanpa melalui tahapan evaluasi yang mendalam. Pola ini umum ditemukan pada pengguna digital muda yang terbiasa dengan konsumsi informasi cepat dan volume konten tinggi.

Setelah mengikuti rangkaian pembelajaran dan simulasi interaktif, siswa mulai menunjukkan pola berpikir yang lebih reflektif. Mereka tidak lagi langsung mempercayai atau menolak suatu konten digital, tetapi terlebih dahulu mengidentifikasi elemen-elemen kunci yang relevan untuk evaluasi keamanan. Perubahan ini terlihat dari meningkatnya kemampuan siswa dalam menjelaskan alasan di balik keputusan mereka, tidak hanya menyatakan bahwa suatu konten mencurigakan, tetapi juga menguraikan indikator teknis dan konteks yang mendasarinya.

Perubahan kognitif ini menandakan terjadinya peningkatan pada level pemahaman analitis, dimana siswa tidak hanya mengetahui apa itu phishing, tetapi juga memahami bagaimana dan mengapa suatu konten dapat dikategorikan sebagai phishing. Dengan demikian, pembelajaran tidak berhenti pada penguasaan istilah, melainkan berkembang menjadi kemampuan berpikir kritis yang dapat diterapkan lintas konteks digital.

3.9 Penguatan Literasi Keamanan Digital sebagai Keterampilan Hidup

Literasi keamanan digital yang dikembangkan melalui program ini tidak hanya relevan dalam konteks akademik, tetapi juga memiliki implikasi langsung terhadap kehidupan sehari-hari siswa. Aktivitas digital siswa tidak terbatas pada pembelajaran formal, melainkan mencakup interaksi media sosial, transaksi daring, penggunaan aplikasi, dan konsumsi informasi digital lainnya. Oleh karena itu, kemampuan untuk mendeteksi ancaman phishing menjadi keterampilan hidup yang esensial.

Hasil kegiatan menunjukkan bahwa siswa mulai menyadari bahwa keamanan digital bukan sekadar tanggung jawab sistem atau aplikasi, melainkan juga tanggung jawab pengguna. Kesadaran ini tercermin dari perubahan sikap siswa yang lebih berhati-hati dalam membagikan informasi pribadi, lebih selektif dalam mengisi formulir daring, dan lebih skeptis terhadap tawaran yang menjanjikan keuntungan instan.

Penguatan literasi keamanan digital ini juga berkontribusi pada pembentukan karakter digital yang bertanggung jawab. Siswa tidak hanya belajar melindungi diri sendiri, tetapi juga menunjukkan kepedulian terhadap lingkungan sekitarnya dengan memperingatkan teman atau keluarga ketika menemukan konten digital mencurigakan. Hal ini menunjukkan bahwa program tidak hanya berdampak pada individu, tetapi juga memiliki potensi membangun budaya keamanan digital dalam komunitas sekolah.

DOI: https://doi.org/10.31004/riggs.v4i4.5304

3.10 Internalitas Pembelajaran dan Pembentukan Kebiasaan Baru

Salah satu indikator keberhasilan program pengabdian masyarakat adalah sejauh mana pembelajaran dapat terinternalisasi dan membentuk kebiasaan baru yang berkelanjutan. Berdasarkan observasi dan umpan balik pasca-workshop, program PHISH-CHECK berhasil mendorong proses internalisasi tersebut.

Siswa mulai menjadikan langkah verifikasi sebagai bagian dari rutinitas alami ketika berinteraksi dengan konten digital. Aktivitas seperti memeriksa URL sebelum login, memastikan domain resmi sebelum mengisi data, dan mencari informasi pendukung melalui mesin pencari tidak lagi dianggap sebagai langkah tambahan yang merepotkan, tetapi sebagai prosedur standar yang wajar dilakukan.

