Evaluasi Kesadaran dan Kebiasaan Keamanan Siber pada Umkm terhadap Ancaman Phishing: Studi Kasus pada Kopi Boutique Cimahi

Andri Sahata Sitanggang*[1], Fhadzrial Dharmawan Saputra[2], Yahdi Nur Alfaiz[3], Audry Satya Pramudika[4], M. Miftah Fauzi[5]
Universitas Komputer Indonesia[1,2,3,4,5]
*e-mail: andri.sahata@email.unikom.ac.id

ABSTRAK
Transformasi digital telah mendorong UMKM memanfaatkan media sosial, e-commerce, dan sistem pembayaran digital untuk meningkatkan daya saing usaha. Namun, ketergantungan terhadap teknologi juga meningkatkan risiko serangan siber, terutama phishing yang memanfaatkan kelemahan pengguna. Penelitian ini bertujuan menganalisis tingkat kesadaran keamanan siber, praktik *cyber hygiene*, faktor penghambat, serta dampak pengalaman menjadi korban phishing pada pelaku UMKM di Kopi Boutique Cimahi. Penelitian menggunakan pendekatan kualitatif dengan metode wawancara semi-terstruktur dan observasi nonpartisipan terhadap pemilik dan karyawan. Data dianalisis secara deskriptif melalui triangulasi hasil wawancara dan observasi dengan mengadaptasi kerangka evaluasi kesadaran keamanan siber. Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan siber masih beragam dan belum diikuti oleh penerapan praktik keamanan digital yang memadai. Sebagian besar informan masih menggunakan metode konvensional dalam pengelolaan kata sandi, belum menerapkan autentikasi dua faktor secara konsisten, serta kesulitan mengenali karakteristik serangan phishing. Hambatan utama meliputi rendahnya literasi digital, minimnya pelatihan, dan belum adanya kebijakan keamanan yang terstruktur sebelum insiden terjadi. Pengalaman menjadi korban phishing meningkatkan kewaspadaan serta mendorong perubahan perilaku dan kebijakan internal, meskipun bersifat reaktif. Penelitian ini menyimpulkan bahwa peningkatan ketahanan siber UMKM memerlukan edukasi berkelanjutan, penguatan kebijakan keamanan, serta penerapan praktik *cyber hygiene* yang konsisten. Temuan ini menjadi dasar bagi penyusunan strategi edukasi keamanan siber yang lebih efektif bagi pelaku UMKM.

Kata kunci : *Kesadaran; Kebiasaan; Keamanan Siber; Ancaman Phishing.*

ABSTRACT
Digital transformation has encouraged micro, small, and medium enterprises (MSMEs) to adopt social media, e-commerce platforms, and digital payment systems to improve business competitiveness. However, this increasing dependence on digital technology has also heightened exposure to cyber threats, particularly phishing attacks that exploit human vulnerabilities. This study aims to analyze cybersecurity awareness, cyber hygiene practices, barriers to cybersecurity implementation, and the impact of phishing experiences among MSME actors at Kopi Boutique Cimahi. A qualitative approach was employed using semi-structured interviews and non-participant observation involving business owners and employees. Data were analyzed descriptively through triangulation of interview and observational findings by adopting the cybersecurity awareness evaluation framework developed. The findings reveal that cybersecurity awareness varies among participants and has not been accompanied by adequate digital security practices. Most informants still relied on conventional password management, had not consistently implemented two-factor authentication, and experienced difficulties in identifying phishing attempts. The main barriers included limited digital literacy, inadequate cybersecurity training, and the absence of structured security policies before cyber incidents occurred. Experiencing phishing attacks increased participants' vigilance and encouraged behavioral and organizational policy changes, although these responses remained largely reactive. The study concludes that strengthening MSME cybersecurity resilience requires continuous cybersecurity education, stronger internal security policies, and consistent implementation of cyber hygiene practices. These findings provide practical implications for developing more effective cybersecurity awareness programs for MSMEs.

Keywords **:** *Awareness; Habits; Cybersecurity; Phishing Threats.*

PENDAHULUAN

Teknologi digital yang berkembang pesat dalam satu dekade terakhir mengubah cara masyarakat dalam menjalankan aktivitas ekonomi, tidak terkecuali bagi pelaku UMKM. Kemudahan akses media sosial,e-commerce, dan sistem pembayaran digital membuka peluang pasar menjadi lebih luas dibandingkan sebelumnya. Tetapi dibalik kemudahan tersebut, ditemukan nya ancaman keamanan siber yang semakin marak dan terus berkembang pesat, sementara pelaku UMKM untuk kesiapan dalam menghadapinya masih jauh dari memadai.

