

URGENSI KEAMANAN SIBER: ANALISIS LITERASI DIGITAL DALAM MEMBENTENGI AKUN DIGITAL DARI ANCAMAN SOCIAL ENGINEERING

¹Ilzam Mantya Firlana, ²Izzul Ahmad Fathoni, ³Najwa Azkiatul Fadilah Al-fikriah, ⁴Sri Devi Komalasari ⁵Anton Nasrullah, ⁶Oktavianto Setyo Nugroho, ⁷Asnawi

¹Ilmu Komputer, ²Sistem Informasi, ³Pendidikan Guru Sekolah Dasar, ⁴Ilmu Pemerintahan, ⁵Pendidikan Matematika ⁶Ilmu Hukum, ⁷Ilmu Hukum

¹Ilmu Komputer, ²Ilmu Komputer, ³Keguruan dan Ilmu Pendidikan, ⁴Keguruan dan Ilmu Pendidikan, ⁵Hukum, ⁶Hukum

Universitas Bina Bangsa, Serang, Banten, Indonesia

[1*jkilzam@gmail.com](mailto:jkilzam@gmail.com), [2ahmadalhafizy@gmail.com](mailto:ahmadalhafizy@gmail.com), [3najwaafa14@gmail.com](mailto:najwaafa14@gmail.com),
[4sridevikomalasari16@gmail.com](mailto:sridevikomalasari16@gmail.com), [5anton.nasrullah@binabangsa.ac.id](mailto:anton.nasrullah@binabangsa.ac.id),
[6Oktavianto.setyo.nugroho@binabangsa.ac.id](mailto:Oktavianto.setyo.nugroho@binabangsa.ac.id) [7srgasnawi@gmail.com](mailto:srgasnawi@gmail.com).

Abstract

Digital literacy and account security are critical elements in mitigating the increasing wave of cyber threats in the modern digital era. As internet penetration and digital service adoption accelerate, cybercrimes such as phishing, social engineering, credential stuffing, and account takeover (ATO) have become increasingly sophisticated. This study aims to analyze the correlation between public digital literacy levels and vulnerability to cyberattacks, as well as to evaluate proactive mitigation strategies to secure digital accounts. Using a descriptive-analytical literature review and empirical data analysis from cybersecurity reports, the findings indicate that low digital literacy significantly increases user susceptibility to fraudulent social engineering tactics. Furthermore, weak password management and the absence of multi-factor authentication (MFA) remain primary vectors for security breaches. The study recommends strengthening comprehensive digital literacy education across formal and informal sectors, coupled with mandatory implementation of multi-factor authentication and behavioral analytics to safeguard personal and organizational accounts against emerging cyber threats.

Keywords: Digital Literacy; Account Security; Cybercrime; Phishing; Multi-Factor Authentication.

Abstrak

Literasi digital dan keamanan akun merupakan elemen krusial dalam memitigasi gelombang ancaman kejahatan siber yang kian meningkat di era digital modern. Seiring dengan percepatan penetrasi internet dan adopsi layanan digital, kejahatan siber seperti *phishing*, rekayasa sosial (*social engineering*), *credential stuffing*, dan pengambilalihan akun (*account takeover/ATO*) menjadi semakin canggih. Penelitian ini bertujuan untuk menganalisis korelasi antara tingkat literasi digital masyarakat dan kerentanan terhadap serangan siber, serta mengevaluasi strategi mitigasi proaktif untuk mengamankan akun digital. Menggunakan metode tinjauan pustaka deskriptif-analitis dan analisis data empiris dari laporan keamanan siber, hasil penelitian menunjukkan bahwa rendahnya literasi digital secara signifikan meningkatkan kerentanan pengguna terhadap taktik penipuan rekayasa sosial. Selain itu, manajemen kata sandi yang lemah dan ketiadaan autentikasi multifaktor (MFA) tetap menjadi vektor utama terjadinya pembobolan keamanan. Penelitian ini merekomendasikan penguatan edukasi literasi digital yang komprehensif di sektor formal maupun informal, disertai penerapan wajib autentikasi multifaktor dan analisis perilaku untuk melindungi akun pribadi maupun organisasi dari ancaman siber yang berkembang.

Kata kunci: Literasi Digital; Keamanan Akun; Kejahatan Siber; *Phishing*; Autentikasi Multifaktor.