Pembentukan kebiasaan ini diperkuat oleh pengalaman langsung dalam simulasi, dimana siswa merasakan sendiri konsekuensi potensial dari keputusan yang diambil. Pembelajaran berbasis pengalaman semacam ini terbukti lebih efektif dalam membentuk kebiasaan dibandingkan instruksi teoritis semata, karena siswa tidak hanya diberi tahu apa yang benar, tetapi mengalami sendiri proses pengambilan keputusan yang aman dan tidak aman.

3.11 Peran Platform PHISH-CHECK dalam Pembelajaran Mandiri Berkelanjutan

Keberadaan platform PHISH-CHECK sebagai media pembelajaran daring memberikan nilai tambah signifikan dalam konteks keberlanjutan program. Tidak seperti workshop konvensional yang berhenti ketika kegiatan selesai, platform ini memungkinkan siswa untuk mengakses kembali materi, simulasi, dan panduan kapan saja sesuai kebutuhan mereka.

Data penggunaan pasca-workshop menunjukkan bahwa siswa memanfaatkan platform tidak hanya untuk mengulang materi yang telah dipelajari, tetapi juga sebagai referensi ketika menghadapi situasi digital yang meragukan. Hal ini mengindikasikan bahwa platform berfungsi sebagai sumber belajar mandiri yang adaptif terhadap kebutuhan aktual siswa.

Selain itu, fleksibilitas akses memungkinkan pembelajaran berlangsung di luar jam sekolah, memperkuat konsep pembelajaran sepanjang hayat. Platform ini juga membuka peluang pengembangan lebih lanjut, baik dari sisi penambahan skenario baru maupun integrasi dengan materi literasi digital lainnya yang relevan dengan perkembangan ancaman siber.

3.12 Dampak Program terhadap Lingkungan Sosial Sekolah

Dampak program tidak hanya dirasakan oleh peserta secara individual, tetapi juga mulai memengaruhi lingkungan sosial sekolah. Interaksi antar siswa setelah kegiatan menunjukkan adanya transfer pengetahuan secara informal, dimana peserta membagikan pengalaman dan pembelajaran mereka kepada teman yang tidak mengikuti workshop.

Fenomena ini menciptakan efek pengganda yang memperluas jangkauan program tanpa intervensi langsung dari tim pelaksana. Ketika siswa menjadi agen penyebar literasi keamanan digital, pesan keamanan menjadi lebih mudah diterima karena disampaikan melalui hubungan sebaya yang setara.

Lingkungan sekolah yang mulai terbiasa mendiskusikan isu keamanan digital juga berpotensi menciptakan norma baru, dimana kehati-hatian dalam aktivitas daring dianggap sebagai perilaku positif dan patut ditiru. Dalam jangka panjang, hal ini dapat berkontribusi pada pengurangan risiko insiden keamanan digital di lingkungan sekolah.

3.13 Keberlanjutan Program dalam Konteks Pengabdian Kepada Masyarakat

Sebagai kegiatan pengabdian kepada masyarakat, keberlanjutan menjadi aspek penting yang menentukan nilai jangka panjang program. Program PHISH-CHECK dirancang dengan mempertimbangkan keberlanjutan sejak tahap perencanaan, baik dari sisi teknologi maupun adopsi oleh mitra sekolah.

Ketersediaan platform berbasis web memungkinkan sekolah untuk terus memanfaatkan materi dan simulasi tanpa ketergantungan penuh pada kehadiran tim pengabdian. Guru dapat menggunakan platform sebagai media pendukung pembelajaran, sementara siswa dapat mengaksesnya secara mandiri sesuai kebutuhan.

Selain itu, potensi pengembangan program ke skala yang lebih luas terbuka dengan menyesuaikan konten terhadap konteks sekolah lain. Dengan pendekatan modular, program dapat direplikasi tanpa memerlukan sumber daya yang besar, sehingga relevan untuk diterapkan pada institusi pendidikan dengan keterbatasan sarana sekalipun.

DOI: https://doi.org/10.31004/riggs.v4i4.5304

3.14 Refleksi Pelaksanaan Program

Refleksi terhadap pelaksanaan program menunjukkan bahwa pendekatan interaktif dan kontekstual merupakan faktor kunci keberhasilan. Keterlibatan aktif siswa selama simulasi dan diskusi membuktikan bahwa pembelajaran keamanan digital akan lebih efektif ketika disampaikan melalui pengalaman langsung yang relevan dengan kehidupan mereka.