Di antara beragam jenis kejahatan siber yang ada, phising salah satu menjadi ancaman yang paling umum ditemui dan paling merugikan bagi pelaku usaha UMKM. Phishing merupakan teknik manipulasi yang dibuat untuk menipu korban agar secara sukarela memberi informasi sensitif seperti kata sandi, kode OTP, atau data rekening, biasanya melalui pesan teks, pesan palsu, atau komunikasi yang disamarkan sebagai platform aplikasi terpercaya. Daeng dkk. (2023), dalam studi mereka terhadap sistem keamanan siber di indonesia, menyatakan bahwa tingkat keberhasilan serangan phishing sangatlah tinggi karena memanfaatkan kelalaian pengguna, bukan karena kelemahan sistem. Fenomena ini menjadikan faktor manusia sebagai titik paling rentan dalam keamanan digital, khususnya pada lingkungan UMKM yang dimana mayoritas penggunanya tidak berlatar belakang keahlian teknologi informasi.

Kesenjangan antara kebijakan keamanan siber dan praktik sehari-hari pengguna menjadi isu pokok yang diangkat oleh Ojala, Sipola, dan Saharinen (2026) dalam penelitian mereka terhadap staf lembaga pendidikan vokasi di Finlandia. Mereka mengungkapkan bahwa staf berlatar belakang non-teknis menampilkan pola kebiasaan digital yang menyimpang jauh dari standar keamanan yang sudah direkomendasikan, bukan karena menolak aturan, melainkan karena ketiadaan pelatihan yang relevan, terstruktur, dan disesuaikan secara individual. Penelitian tersebut secara khusus mengevaluasi tingkat kesadaran dan kebiasaan keamanan siber sebagai dua dimensi yang saling berkaitan tetapi sering kali tidak selaras. Temuan ini memiliki sangat relevan untuk diadaptasi ke dalam konteks UMKM di indonesia. Dimana kondisi serupa bahkan cenderung lebih parah sangat mungkin terjadi mengingat keterbatasan sumber daya serta minimnya ekosistem pendukung literasi digital pada tingkat usaha kecil.

Perkembangan ekosistem digital yang semakin menimbulkan konsekuensi dual bagi pelaku UMKM, di satu sisi membuka peluang bisnis yang lebih ekspansif, di sisi lain menjadikan mereka sebagai sasaran baru kejahatan siber. Susanto dkk. (2023), dalam kajian mereka terhadap manajemen keamanan siber di era digital, menegaskan bahwa serangan siber seperti ransomware, phishing, dan hacking tidak lagi mengincar perusahaan besar, melainkan telah merambah ke entitas usaha kecil yang sering kali kekurangan terhadap kesiapan teknis yang memadai. Temuan ini diperkuat oleh Budiyanto dan Mabruri (2025), yang mencatat bahwa ancaman siber di indonesia menimbulkan dampak yang berlapis, mulai dari kerugian finansial individu hingga ketidakstabilan organisasi, serta menyoroti tantangan utama bukan pada ketiadaan teknologi pengaman, melainkan pada tingkat kesadaran pengguna yang rendah dalam mengenali dan merespon ancaman yang terus berevolusi dengan cepat.

Dalam konteks kejahatan siber yang menargetkan pada pengguna awam, phishing menduduki posisi paling dominan. Daeng dkk. (2023). Mencatat bahwa tingkat keberhasilan serangan phishing di indonesia sangat tinggi karena memanfaatkan kelalaian manusia sebagai titik lemah utama dalam rantai keamanan digital, bukan karena kelemahan sistem nya. Dewanto dkk. (2024), memperdalam temuan nya melalui analisis mekanisme penipuan berbasis media sosial, dna menyimpulkan bahwa banyak korban tidak menyadari sedang dimanipulasi hingga kerugian telah terjadi. Mereka menekankan bahwa keamanan siber tidak hanya bergantung pada sistem, melainkan sangat ditentukan oleh tingkat kewaspadaan pengguna. Kondisi ini menjadi tantangan khusus bagi UMKM, dimana seluruh karyawan nya merupakan pengguna aktif platform digital namun hampir tidak pernah mendapatkan pembekalan tentang keamanan siber yang dibuat secara terstruktur.

Kopi Boutique Cimahi merupakan UMKM di sektor kuliner yang berlokasi di Jalan Gatot Subroto No. 14, Cimahi Tengah, serta telah mengintegrasikan berbagai platform digital dalam operasional hariannya, mencakup pemesanan daring melalui Go-Food dan Grab-Food, pengelolaan pemasaran via instagram, serta

transaksi non tunai berbasis QRIS dan mobile banking. Ketergantungan yang tinggi terhadap ekosistem digital ini, menjadikan Kopi Boutique sebagai objek studi yang relevan dan kaya data untuk mengkaji persoalan kesadaran serta kebiasaan keamanan siber di kalangan UMKM.