PENDAHULUAN

Transformasi digital telah mengubah pola interaksi masyarakat dalam menjalankan berbagai aktivitas sehari-hari. Internet tidak lagi hanya digunakan sebagai sarana mencari informasi, tetapi telah menjadi bagian dari aktivitas pendidikan, komunikasi, perdagangan, transaksi keuangan, pelayanan publik, pekerjaan, hiburan, dan penyimpanan data pribadi. Perkembangan tersebut menyebabkan semakin banyak individu memiliki akun pada berbagai platform digital. Akun surat elektronik, media sosial, aplikasi perbankan, dompet digital, marketplace, sistem akademik, serta berbagai layanan berbasis cloud menyimpan informasi yang bernilai bagi pemilik maupun pihak lain. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) melaporkan bahwa jumlah pengguna internet Indonesia pada tahun 2024 mencapai 221.563.479 jiwa atau sekitar 79,5% dari populasi. Angka tersebut menunjukkan bahwa internet telah menjadi bagian penting dari kehidupan masyarakat Indonesia [1]. Peningkatan jumlah pengguna internet sekaligus menunjukkan semakin luasnya permukaan serangan yang dapat dimanfaatkan oleh pelaku kejahatan siber. Semakin banyak masyarakat menggunakan layanan digital, semakin besar pula kebutuhan terhadap kemampuan menjaga keamanan identitas dan akun digital. Peningkatan penggunaan teknologi tidak selalu diikuti oleh peningkatan pemahaman mengenai keamanan digital. Pengguna dapat memiliki kemampuan menggunakan aplikasi, media sosial, mesin pencari, dan layanan digital, tetapi belum tentu memiliki kemampuan untuk mengenali ancaman siber. Kondisi tersebut menunjukkan bahwa literasi digital tidak cukup dipahami sebagai kemampuan mengoperasikan perangkat atau aplikasi. Literasi digital juga mencakup kemampuan berpikir kritis, memahami risiko, menjaga privasi, melakukan verifikasi informasi, serta mengambil keputusan yang aman ketika berinteraksi di ruang digital. Kondisi tersebut relevan dengan hasil penelitian Oktapiyadi, Saepudin, dan Yanto yang menunjukkan adanya hubungan signifikan antara literasi digital dengan perilaku keamanan siber pada mahasiswa. Meskipun hubungan yang ditemukan berada pada tingkat rendah, hasil tersebut menunjukkan bahwa literasi digital tetap menjadi salah satu aspek yang berhubungan dengan perilaku keamanan siber pengguna [1]. Temuan tersebut sekaligus menunjukkan bahwa peningkatan pengetahuan perlu disertai pembentukan perilaku keamanan yang dapat diterapkan dalam aktivitas digital sehari-hari. Permasalahan keamanan digital semakin kompleks karena pelaku kejahatan tidak selalu membutuhkan

kemampuan teknis yang sangat tinggi untuk menyerang korban. Salah satu pendekatan yang banyak digunakan adalah social engineering. ENISA menjelaskan bahwa social engineering mencakup berbagai aktivitas yang bertujuan mengeksploitasi kesalahan atau perilaku manusia agar korban memberikan informasi sensitif, membuka dokumen, mengakses situs, atau memberikan akses terhadap layanan tertentu [2]. Dengan demikian, manusia menjadi bagian penting dalam rantai keamanan siber.

Phishing merupakan salah satu bentuk social engineering yang memanfaatkan pesan atau halaman palsu untuk mengarahkan pengguna agar menyerahkan informasi tertentu. Pesan dapat dibuat menyerupai komunikasi resmi dari bank, marketplace, media sosial, lembaga pendidikan, perusahaan, atau bahkan seseorang yang dikenal korban. Teknik tersebut memanfaatkan kepercayaan pengguna terhadap identitas atau merek tertentu. Penelitian mengenai keamanan media sosial menunjukkan bahwa phishing dapat dilakukan melalui pembuatan halaman yang menyerupai layanan asli serta penggunaan email spoofing sebagai sarana distribusi tautan berbahaya [3].

Selain phishing, ancaman social engineering juga dapat muncul dalam bentuk smishing dan vishing. Smishing menggunakan pesan singkat atau aplikasi komunikasi, sedangkan vishing menggunakan komunikasi suara atau telepon. Pelaku dapat menggunakan narasi mengenai hadiah, pengembalian dana, verifikasi akun, transaksi mencurigakan, perubahan kebijakan, pemblokiran akun, atau kebutuhan mendesak lainnya. Tujuan akhirnya adalah membuat korban mengambil keputusan secara cepat tanpa melakukan verifikasi.

Perkembangan kecerdasan buatan juga menambah kompleksitas ancaman. World Economic Forum melaporkan bahwa perkembangan teknologi generative artificial intelligence dapat meningkatkan kemampuan pelaku kejahatan dalam membuat serangan social engineering yang lebih meyakinkan dan berskala lebih besar. Dalam Global Cybersecurity Outlook 2025, sebanyak 42% organisasi yang disurvei melaporkan adanya peningkatan phishing dan social engineering pada 2024, sementara hampir 47% organisasi menyebut kemajuan adversarial berbasis GenAI sebagai salah satu kekhawatiran utama [4].

Laporan Global Cybersecurity Outlook 2026 juga menunjukkan bahwa cyber-enabled fraud dan phishing menjadi perhatian utama para pemimpin organisasi. Sebanyak 77% responden melaporkan peningkatan cyber-enabled fraud dan

phishing secara keseluruhan, sedangkan bentuk serangan yang banyak dilaporkan meliputi phishing, termasuk vishing dan smishing, payment fraud, dan identity theft [4].

Data tersebut memperlihatkan bahwa edukasi keamanan siber kepada masyarakat tidak dapat hanya menitikberatkan pada aspek teknis. Pengguna perlu diberikan pemahaman mengenai bagaimana pelaku membangun skenario penipuan, bagaimana mengenali tanda-tanda pesan mencurigakan, bagaimana melakukan verifikasi, serta tindakan apa yang harus dilakukan ketika menerima pesan atau tautan yang tidak dikenal.

Dalam konteks keamanan akun, kata sandi menjadi salah satu komponen yang sangat penting. Penggunaan kata sandi yang sama pada banyak layanan dapat meningkatkan risiko karena apabila satu layanan mengalami kebocoran kredensial, informasi tersebut dapat dicoba kembali pada layanan lain. Ancaman tersebut dikenal sebagai credential stuffing. Selain itu, penggunaan kata sandi yang mudah ditebak juga meningkatkan kemungkinan terjadinya pengambilalihan akun.