Namun demikian, refleksi juga mengungkapkan ruang untuk perbaikan. Perbedaan tingkat kemampuan awal siswa menuntut pendekatan yang lebih adaptif agar setiap peserta dapat memperoleh manfaat optimal. Pengembangan fitur diferensiasi atau jalur pembelajaran bertahap dapat menjadi pertimbangan pada implementasi berikutnya.

Refleksi ini menjadi dasar penting bagi penyempurnaan program di masa depan, sekaligus menegaskan bahwa pengabdian masyarakat merupakan proses pembelajaran dua arah, tidak hanya bagi peserta, tetapi juga bagi tim pelaksana.

Hasil kegiatan menunjukkan bahwa sebelum mengikuti program, sebagian besar siswa telah memiliki kesadaran awal terhadap keberadaan penipuan daring. Namun, kesadaran tersebut belum disertai kemampuan untuk mengidentifikasi indikator teknis phishing secara spesifik. Banyak siswa masih mengandalkan perasaan atau pengalaman pribadi dalam menilai keamanan suatu konten digital.

Setelah mengikuti simulasi interaktif pada platform PHISH-CHECK, siswa mulai menunjukkan peningkatan kemampuan analisis teknis. Pada skenario login palsu, siswa mampu mengidentifikasi perbedaan struktur URL, domain yang tidak sesuai, serta inkonsistensi elemen visual. Proses diskusi pasca-simulasi membantu siswa memahami alasan teknis di balik setiap indikator yang ditemukan.

Skenario undian hadiah dan formulir beasiswa memperkuat pemahaman siswa mengenai teknik manipulasi psikologis yang umum digunakan dalam phishing. Siswa mulai memahami pentingnya verifikasi sumber informasi, kewajaran permintaan data, serta konteks komunikasi digital. Hal ini menunjukkan pergeseran dari pendekatan intuitif menuju evaluasi yang lebih rasional dan sistematis.

Keterlibatan siswa yang berlanjut pada platform setelah workshop menunjukkan bahwa PHISH-CHECK memiliki potensi sebagai media pembelajaran mandiri. Siswa memanfaatkan platform untuk mengulang simulasi dan memperdalam pemahaman, yang sejalan dengan konsep pembelajaran berkelanjutan dalam literasi keamanan digital.

4. Kesimpulan

Pengembangan modul edukasi interaktif berbasis web melalui platform PHISH-CHECK terbukti mampu meningkatkan literasi keamanan digital siswa MA Raudlatul Hidayah, khususnya dalam mengenali dan mendeteksi ancaman phishing. Melalui pendekatan pembelajaran berbasis pengalaman dan simulasi interaktif, siswa tidak hanya memperoleh pemahaman konseptual mengenai phishing, tetapi juga mengembangkan kemampuan analisis teknis serta pola pikir sistematis dalam mengevaluasi konten digital yang berpotensi berbahaya. Hasil kegiatan menunjukkan adanya pergeseran signifikan dari pendekatan intuitif menuju pendekatan berbasis indikator konkret, seperti analisis struktur URL, verifikasi domain, serta identifikasi inkonsistensi visual dan permintaan data yang tidak wajar. Perubahan ini mencerminkan peningkatan kesadaran dan keterampilan praktis siswa dalam melindungi diri dari risiko keamanan digital yang semakin kompleks. Platform PHISH-CHECK tidak hanya berfungsi sebagai media pembelajaran selama kegiatan workshop, tetapi juga sebagai sarana pembelajaran mandiri yang mendukung penguatan literasi keamanan digital secara berkelanjutan. Tingkat keterlibatan pasca-kegiatan menunjukkan bahwa siswa memanfaatkan platform sebagai referensi dalam menghadapi situasi digital sehari-hari. Secara keseluruhan, program ini berpotensi direplikasi dan dikembangkan sebagai model edukasi keamanan siber berbasis sekolah. Dengan dukungan institusi dan integrasi ke dalam kegiatan pembelajaran, program PHISH-CHECK dapat berkontribusi dalam membangun generasi pelajar yang lebih sadar, kritis, dan siap menghadapi tantangan keamanan di era digital.