Penelitian Ojala, Sipola, dan Saharinen (2026) menjadi landasan teoritis primer dalam kajian ini. Dengan menerapkan pendekatan kualitatif dengan wawancara mendalam terhadap staf lembaga pendidikan vokasi di Finlandia, mereka mengidentifikasi kesenjangan yang signifikan antara kebijakan keamanan siber yang telah ditetapkan secara institusional dengan praktik keseharian penggunanya. Staf dengan latar belakang non-teknis memperlihatkan kebiasaan pola kebiasaan digital yang menyimpang jauh dari standar keamanan yang sudah direkomendasikan, bukan karena akibat pengabaian regulasi, melainkan karena ketiadaan pelatihan yang relevan dan personal. Kajian tersebut secara umum mengevaluasi kesadaran sebagai pemahaman yang diimplementasikan sehari-hari. Kerangka evaluatif inilah yang yang diadaptasi dalam penelitian ini untuk menganalisis kondisi yang ada di Kopi Boutique Cimahi.

Wijaya dan Juardi (2026) memperkenalkan dimensi solusi dengan menemukan bahwa edukasi keamanan siber berbasis komunitas dan menggunakan media sederhana terbukti lebih efektif diserap oleh masyarakat yang awam dibandingkan dengan program formal yang bersifat *top-down.* Temuan ini memiliki relevansi tinggi karena menunjukan bahwa isu kesadaran keamanan siber di kalangan UMKM tidak dapat diselesaikan melalui pendekatan teknis semata, melainkan membutuhkan pemahaman mendalam terhadap konteks sosial dan kebiasaan pengguna yang ada.

Dari perspektif regulasi, Suari dan Sarjana (2023) mencatat bahwa perlindungan data pribadi di indonesia masih tersebar di berbagai instrumen hukum dan belum terintegrasi secara optimal dalam satu kerangka komprehensif, sehingga masyarakat awam termasuk UMKM kesulitan dalam memahami hak serta kewajiban mereka ketika dihadapi dengan kebocoran data. Kondisi ini juga dipertegas oleh Asherli dan Wiraguna (2025), yang menganalisis perlindungan data dalam konteks serangan phishing berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Mereka mengungkapkan bahwa pelaku UMKM secara umum tidak mengetahui mekanisme pelaporan yang ada serta tidak memahami terhadap prosedur pemulihan pasca terjadinya insiden.

Secara keseluruhan, tinjauan literatur ini menunjukan bahwa isu keamanan siber di kalangan UMKM bersifat multidimensi, meliputi aspek teknis dan perilaku pengguna. Secara spesifik mengevaluasi kesadaran dan kebiasaan keamanan siber pada UMKM korban phishing di indonesia masih sangat terbatas. Penelitian ini hadir untuk mengisi celah tersebut melalui studi kasus mendalam pada Kopi Boutique Cimahi.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode wawancara semi-terstruktur (*semi structured*). Pendekatan ini dipilih karena penelitian bertujuan untuk menganalisis,Mengevaluasi tingkat kesadaran keamanan siber di kalangan pelaku UMKM non-IT, dengan fokus pada pemahaman mereka terhadap ancaman phishing dan risiko digital dalam konteks operasional usaha. Dengan metode kualitatif memungkinkan mencari informasi lebih dalam mengenai bagaimana pemahaman tentang keamanan siber pada pelaku UMKM di sekitar. Penelitian ini dilaksanakan di Kopi Boutique Cimahi, Jalan Gatot Subroto No.14, Karang Mekar, Kec. Cimahi Tengah, Kota Cimahi, Jawa Barat.

Wawancara secara mendalam ini dilakukan oleh penulis.Wawancara ini bersifat semi-terstruktur, memungkinkan fleksibilitas dalam menggali informasi dari narasumber tentang pemahaman, tantangan, solusi dan kebijakan terkait keamanan siber. Teknik ini merujuk pada kerangka metodologi Ojala dkk. (2026) yang membuktikan efektivitas dalam menggali pengalaman informan non-teknis yang berkaitan dengan keamanan siber. Beberapa topik yang diangkat meliputi: Pengalaman mereka tentang serangan siber, Kesiapan pelaku UMKM dalam menghadapi ancaman siber, dan Upaya edukasi pelaku UMKM yang sudah dilakukan.