National Institute of Standards and Technology (NIST) merekomendasikan penggunaan autentikasi multifaktor sebagai salah satu langkah penting untuk meningkatkan keamanan akun. NIST juga menjelaskan bahwa phishing merupakan salah satu cara umum untuk memperoleh kata sandi dengan cara menipu pengguna agar memasukkan kredensial pada situs yang dikendalikan penyerang [5].

Laporan Verizon Data Breach Investigations Report juga menunjukkan pentingnya faktor manusia dalam keamanan siber. Laporan tersebut menempatkan phishing dan pretexting sebagai pola yang penting dalam insiden social engineering serta merekomendasikan penggunaan MFA, pembaruan perangkat lunak, pelatihan pengguna, perlindungan data, pengujian pertahanan, dan perencanaan respons insiden [6].

Di Indonesia, kebutuhan terhadap literasi keamanan siber juga semakin relevan. Kementerian Komunikasi dan Digital menekankan pentingnya penguatan literasi digital dan keamanan siber seiring dengan perkembangan transformasi digital. Tantangan ruang digital tidak hanya berupa hoaks dan cyberbullying, tetapi juga kejahatan siber yang membutuhkan kemampuan pengguna dalam menjaga keamanan dirinya [7].

Penelitian mengenai masyarakat pedesaan di Indonesia juga menunjukkan bahwa literasi digital, khususnya terkait keamanan siber, masih menjadi tantangan. Hasil penelitian tersebut menemukan adanya kekurangan pemahaman mengenai phishing, malware, dan privasi data, serta

merekomendasikan program literasi digital berbasis komunitas yang memberikan keterampilan praktis seperti membuat kata sandi yang kuat dan mengenali upaya phishing [8].

Temuan tersebut memperkuat alasan pelaksanaan kegiatan pengabdian kepada masyarakat yang mengangkat tema keamanan akun digital. Edukasi perlu dilakukan dengan pendekatan sederhana, komunikatif, dan praktis agar peserta tidak hanya memahami definisi ancaman siber, tetapi juga dapat menerapkan langkah perlindungan secara mandiri.

Tujuan kegiatan pengabdian kepada masyarakat ini adalah meningkatkan pemahaman peserta mengenai ancaman social engineering, meningkatkan kemampuan peserta dalam mengidentifikasi pesan atau tautan mencurigakan, meningkatkan kesadaran terhadap pentingnya menjaga data pribadi dan kredensial, serta mendorong penerapan praktik keamanan akun seperti penggunaan kata sandi yang kuat dan unik serta MFA.

Manfaat kegiatan diharapkan dapat dirasakan secara langsung oleh peserta dalam aktivitas digital sehari-hari. Peserta diharapkan mampu menerapkan prinsip berhenti, periksa, dan verifikasi sebelum membuka tautan atau memberikan informasi pribadi. Selain itu, peserta diharapkan mampu mengenali pola manipulasi psikologis yang digunakan dalam social engineering sehingga tidak mudah mengambil keputusan berdasarkan rasa takut, panik, rasa ingin tahu, atau iming-iming keuntungan.

Dengan demikian, kegiatan pengabdian ini tidak hanya berorientasi pada penyampaian informasi, tetapi juga pada perubahan perilaku keamanan digital. Pendekatan tersebut penting karena keamanan akun merupakan tanggung jawab bersama antara penyedia layanan, pengembang sistem, organisasi, dan pengguna [9].

METODE PENGABDIAN MASYARAKAT

2.1 Lokasi, Waktu, dan Sasaran Kegiatan

Kegiatan pengabdian kepada masyarakat, dilaksanakan di (KANTOR DESA/TAMBILUK/UNIVERSITAS BINA BANGSA /PETIR), (KABUPATEN SERANG), Provinsi Banten pada (25-JULI-2026).

Sasaran kegiatan adalah MASYARAKAT yang aktif menggunakan perangkat digital dan layanan internet dalam kehidupan sehari-hari. Jumlah peserta yang mengikuti kegiatan sebanyak 60 peserta.

Pemilihan sasaran didasarkan pada tingginya ketergantungan masyarakat terhadap perangkat digital serta pentingnya kemampuan menjaga akun dan data pribadi. Kegiatan dirancang agar materi dapat diterapkan oleh peserta tanpa membutuhkan latar belakang teknis di bidang komputer atau keamanan siber.

2.2 Tahapan Pelaksanaan

Metode pengabdian terdiri atas tahap identifikasi masalah, persiapan materi, pelaksanaan edukasi, simulasi dan praktik, evaluasi, serta pendampingan. Tahap pertama adalah identifikasi masalah. Tim melakukan observasi dan komunikasi awal dengan pihak perangkat desa untuk mengetahui kebiasaan peserta dalam menggunakan internet, jenis akun digital yang banyak digunakan, pemahaman terhadap phishing, kebiasaan penggunaan kata sandi, serta penggunaan MFA.

Tahap kedua adalah penyusunan materi. Materi disusun berdasarkan hasil identifikasi kebutuhan serta literatur mengenai keamanan siber. Materi meliputi pengertian keamanan siber, keamanan akun digital, data pribadi, social engineering, phishing, smishing, vishing, credential stuffing, account takeover, keamanan kata sandi, MFA, verifikasi tautan, dan langkah pelaporan apabila mengalami penipuan.