Referensi

1. Asosiasi Penyelenggara Jasa Internet Indonesia. (2023). Profil Pengguna Internet Indonesia 2023. Asosiasi Penyelenggara Jasa Internet Indonesia, Jakarta.
2. Badan Siber dan Sandi Negara. (2024). Laporan Tahunan Lanskap Keamanan Siber Indonesia 2023. Badan Siber dan Sandi Negara, Jakarta.
3. Febriyani, W., Fathia, D., Widjajarto, A., & Lubis, M. (2023). Security awareness strategy for phishing email scams: A case study of one company in Singapore. International Journal on Informatics Visualization, 7(3), 808–814.

DOI: https://doi.org/10.31004/riggs.v4i4.5304

4. Kurniawan, Y., Santoso, S. I., Wibowo, R. R., Anwar, N., Bhutkar, G., & Halim, E. (2023). Analysis of higher education students' awareness in Indonesia on personal data security in social media. Sustainability, 15(4), 3814. doi:10.3390/su15043814

5. Permadi, R., & Ramli, R. (2024). Analisis tingkat kesadaran keamanan informasi pada pelajar sekolah menengah. Jurnal Keamanan Informasi, 6(1), 12–22.

6. Nur'aini, R. J., & Simanjuntak, M. (2025). Phishing awareness and security concerns: Analyzing the role of anti-phishing knowledge and internet experience in online banking users. Jurnal Ilmiah Keluarga & Konsumen, 18(2), 121–133. doi:10.24156/jikk.2025.18.2.121

7. Kementerian Komunikasi dan Informatika Republik Indonesia. (2021). Modul Literasi Digital: Keamanan Digital. Jakarta: Kominfo RI.

8. Permadi, R. B., & Ramli, K. (2024). Analysis of measuring information security awareness for employees at institution XYZ. MALCOM: Indonesian Journal of Machine Learning and Computer Science, 4(4), 1330–1338. doi:10.57152/malcom.v4i4.1453

9. Prasetyo Eka Putra, F., Ubaidi, A., Zulfikri, A., Arifin, G., & Ilhamsyah, R. M. (2024). Analysis of phishing attack trends, impacts and prevention methods: Literature study. Brilliance: Research of Artificial Intelligence, 4(1), 413–422. doi:10.47709/brilliance.v4i1.4357

10. Suryani, N., & Sugiyanto. (2020). Pembelajaran berbasis simulasi untuk meningkatkan pemahaman siswa. Jurnal Inovasi Pendidikan, 7(1), 45–54.

11. Wahyudi, A., & Hidayat, T. (2021). Ancaman phishing dan upaya mitigasi pada pengguna internet pemula. Jurnal Sistem Informasi, 17(2), 98–107.

12. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. Proceedings of the 3rd Symposium on Usable Privacy and Security, 88-99. https://doi.org/10.1145/1280680.1280692

13. Yuliana, E., & Hartono, R. (2020). Literasi keamanan digital sebagai kompetensi abad ke-21. *Jurnal Pendidikan dan Kebudayaan*, 25(3), 321–330.

14. Zulfikar, M., & Kurniawan, D. (2021). Peran sekolah dalam membangun kesadaran keamanan siber siswa. Jurnal Pengabdian Masyarakat Bidang Pendidikan, 2(2), 101–109.

15. Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576-586. https://doi.org/10.1016/j.dss.2011.03.002

16. Haryanto, A., & Prasetyo, D. (2022). Tingkat literasi keamanan digital pada pengguna internet remaja di Indonesia. Jurnal Teknologi Informasi dan Pendidikan, 15(2), 134–142.

DOI: https://doi.org/10.31004/riggs.v4i4.5304