Observasi dilakukan secara non-partisipan untuk mengamati praktik keamanan digital pelaku usaha dan karyawan secara langsung dalam aktivitas operasional sehari-hari. Teknik ini dipilih untuk melengkapi data wawancara yang bersifat self-report, karena pemahaman yang dinyatakan informan tidak selalu selaras dengan perilaku yang dipraktikkan. Sebagaimana ditekankan Ojala et al. (2026), kesenjangan antara kesadaran dan kebiasaan keamanan siber justru sering muncul pada tataran praktik, sehingga pengamatan

langsung diperlukan untuk menangkap kebiasaan nyata yang tidak terungkap melalui wawancara. Aspek yang diamati meliputi: Cara merespons pesan atau tautan masuk (langsung membuka atau memverifikasi terlebih dahulu). Pengelolaan dan pembagian akses akun digital usaha (Instagram, GoFood, GrabFood). Praktik pengelolaan kata sandi dan penggunaan perangkat pribadi maupun perangkat usaha. Alur transaksi nontunai berbasis QRIS dan mobile banking. Hasil pengamatan dicatat dalam bentuk catatan lapangan (*field notes*) yang kemudian digunakan sebagai sumber triangulasi terhadap data wawancara.

HASIL DAN PEMBAHASAN

Hasil Penelitian

Tingkat Kesadaran Keamanan Siber terhadap Ancaman *Phishing*

Hasil wawancara mengenai pemahaman informan terhadap istilah dan konsep *phishing* sebelum insiden terjadi menunjukkan tingkat kesadaran yang bervariasi. Salma mengaku pernah mendengar istilah tersebut, tetapi tidak memahami maknanya secara utuh, sehingga kesadarannya dapat dikategorikan bersifat permukaan, yakni sekadar mengenal istilah tanpa memahami substansi maupun risikonya. Kondisi serupa juga dialami oleh Muhammad Fahri, yang bahkan mengaku sama sekali belum pernah mendengar istilah *phishing* sebelum insiden yang menimpanya.

Sebaliknya, April telah memperoleh informasi mengenai *phishing* dari media sosial dan telah melakukan diskusi internal bersama rekan kerja terkait pentingnya kehati-hatian dalam menanggapi pesan dari sumber tidak dikenal, sehingga tingkat kesadarannya relatif lebih baik dibandingkan informan lain meskipun ia belum pernah mengalami insiden secara langsung. Tingkat pemahaman paling komprehensif ditunjukkan oleh Pak Heru, yang selain memperoleh informasi dari sumber daring dan lingkungan pertemanan, juga pernah mengikuti kegiatan pelatihan keamanan digital sebelum insiden terjadi.

Menariknya, informan admin media sosial sejak awal telah memahami definisi umum *phishing* sebagai upaya pengambilan data pribadi maupun data perusahaan, dan memperoleh pemahaman tersebut dari lingkaran pertemanan. Namun demikian, pemahaman konseptual tersebut ternyata tidak berbanding lurus dengan kewaspadaan pada tataran praktik, karena informan tetap memberikan kode OTP tatkala dihubungi pihak yang mengaku berasal dari bank dengan iming-iming nominal transaksi yang lebih besar. Sementara itu, Fajar Haris memperoleh pemahaman mengenai *phishing* bukan dari sumber formal, melainkan dari penjelasan anaknya, yang mengindikasikan bahwa kesadaran keamanan siber pada sebagian informan terbentuk melalui transfer pengetahuan informal antargenerasi, bukan melalui edukasi institusional.

Pada aspek respons terhadap pesan, tautan, atau berkas dari sumber yang tidak dikenal, ditemukan pola kehati-hatian yang berbeda antarinforman. Pak Heru menerapkan kebijakan mengabaikan pesan-pesan yang dianggap mencurigakan, kecuali yang berasal dari akun resmi terverifikasi. April membiasakan diri memastikan identitas pengirim sebelum menanggapi pesan yang tidak dikenal. Fajar Haris lebih memilih berkonsultasi dengan anaknya sebelum mengambil keputusan atas pesan yang dianggap janggal. Adapun Salma mengaku langsung membuka berkas berformat aplikasi yang dikirimkan oleh nomor tidak dikenal tanpa melakukan verifikasi terlebih dahulu, sebuah tindakan yang pada akhirnya menyebabkan perangkatnya mengalami gangguan fungsi disertai permintaan sejumlah uang.

Kebiasaan Pengelolaan Keamanan Digital (*Cyber Hygiene*)

Terkait pengelolaan kata sandi, mayoritas informan (April, informan admin media sosial, Muhammad Fahri, dan Salma) menyatakan menyimpan kata sandi akun usaha pada berkas lembar kerja elektronik (spreadsheet) atau catatan manual, bukan pada aplikasi pengelola kata sandi yang bersifat terenkripsi. Kondisi yang relatif berbeda ditunjukkan oleh Pak Heru selaku HRD, yang menyebutkan bahwa penyimpanan kata sandi dilakukan melalui basis data internal perusahaan, meskipun caranya masih bersifat konvensional dan sengaja menghindari layanan penyimpanan kata sandi berbasis akun Google karena pertimbangan risiko akses otomatis. Dari sisi rutinitas pembaruan, hanya informan admin media sosial yang menyebutkan kebiasaan mengganti kata sandi secara berkala setiap satu bulan sekali, sementara informan lain tidak menyebutkan adanya rutinitas pembaruan kata sandi.