Tahap ketiga adalah penyampaian materi melalui ceramah interaktif. Metode ceramah digunakan untuk menyampaikan konsep dasar secara sistematis. Agar peserta tidak hanya menerima informasi secara satu arah, penyampaian materi disertai pertanyaan pemantik dan contoh kasus yang dekat dengan kehidupan sehari-hari.

Tahap keempat adalah tanya jawab dan diskusi. Peserta diberikan kesempatan untuk menyampaikan pengalaman ketika menerima pesan mencurigakan, menerima telepon yang mengatasnamakan lembaga tertentu, mendapatkan permintaan kode OTP, atau menerima tautan hadiah dan promosi. Diskusi diarahkan untuk mengidentifikasi kesalahan dan menentukan tindakan yang lebih aman.

Tahap kelima adalah simulasi. Peserta diberikan beberapa contoh pesan digital yang telah dibuat khusus untuk kebutuhan pembelajaran. Pesan tersebut tidak menggunakan akun, data, kredensial, atau tautan nyata milik peserta. Peserta diminta mengidentifikasi indikator yang menunjukkan bahwa suatu pesan berpotensi menjadi phishing atau social engineering.

Tahap keenam adalah praktik keamanan akun. Peserta diarahkan untuk memeriksa pengaturan keamanan akun masing-masing, meninjau penggunaan kata sandi, memeriksa opsi MFA, serta memahami cara melakukan pemulihan akun. Praktik dilakukan tanpa meminta peserta

menyampaikan kata sandi, kode OTP, PIN, atau informasi autentikasi kepada tim pengabdian.

Tahap ketujuh adalah evaluasi. Evaluasi dilakukan melalui pre-test dan post-test untuk mengukur perubahan pengetahuan peserta. Evaluasi persepsi peserta terhadap kegiatan dilakukan melalui kuesioner skala Likert [10].

2.3 Materi Pelatihan

Materi utama kegiatan disusun dalam beberapa pokok bahasan. Pertama adalah pengenalan keamanan siber dan keamanan akun digital. Peserta diberikan pemahaman bahwa keamanan akun tidak hanya berkaitan dengan sistem komputer, tetapi juga kebiasaan pengguna.

Kedua adalah pengenalan social engineering. Peserta dijelaskan bahwa pelaku dapat memanfaatkan kondisi psikologis seperti rasa takut, rasa percaya, urgensi, otoritas, rasa ingin tahu, dan keinginan memperoleh keuntungan.

Ketiga adalah pengenalan phishing. Peserta diberikan contoh ciri-ciri pesan mencurigakan, antara lain adanya permintaan login, permintaan data pribadi, ancaman pemblokiran akun, hadiah yang tidak wajar, penggunaan bahasa yang mendesak, alamat pengirim yang tidak sesuai, domain yang mencurigakan, serta tautan yang tidak mengarah ke layanan resmi.

Keempat adalah keamanan kata sandi. Peserta diberikan pemahaman mengenai pentingnya kata sandi yang panjang, sulit ditebak, dan tidak digunakan kembali pada banyak layanan. Peserta juga diberikan pemahaman mengenai risiko menggunakan kata sandi yang sama untuk email, media sosial, marketplace, dan layanan keuangan.

Kelima adalah MFA. Peserta diberikan penjelasan mengenai konsep autentikasi berlapis dan manfaatnya dalam mengurangi risiko pengambilalihan akun. NIST merekomendasikan MFA sebagai salah satu langkah penting untuk memperkuat keamanan akun [5].

Keenam adalah respons terhadap insiden. Peserta diberikan langkah yang dapat dilakukan ketika merasa menjadi korban, antara lain menghentikan komunikasi dengan pelaku, tidak memberikan kode OTP atau kredensial tambahan, mengganti kata sandi melalui aplikasi atau situs resmi, mengaktifkan MFA, memeriksa aktivitas login, serta menghubungi penyedia layanan melalui kanal resmi [11].

Panjang Naskah

“OPTIMALISASI PELAYANAN PUBLIK DESA BERBASIS DIGITAL MELALUI EDUKASI ADMINISTRASI DAN LITERASI DIGITAL”

Tabel 1. Indikator Identifikasi Pesan Berpotensi Phishing

Indikator	Contoh Kondisi	Tindakan Aman
Permintaan OTP	Pengirim meminta kode OTP untuk verifikasi	Jangan memberikan OTP
Tautan mencurigakan	Alamat situs tidak sesuai layanan resmi	Jangan membuka
Bahasa mendesak	"Akun akan ditutup dalam 10 menit"	Lakukan verifikasi
Hadiah tidak wajar	Mendapat hadiah tanpa mengikuti program	Jangan memberikan data
Identitas tidak jelas	Pengirim mengaku sebagai petugas	Hubungi kanal resmi
Permintaan kata sandi	Pengirim meminta password	Jangan memberikan
Lampiran tidak dikenal	File dikirim tanpa konteks jelas	Jangan membuka sebelum diverifikasi



Sumber: (BIDANG 5 Tata Kelola Pemerintahan Desa/Kelurahan Pelayanan Publik dan Inovasi Teknologi,2026)

Gambar 1. Foto Bidang Ke-5 Bersama Narasumber



Gambar 2. Foto Bersama

Sumber: (KKM 41 TAMBILUK,2026)


 Gambar 3. Foto Narasumber
Sumber: (Faisal Akhmad, S.Kom., M.T.I,2026)

 Sumber: (Faisal Akhmad, S.Kom., M.T.I,2026)
Gambar 3. Penyerahan Sertifikat Kepada Narasumber

HASIL DAN PEMBAHASAN

3.1 Kondisi Awal Peserta

Berdasarkan hasil identifikasi awal, penggunaan perangkat digital telah menjadi bagian dari aktivitas peserta. Peserta menggunakan perangkat digital untuk **LITERASI DIGITAL**.

Permasalahan utama yang menjadi perhatian adalah masih adanya peserta yang belum memahami bahwa keamanan akun tidak cukup hanya dilakukan dengan menggunakan kata sandi. Dalam praktiknya, keamanan akun juga dipengaruhi oleh kebiasaan pengguna ketika menerima pesan, membuka tautan, mengunduh dokumen, memberikan informasi pribadi, dan menggunakan kode autentikasi.

Temuan tersebut sejalan dengan penelitian mengenai masyarakat pedesaan yang menunjukkan

adanya kesenjangan pemahaman terhadap phishing, malware, dan privasi data [8]. Hasil tersebut menunjukkan bahwa edukasi keamanan digital perlu diarahkan pada keterampilan praktis, bukan hanya pemahaman terminologi[12].

3.2 Pelaksanaan Edukasi Keamanan Siber

Kegiatan diawali dengan pembukaan dan penyampaian tujuan. Peserta diberikan pemahaman bahwa keamanan siber bukan hanya tanggung jawab ahli teknologi informasi. Setiap pengguna akun digital mempunyai peran dalam menjaga keamanan informasi pribadi.

Pada sesi pertama, pemateri menjelaskan konsep dasar keamanan siber. Materi difokuskan pada tiga aspek utama, yaitu kerahasiaan, integritas, dan ketersediaan informasi. Peserta kemudian diajak menghubungkan ketiga konsep tersebut dengan aktivitas sehari-hari.

Pada sesi kedua, pemateri menjelaskan social engineering. Penjelasan menggunakan pendekatan berbasis kasus agar peserta dapat memahami bahwa pelaku tidak selalu menyerang sistem secara langsung. Pelaku dapat terlebih dahulu memanipulasi korban untuk memberikan informasi atau melakukan tindakan tertentu [13].

ENISA menjelaskan social engineering sebagai aktivitas yang mengeksploitasi perilaku manusia untuk memperoleh informasi atau akses [2]. Pendekatan ini membuat edukasi menjadi penting karena teknologi keamanan yang baik dapat tetap menghadapi risiko apabila pengguna memberikan kredensial secara sukarela kepada pihak yang salah. Pada sesi ketiga, peserta diperkenalkan dengan phishing. Pemateri memberikan beberapa contoh pesan yang memiliki karakteristik berbeda. Peserta diminta menentukan apakah pesan tersebut aman, mencurigakan, atau berpotensi phishing.

Beberapa indikator yang diperhatikan meliputi alamat pengirim, gaya bahasa, penggunaan ancaman, permintaan informasi pribadi, permintaan kode OTP, tautan yang tidak sesuai, serta adanya tekanan waktu[14].

3.3 Simulasi Identifikasi Phishing

Simulasi dilakukan menggunakan contoh pesan yang dibuat khusus untuk kegiatan. Contoh tidak menggunakan kredensial nyata dan tidak mengarahkan peserta ke situs berbahaya.

Tabel 1 menunjukkan contoh indikator yang digunakan dalam simulasi. Tabel 1. Indikator Identifikasi Pesan Berpotensi Phishing

Indikator	Contoh Kondisi	Tindakan Aman
Permintaan OTP	Pengirim meminta kode OTP untuk verifikasi	Jangan memberikan OTP

Tautan mencurigakan	Alamat situs tidak sesuai layanan resmi	Jangan membuka
Bahasa mendesak	"Akun akan ditutup dalam 10 menit"	Lakukan verifikasi
Hadiah tidak wajar	Mendapat hadiah tanpa mengikuti program	Jangan memberikan data
Identitas tidak jelas	Pengirim mengaku sebagai petugas	Hubungi kanal resmi
Permintaan kata sandi	Pengirim meminta password	Jangan memberikan
Lampiran tidak dikenal	File dikirim tanpa konteks jelas	Jangan membuka sebelum diverifikasi

Sumber: Dokumentasi Penulis, 2026.

Hasil simulasi menunjukkan bahwa peserta perlu dibiasakan untuk tidak langsung mempercayai pesan hanya karena menggunakan logo atau nama lembaga yang dikenal. Identitas visual dapat ditiru dan digunakan untuk meningkatkan kepercayaan korban[15].

Penelitian Ansyafa dkk. juga menunjukkan bahwa phishing dapat menggunakan halaman yang menyerupai layanan media sosial dan distribusi melalui email spoofing [3]. Kondisi tersebut menunjukkan bahwa tampilan yang terlihat resmi tidak dapat dijadikan satu-satunya dasar untuk menentukan keamanan sebuah komunikasi.