Pada aspek pembagian akses akun usaha, ditemukan kecenderungan pemberian akses yang bersifat selektif dan terbatas. April dan Salma menjelaskan bahwa akses akun usaha hanya diberikan kepada karyawan yang masih aktif bekerja dan akan dicabut apabila karyawan tersebut berhenti atau ketika jam operasional telah usai, sebagai upaya mencegah penyalahgunaan akun untuk kepentingan pribadi. Informan admin media sosial menerapkan mekanisme yang lebih berjenjang, yakni meminta persetujuan atasan terlebih dahulu sebelum membagikan akses kepada pihak lain, dan memasukkan kredensial akun secara langsung tanpa memperlihatkan kata sandi kepada peminjam. Pendekatan yang lebih ketat diterapkan oleh Pak Heru, yang lebih memilih meminjamkan perangkat fisik berisi akun terkait dibandingkan membagikan kredensial secara langsung, disertai dengan konfirmasi keperluan penggunaan akun tersebut.

Untuk transaksi non-tunai, seluruh informan yang bertugas di area operasional dan kasir menyatakan penggunaan QRIS dan aplikasi mobile banking secara rutin dalam aktivitas hariannya, namun tidak satu pun informan yang secara eksplisit menyebutkan adanya kebiasaan verifikasi keamanan tambahan, seperti autentikasi dua faktor, sebelum terjadinya insiden *phishing* yang mereka alami.

Faktor Penghambat Kesadaran dan Kebiasaan Keamanan Siber

Berdasarkan penuturan informan, teridentifikasi beberapa faktor yang menghambat terbentuknya kesadaran dan kebiasaan keamanan siber yang memadai di lingkungan Kopi Boutique Cimahi. Pertama, minimnya literasi dasar mengenai definisi dan cara kerja *phishing*, sebagaimana disampaikan oleh Salma, Muhammad Fahri, dan Fajar Haris, yang mengakui belum memahami istilah tersebut sebelum mengalami maupun mendekati insiden. Kedua, rendahnya minat untuk mengikuti kegiatan pelatihan keamanan digital secara formal, sebagaimana diungkapkan Salma yang menyebutkan bahwa banyak karyawan enggan mengikuti pelatihan meskipun kesempatan tersedia.

Ketiga, adanya preferensi terhadap format pelatihan yang dipandu langsung oleh praktisi profesional di bidang teknologi informasi dibandingkan materi tertulis atau daring, sebagaimana disampaikan oleh Salma dan diperkuat oleh pernyataan Muhammad Fahri yang menilai pelatihan semacam itu akan lebih mudah dipahami. Keempat, kesulitan dalam membedakan pesan yang bersifat *phishing* dari pesan yang asli menjadi hambatan yang disampaikan oleh Pak Heru dan Muhammad Fahri, yang menyatakan bahwa tantangan utama justru terletak pada identifikasi awal terhadap indikasi kecurangan, bukan pada ketiadaan kemauan untuk bersikap waspada.

Kelima, ketiadaan kebijakan formal mengenai pengelolaan keamanan digital sebelum insiden terjadi turut teridentifikasi sebagai faktor penghambat struktural, tercermin dari adanya perubahan aturan internal yang baru diterapkan Kopi Boutique setelah insiden dialami, sebagaimana disampaikan oleh Salma dan April, khususnya terkait pembatasan pihak yang berwenang mengelola akses email dan akun usaha.

Pengalaman sebagai Korban Phishing dan Dampaknya terhadap Kewaspadaan

Pengalaman paling signifikan dituturkan oleh Salma, yang menceritakan bahwa insiden *phishing* berbasis berkas aplikasi (APK) dialaminya pada saat kondisi operasional kafe sedang padat oleh pesanan pelanggan, baik secara langsung maupun melalui platform GrabFood dan ShopeeFood. Kondisi tersebut menyebabkan berkurangnya kewaspadaan informan sehingga berkas yang dikirimkan oleh nomor tidak dikenal dibuka tanpa verifikasi, yang berujung pada terkuncinya perangkat disertai pesan permintaan sejumlah uang. Pada kesempatan lain, informan yang sama juga menuturkan pengalaman memberikan kode OTP kepada pihak yang mengatasnamakan mitra GrabFood dengan dalih verifikasi guna memproses pesanan dalam jumlah besar, yang pada akhirnya menyebabkan hilangnya dana usaha pada rekening bank terkait.