3.4 Praktik Pengamanan Akun

Setelah simulasi, kegiatan dilanjutkan dengan praktik pengamanan akun. Peserta diarahkan untuk memeriksa pengaturan keamanan pada akun masing-masing.

Praktik meliputi pemeriksaan penggunaan kata sandi, pemeriksaan perangkat yang pernah digunakan untuk login, pemeriksaan aktivitas login, serta pemeriksaan ketersediaan MFA.

Peserta tidak diminta untuk menyerahkan password, PIN, OTP, kode pemulihan, atau informasi autentikasi kepada tim. Prinsip tersebut ditekan agar kegiatan edukasi keamanan tidak justru menciptakan risiko baru terhadap privasi peserta.

NIST merekomendasikan MFA sebagai langkah penting dalam meningkatkan keamanan akun [5]. Penggunaan MFA memberikan lapisan autentikasi tambahan sehingga kata sandi yang diketahui pihak lain tidak selalu cukup untuk mendapatkan akses.

Verizon juga menempatkan MFA dan pelatihan pengguna sebagai bagian dari strategi pencegahan terhadap insiden keamanan [16]. Dengan demikian, edukasi yang diberikan dalam kegiatan ini menggabungkan aspek manusia dan aspek teknik

3.5 Pembahasan

Hasil kegiatan memperlihatkan bahwa edukasi keamanan siber perlu menggabungkan pengetahuan konseptual dengan latihan praktis. Peserta tidak cukup hanya mengetahui definisi phishing, tetapi perlu mampu mengenali tandatandanya ketika berhadapan dengan pesan digital. Hal tersebut menjadi semakin penting karena teknik social engineering berkembang mengikuti pola komunikasi masyarakat. Pelaku tidak hanya menggunakan email, tetapi juga dapat menggunakan pesan singkat, media sosial, telepon, aplikasi komunikasi, dan platform digital lainnya.

World Economic Forum menekankan bahwa perkembangan AI dapat meningkatkan kemampuan pelaku dalam membuat phishing dan social engineering menjadi lebih meyakinkan [17]. Oleh sebab itu, pendekatan edukasi harus menekankan proses berpikir kritis, bukan hanya menghafalkan ciri-ciri pesan phishing.

Peserta perlu dibiasakan mengajukan beberapa pertanyaan sebelum melakukan tindakan. Pertanyaan tersebut antara lain: siapa pengirimnya, mengapa pesan dikirim, apakah permintaan tersebut masuk akal, apakah tautan benar-benar berasal dari layanan resmi, apakah terdapat tekanan waktu, serta apakah informasi dapat diverifikasi melalui kanal resmi. Pendekatan tersebut dapat diringkas dalam prinsip "berhenti, periksa, dan verifikasi". Berhenti berarti tidak langsung mengikuti instruksi pesan. Periksa berarti melihat identitas pengirim, isi pesan, alamat situs, serta konteks komunikasi. Verifikasi berarti menghubungi pihak yang sebenarnya melalui kanal resmi [18].

Kegiatan juga menekankan pentingnya pengelolaan kata sandi. Pengguna sering kali memilih kata sandi yang mudah diingat dan menggunakan kata sandi yang sama pada berbagai layanan. Kebiasaan tersebut berisiko karena satu kebocoran dapat berdampak pada banyak akun.

Keamanan kata sandi perlu disertai MFA. MFA memberikan perlindungan tambahan ketika password diketahui pihak lain. NIST secara khusus menempatkan MFA sebagai langkah penting untuk meningkatkan keamanan akun [5]. Dengan demikian, edukasi mengenai password dan MFA harus dilakukan secara bersamaan.

Hubungan antara literasi digital dan keamanan siber juga didukung oleh penelitian Oktapiyadi dkk. yang menunjukkan hubungan signifikan antara dimensi literasi digital dan perilaku keamanan siber mahasiswa [1]. Meskipun hubungan tersebut tidak kuat, hasil penelitian menunjukkan bahwa

kemampuan digital memiliki keterkaitan dengan perilaku keamanan.

Penelitian Iskandar dkk. terhadap mahasiswa PTKI di Indonesia juga menunjukkan bahwa tingkat literasi digital berada pada level sedang dan terdapat ruang perbaikan pada sejumlah dimensi literasi digital [19]. Temuan tersebut memperlihatkan bahwa pendidikan literasi digital masih diperlukan bahkan pada kelompok masyarakat yang telah terbiasa menggunakan teknologi. Kegiatan pengabdian juga memiliki kesesuaian dengan penelitian pengabdian sebelumnya. Giap dkk. melaksanakan kegiatan edukasi keamanan siber di lingkungan sekolah melalui ceramah interaktif, diskusi, tanya jawab, dan pendampingan. Hasil kegiatan tersebut menunjukkan adanya peningkatan pemahaman peserta mengenai ancaman keamanan digital [16]. Pendekatan tersebut mendukung penggunaan metode interaktif dalam kegiatan ini.

Dengan demikian, metode ceramah saja tidak cukup. Ceramah digunakan untuk membangun dasar pengetahuan, sedangkan diskusi dan simulasi digunakan untuk melatih kemampuan berpikir kritis. Praktik digunakan untuk membantu peserta menerapkan pengetahuan pada pengaturan keamanan akun.

Penguatan Soft Skill dan Kecerdasan Emosional di Ruang Digital. Sesi ini difasilitasi oleh Endi Sutrisna dan Dethia Hs Suci Nurani. Materi bersifat aplikatif dan meliputi: (a) teknik pengelolaan emosi (emotion regulation) dan stres khususnya saat berinteraksi di media sosial; (b) literasi digital kritis untuk mengidentifikasi hoaks, ujaran kebencian, dan konten berbahaya; (c) praktik komunikasi empatik dan asertif dalam jaringan untuk mencegah dan menangani konflik (cyberbullying); serta (d) perencanaan penggunaan media sosial yang positif dan produktif untuk pengembangan diri [20].

3.6 Faktor Pendukung dan Penghambat

Faktor pendukung kegiatan adalah tingginya penggunaan perangkat digital oleh peserta, relevansi topik dengan kehidupan sehari-hari, serta tersedianya perangkat smartphone yang dapat digunakan untuk praktik.

Faktor lain yang mendukung adalah meningkatnya perhatian masyarakat terhadap keamanan data pribadi dan penipuan digital. Peserta dapat menghubungkan materi dengan pengalaman yang pernah mereka alami.

Adapun faktor penghambat yang perlu diperhatikan adalah perbedaan tingkat kemampuan digital peserta. Peserta yang telah terbiasa menggunakan

layanan digital dapat memahami materi lebih cepat dibandingkan peserta yang masih terbatas dalam penggunaan teknologi.

Keterbatasan waktu juga dapat menjadi kendala dalam praktik pengamanan akun. Beberapa peserta mungkin menggunakan layanan digital yang berbeda sehingga instruksi pengaturan MFA atau keamanan akun tidak selalu sama.

Oleh karena itu, kegiatan lanjutan perlu menyediakan modul sederhana yang dapat digunakan peserta secara mandiri setelah kegiatan selesai.

3.7 Rencana Keberlanjutan Program

Program literasi keamanan siber sebaiknya tidak berhenti pada satu kali penyuluhan. Ancaman siber terus berkembang sehingga materi edukasi perlu diperbarui secara berkala.

Keberlanjutan kegiatan dapat dilakukan melalui penyebaran modul keamanan digital, poster edukasi, video singkat, pendampingan berkala, dan pembentukan kelompok kecil yang berfungsi sebagai penggerak literasi digital di lingkungan masyarakat.

Materi lanjutan dapat mencakup keamanan media sosial, keamanan transaksi digital, keamanan perangkat smartphone, privasi digital, pengenalan deepfake, keamanan Wi-Fi, pengelolaan aplikasi, dan prosedur pelaporan insiden.

Pengembangan program juga dapat diarahkan pada simulasi berkala. Peserta diberikan contoh kasus baru sehingga kemampuan mengenali pola manipulasi dapat terus dilatih.

KESIMPULAN

Kegiatan pengabdian kepada masyarakat mengenai literasi digital dan keamanan akun digital memiliki relevansi yang tinggi dengan perkembangan penggunaan internet dan meningkatnya ancaman social engineering. Social engineering memanfaatkan aspek manusia sehingga perlindungan akun tidak cukup dilakukan hanya dengan teknologi, tetapi harus disertai peningkatan pengetahuan dan perilaku pengguna.

Materi utama yang perlu dikuasai masyarakat meliputi pengenalan social engineering, phishing, smishing, vishing, keamanan kata sandi, perlindungan data pribadi, verifikasi informasi, serta penggunaan MFA. Pendekatan ceramah interaktif, tanya jawab, diskusi, simulasi, dan praktik dapat digunakan untuk membantu peserta memahami sekaligus menerapkan konsep keamanan digital.

Kegiatan ini juga menunjukkan pentingnya mengubah pola edukasi dari sekadar penyampaian definisi menuju pembelajaran berbasis kasus.

Peserta perlu dilatih untuk mengenali pola manipulasi, melakukan verifikasi, dan mengambil keputusan secara hati-hati sebelum memberikan informasi atau mengakses tautan.

Evaluasi menggunakan pre-test dan post-test serta skala Likert dapat digunakan untuk mengukur keberhasilan program secara objektif. Nilai hasil evaluasi aktual perlu dimasukkan berdasarkan data lapangan kegiatan KKM sehingga persentase peningkatan dan tingkat kepuasan peserta dapat dipertanggungjawabkan secara akademik. Program lanjutan disarankan dilakukan secara berkala dengan materi yang diperbarui mengikuti perkembangan ancaman siber. Edukasi dapat dikembangkan menjadi modul, poster, video pendek, simulasi phishing yang aman, serta pendampingan keamanan akun. Dengan pendekatan berkelanjutan, masyarakat diharapkan tidak hanya menjadi pengguna teknologi yang aktif, tetapi juga menjadi pengguna yang kritis, waspada, dan bertanggung jawab terhadap keamanan informasi pribadi.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada (UNIVERSITAS BINA BANGSA), (Dr. Anton Nasrullah., S.Pd. M.Pd.) (Desa Tambiluk) serta seluruh peserta yang telah mendukung pelaksanaan kegiatan pengabdian kepada masyarakat ini.

Ucapan terima kasih juga disampaikan kepada pihak yang telah membantu menyediakan tempat, fasilitas, perangkat pendukung, serta memberikan dukungan selama proses persiapan dan pelaksanaan kegiatan.