Pengalaman serupa dituturkan oleh Pak Heru, yang menerima pesan elektronik mengatasnamakan pihak bank dengan tawaran sejumlah dana, dengan syarat memberikan kode OTP yang diterima. Karena ketidaktahuan akan modus tersebut, informan memberikan kode dimaksud tanpa kecurigaan, dan pada keesokan harinya mendapati saldo rekening telah terkuras habis.

Muhammad Fahri mengalami insiden serupa, yang diawali dengan adanya percobaan masuk (*login*) pada akun usaha, kemudian diikuti oleh pesan elektronik yang meminta nama pengguna dan kata sandi bank dengan dalih keperluan verifikasi *login*. Adapun informan admin media sosial mengalami insiden ketika

menerima pesan melalui Instagram yang mengatasnamakan pihak bank dan meminta kode OTP dengan iming-iming dapat memproses transaksi dalam nominal yang lebih besar, sehingga informan yang tergiur oleh tawaran tersebut memberikan kode OTP.

Berbeda dengan informan lain, Fajar Haris berhasil terhindar dari potensi kerugian berkat peran anggota keluarganya. Ketika menerima pesan dari nomor tidak dikenal yang meminta data rekening dengan dalih memastikan tidak adanya dana yang salah kirim, informan terlebih dahulu mengonsultasikan hal tersebut kepada anaknya, yang kemudian mengidentifikasi pesan tersebut sebagai upaya penipuan sehingga tindak lanjut berupa pemblokiran rekening dan pembaruan kata sandi segera dilakukan.

Pascainsiden, seluruh informan yang pernah menjadi korban melaporkan adanya perubahan perilaku maupun kebijakan sebagai bentuk mitigasi risiko serupa di masa mendatang. Kopi Boutique secara institusional telah melaporkan insiden yang menimpa Salma kepada pihak bank dan penyedia platform terkait, namun proses tersebut tidak dapat dilanjutkan karena keterbatasan bukti pendukung. Selain itu, ditetapkan pula kebijakan baru mengenai pembatasan pihak yang berwenang mengakses email dan akun usaha. Pada tataran individu, Pak Heru menyatakan telah menerapkan sistem autentikasi dua faktor (kunci ganda) pada seluruh akun pribadinya, Muhammad Fahri membiasakan diri mengganti kata sandi secara lebih sering, sementara keluarga Fajar Haris memperbarui nomor WhatsApp dan kata sandi rekening bank sebagai langkah antisipatif meskipun tidak mengalami kerugian secara langsung.

Pembahasan

Kesenjangan antara Kesadaran Kognitif dan Praktik Keamanan

Temuan pada penelitian ini memperkuat kerangka evaluatif yang dikemukakan oleh Ojala, Noponen, dan Savolainen (2026), yang menegaskan bahwa kesadaran dan kebiasaan keamanan siber merupakan dua dimensi berbeda yang sering kali tidak selaras satu sama lain. Kasus informan admin media sosial menjadi ilustrasi paling jelas dari kesenjangan tersebut, sebab informan telah memiliki pemahaman konseptual yang relatif memadai mengenai definisi *phishing*, namun tetap bersedia memberikan kode OTP ketika dihadapkan pada situasi yang menawarkan keuntungan transaksional. Kondisi ini menunjukkan bahwa pengetahuan kognitif semata tidak serta-merta mampu mencegah perilaku berisiko apabila tidak disertai dengan kebiasaan verifikasi yang konsisten dan internalisasi kewaspadaan pada tataran praktik operasional sehari-hari.

Faktor Manusia sebagai Titik Lemah Utama dalam Rantai Keamanan Siber

Hasil penelitian ini turut relevan dengan temuan Daeng dkk. (2023), yang menyimpulkan bahwa tingginya tingkat keberhasilan serangan *phishing* di Indonesia lebih banyak disebabkan oleh kelalaian pengguna dibandingkan kelemahan sistem teknis. Pola yang terungkap pada insiden yang dialami Salma dan Pak Heru memperlihatkan bagaimana pelaku *phishing* memanfaatkan momen kelengahan situasional, seperti kepadatan pesanan pelanggan maupun ketidaktahuan atas skema penipuan, sebagai celah rekayasa sosial (*social engineering*) untuk memperoleh kode OTP maupun data rekening. Pola serupa juga sejalan dengan temuan Dewanto dkk. (2024) yang menekankan bahwa banyak korban penipuan berbasis media sosial baru menyadari telah dimanipulasi setelah kerugian benar-benar terjadi, sebagaimana tercermin dari pengakuan Pak Heru yang baru mengetahui saldo rekeningnya terkuras pada keesokan harinya.