DAFTAR PUSTAKA

- [1] W. Oktapiyadi, E. Saepudin, and A. Yanto, "HUBUNGAN LITERASI DIGITAL DENGAN PERILAKU," vol. 5, pp. 164–180, 2024, doi: 10.24036/ib.v5i2.464.
- [2] C. Ciuchi, "Operationalizing the Cyber Threat Landscape: Key Considerations and Challenges in Developing a Specific Organizational Program," vol. XI, pp. 61–68, 2024.
- [3] D. Fata, "ANALISIS KEAMANAN INFORMASI PENGGUNA MEDIA SOSIAL," vol. 2, no. 1, pp. 21–28, 2021.
- [4] A. Myrsalieva, E. Abdrakhmanova, and M. Moldomyrzaev, *The Role of Cyberattacks in Political and Economic Stability: Transforming National and International Approaches*, no. 2. 2026.
- [5] K. Labunets and R. Pouw, "Department of Information and Computing Science Human Computer Interaction master thesis More Factors, More Problems: Multi-Factor

- Authentication Usability in Educational Institutions First supervisor : Jan van Acken Second supervisor : Eelco Herder Candidate : Internship supervisor :," 2026.
- [6] K. Khadka, "Forecasting Risks, Challenges, and Innovations: A Cybersecurity Perspective".
- [7] D. Bagi, P. Dan, A. Di, K. Komunikasi, and D. A. N. Digital, "Peran kepemimpinan meutya hafid dalam mendorong kebijakan perlindungan digital bagi perempuan dan anak di kementerian komunikasi dan digital (2024 – 2026)," vol. 12, no. 2, 2026.
- [8] S. W. Dananjoyo, Y. P. Widhoyoko, and W. L. Mahadewa, "L I T E R A S I D I G I T A L D I K A L A N G A N M A S Y A R A K A T P E D E S A A N : U P A Y A M E N N I N G K A T K A N K E S A D A R A N," vol. 1, no. 2, pp. 1–9, 2022.
- [9] R. Hidayat and N. Anwar, "FORENSIC ANALYSIS OF WEB PHISHING AND SOCIAL ENGINEERING USING THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY METHOD CASE STUDY," vol. 1, pp. 12–25, 2024, doi: 10.29121/DigiSecForensics.v1.i1.202.
- [10] R. Wijaya, D. Juardi, and T. Timur, "Edukasi masyarakat tentang keamanan siber dalam tantangan dan solusi di era digital," vol. 14, no. 1, pp. 298–305.
- [11] N. A. Istiqomah and N. A. Lorenza, "Pustakaloka THE IMPACT OF DIGITAL LITERACY ON PHISHING PREVENTION BEHAVIOUR : A LITERATURE REVIEW," vol. 17, no. 2, pp. 102–125, 2025, doi: 10.21154/pustakaloka.v17i2.10495.
- [12] E. Sutrisna *et al.*, "No Title," vol. 2, no. 1, pp. 131–138, 2026.
- [13] M. Schmitt and I. Flechais, "Digital deception : generative artificial intelligence in social engineering and phishing," 2024.
- [14] C. Inertia, "CYBERSECURITY INERTIA AND SOCIAL ENGINEERING :," vol. 20, no. 3, pp. 139–150, 2019.
- [15] D. Novita and A. Herwanto, "Cyber Security and Network Management A Social Engineering Mitigation Model Based on Digital Se- curity Literacy for Social Media Users in Indonesia," 2026.
- [16] D. Chapagain, "SEAtch : Deception Techniques in Social Engineering Attacks : An Analysis of Emerging Trends and Countermeasures," pp. 1–10.
- [17] M. K. Nazri, M. Irwan, and P. Nasution, "Tinjauan Keamanan Data Terhadap Fenomena Kejahatan Social Engineering Pada Pengguna Platform Pembayaran Digital Di Indonesia," pp. 287–299, 2026.
- [18] O. Bulatova, E. Roland, and S. Sarbash, "Europe in the World Economic System DEVELOPMENT OF THE EUROPEAN SECURITY COMPLEX IN THE CONTEXT OF CURRENT POSITIONS OF THE EU COUNTRIES," vol. 23, no. June, pp. 0–1, 2024.
- [19] N. Ramadani, D. R. Utami, M. K. A. Rosa, D. N. Sari, and Y. Juliana, "PENINGKATAN LITERASI DIGITAL MELALUI EDUKASI KEAMANAN DIGITAL DAN ETIKA BERMEDIA SOSIAL," vol. 7, pp. 21–25, 2026.
- [20] P. K. Sari *et al.*, "Evaluating AI-Based Learning Platform to Increase Cybersecurity Awareness: Case Study of Indonesian Students," vol. 15, no. 9, pp. 1971–1981, 2025.

Peringatan

Redaksi sangat menghargai naskah yang dikirimkan, namun banyak kesalahan fatal dari Author adalah tidak membaca dengan baik panduan di TEMPLATE ini, sehingga naskah yang dikirim tidak sesuai aturan template. Untuk beberapa alasan, naskah yang tidak sesuai template terkadang langsung di REJECT dan/atau minta di perbaiki jika kesalahannya minor. Untuk itu, lebih baik dibaca berulang kali, cek dan ricek sebelum submit naskah. Tujuannya untuk mempercepat proses naskah di SENAPAS dan secara tidak langsung Anda telah ikut membantu pengelola Jurnal.

Atas berkenannya, diucapkan terima kasih.