Selanjutnya, hambatan-hambatan yang teridentifikasi turut mengonfirmasi pandangan Susanto et al. (2023) serta Budiyanto dan Mabruri (2025) yang menegaskan bahwa tantangan utama keamanan siber pada entitas usaha kecil bukan terletak pada ketiadaan teknologi, melainkan pada rendahnya tingkat kesadaran pengguna dalam mengenali ancaman yang terus berevolusi. Rendahnya minat mengikuti pelatihan serta minimnya literasi dasar mengenai *phishing* yang ditemukan pada mayoritas informan menunjukkan bahwa aspek manusia tetap menjadi variabel paling menentukan dalam efektivitas pertahanan siber di lingkungan UMKM seperti Kopi Boutique Cimahi.

Peran Konteks Sosial dan Kebutuhan Pendekatan Edukasi Kontekstual

Preferensi informan terhadap format pelatihan yang dipandu langsung oleh praktisi profesional, sebagaimana disampaikan Salma, serta pola transfer pengetahuan informal antargenerasi yang dialami Fajar

Haris melalui bimbingan anaknya, memperkuat argumentasi Wijaya dan Juardi (2026) bahwa edukasi keamanan siber berbasis komunitas dengan media yang sederhana cenderung lebih efektif diserap oleh kelompok masyarakat awam dibandingkan program formal yang bersifat teknis.

Temuan ini mengindikasikan bahwa strategi peningkatan literasi keamanan siber pada UMKM sebaiknya tidak semata mengandalkan pendekatan teknis atau kebijakan formal, melainkan turut mempertimbangkan konteks sosial serta pola komunikasi yang telah lazim digunakan pada lingkungan usaha tersebut.

Implikasi terhadap Perlindungan Data Pribadi dan Pemulihan Pascainsiden

Pengalaman Kopi Boutique yang melaporkan insiden *phishing* kepada pihak bank dan penyedia platform, namun tidak dapat ditindaklanjuti karena keterbatasan bukti, mengafirmasi kajian Suari dan Sarjana (2023) mengenai fragmentasi kerangka hukum perlindungan data pribadi di Indonesia yang menyulitkan masyarakat awam, termasuk pelaku UMKM, dalam memahami hak dan mekanisme pemulihan yang tersedia.

Temuan ini juga selaras dengan hasil kajian Asherli dan Wiraguna (2025) terhadap Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang menyebutkan bahwa pelaku UMKM pada umumnya tidak mengetahui mekanisme pelaporan yang berlaku maupun prosedur pemulihan pascainsiden *phishing*. Dengan demikian, keberadaan kerangka hukum perlindungan data pribadi belum sepenuhnya dapat diakses secara efektif oleh pelaku usaha berskala kecil, sehingga upaya pemulihan kerugian akibat *phishing* pada praktiknya masih menghadapi kendala yang signifikan.

Sintesis Temuan

Secara keseluruhan, temuan-temuan pada penelitian ini menunjukkan bahwa tingkat kesadaran keamanan siber pada pelaku UMKM Kopi Boutique Cimahi bersifat heterogen dan sebagian besar masih berada pada tahap pengenalan istilah tanpa pemahaman risiko yang mendalam. Kebiasaan pengelolaan keamanan digital yang dipraktikkan, khususnya dalam pengelolaan kata sandi dan pembagian akses akun, masih mengandalkan metode konvensional yang rentan terhadap kebocoran data.

Faktor penghambat yang teridentifikasi bersifat multidimensi, meliputi rendahnya literasi dasar, minimnya minat pada pelatihan formal, serta ketiadaan kebijakan keamanan yang terstruktur sebelum insiden terjadi. Adapun pengalaman menjadi korban *phishing* terbukti menjadi titik balik penting yang mendorong perubahan kewaspadaan serta kebiasaan keamanan siber, baik pada tataran individu maupun institusional, sekalipun perubahan tersebut masih bersifat reaktif dan baru diterapkan setelah kerugian telah terjadi.

SIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa tingkat kesadaran keamanan siber pada pelaku UMKM di Kopi Boutique Cimahi masih bervariasi dan secara umum belum diimbangi dengan penerapan praktik keamanan digital yang memadai. Sebagian besar informan hanya mengenal istilah phishing secara umum tanpa memahami mekanisme, karakteristik, maupun langkah pencegahannya secara komprehensif, sehingga tetap rentan menjadi korban rekayasa sosial. Temuan penelitian menunjukkan adanya kesenjangan antara pengetahuan kognitif dan perilaku nyata dalam menjaga keamanan digital, yang tercermin dari kebiasaan menyimpan kata sandi secara konvensional, belum diterapkannya autentikasi dua faktor sebelum insiden, serta rendahnya kebiasaan melakukan verifikasi terhadap pesan atau tautan mencurigakan. Faktor utama yang menghambat terbentuknya budaya keamanan siber meliputi rendahnya literasi digital, minimnya pelatihan yang terstruktur, ketiadaan kebijakan keamanan internal sebelum insiden, serta kesulitan membedakan komunikasi asli dengan modus phishing. Pengalaman menjadi korban phishing terbukti meningkatkan kewaspadaan individu maupun organisasi melalui perubahan kebijakan dan perilaku, namun perubahan tersebut bersifat reaktif setelah kerugian terjadi. Oleh karena itu, peningkatan keamanan siber pada UMKM tidak cukup hanya mengandalkan teknologi, tetapi memerlukan penguatan literasi keamanan digital, pelatihan yang kontekstual dan berkelanjutan, penyusunan kebijakan keamanan yang jelas, serta

penerapan praktik cyber hygiene secara konsisten agar ketahanan UMKM terhadap ancaman siber, khususnya phishing, dapat ditingkatkan secara berkelanjutan.

DAFTAR PUSTAKA

Ajmera, P. (2025). Cybersecurity in the Internet of Things: Trends and challenges in a nascent field. *Computer Law & Security Review, 59*, 106204.

Asherli, B. F., & Wiraguna, S. A. (2025). Perlindungan keamanan data pribadi di era digital menghadapi serangan phishing ditinjau dari Undang-Undang Perlindungan Data Pribadi Nomor 27 Tahun 2022. *Jurnal Hukum, Administrasi Publik dan Negara, 2*(4), 1–14.

Budiyanto, D., & Mabruri, M. (2025, February). Pentingnya keamanan siber dalam era digital: Tinjauan global dan kondisi di Indonesia. In *Prosiding Seminar Nasional Sains dan Teknologi "SainTek"* (Vol. 2, No. 1, pp. 981–994).

Daeng, Y., Levin, J., Karolina, K., Prayudha, M. R., Ramadhani, N. P., Noverto, N., ... & Virgio, V. (2023). Analisis penerapan sistem keamanan siber terhadap kejahatan siber di Indonesia. *Innovative: Journal of Social Science Research, 3*(6), 1135–1145.

Gustryan, M., & Hoesein, Z. A. (2025). Peran Undang-Undang ITE dan Undang-Undang Perlindungan Data Pribadi dalam perlindungan data dan privasi di era ekonomi digital. *Jurnal Minfo Polgan, 14*(2), 3333–3343.

Lubis, M., Luthfi, M. I., Saedudin, R. R., Muttaqin, A. N., & Lubis, A. R. (2026). The integration of ISO 27005 and NIST SP 800-30 for Security Operation Center (SOC) framework effectiveness in the non-bank financial industry. *Computers, 15*(1), 60.

Lutfi, M. P., Kurniasari, E., & Putri, F. E. A. (2024). Urgensi perlindungan hukum terhadap data privasi nasabah bank di era perkembangan digital. *Jurnal Multidisiplin Ilmu Akademik, 1*(5), 210–218.

Moorthy, R. S., & Pabitha, P. (2020). Optimal detection of phishing attack using SCA based K-NN. *Procedia Computer Science, 171*, 1716–1725.

Nagalay, F. S. S., Sriyanto, S., & Zarnelly, Z. (2024). Analisis penerapan algoritma decision tree dalam keamanan siber untuk klasifikasi situs website phishing. *Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, 10*(1), 1–8.

Ojala, A. L., Sipola, T., & Saharinen, K. (2026). Cybersecurity awareness and hygiene development in Finnish vocational education: Staff perceptions, training gaps and diverse learning pathways. *Information & Computer Security, 34*(1), 66–85.

Rif'at, E. M., & Dompak, T. (2025). Hak asasi manusia di era digital: Tantangan dan peluang dalam mengatasi kejahatan siber. *Jurnal Ilmu Multidisiplin, 3*(1), 86–98.

Rohmah, R. N. (2022). Upaya membangun kesadaran keamanan siber pada konsumen e-commerce di Indonesia. *Cendekia Niaga, 6*(1), 1–11.

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia. *Jurnal Analisis Hukum, 6*(1), 132–142.

Vladov, S., Vysotska, V., Ścisło, Ł., Dymczyk, R., Posashkov, O., Nazarkevych, M., ... & Pylypenko, Y. (2026). Neural network method for detecting low-intensity DDoS attacks with stochastic fragmentation and its adaptation to law enforcement activities in the cyber protection of critical infrastructure facilities. *Computers, 15*(2), 84.

Widianingrum, A. R. (2024). Analisis implementasi kebijakan hukum terhadap penanganan kejahatan siber di era digital. *Journal Iuris Scientia, 2*(2), 90–102.