QOLAMUNA
https://jurnal.qolamuna.id/index.php/JQ
e-ISSN : 3063-8925
Vol. 3 No. 1 Mei - Oktober 2026

KEAMANAN DIGITAL DI ERA TRANSFORMASI TEKNOLOGI: PERAN LITERASI DAN PERILAKU DALAM PERLINDUNGAN DIRI

Sowam Fatkhul Mufid[1], Akbar Uray Alkadry[2]
[1] Prodi Pendidikan Agama Islam, Universitas Singaperbangsa Karawang, Indonesia
[1]sowamfatkhulmufid@gmail.com [2]akbar.uray@gmail.com

INFO ARTIKEL
Riwayat Artikel:
Diterima: 17-05-26
Disetujui: 30-05-26

Kata Kunci:
keamanan digital, kesadaran siber, literasi digital, phishing, perilaku pengguna

Abstract: *This study aims to analyze individual awareness of digital security, identify dominant cyber threats, and formulate effective self-protection strategies in the digital era. The research employs a descriptive qualitative approach supported by simple quantitative data collected through online surveys and limited interviews conducted from January to March 2026. The findings indicate that despite high internet usage, users' awareness of digital security remains relatively low, primarily due to limited digital literacy and inadequate formal education on cybersecurity. Phishing, online fraud, and account hacking emerge as the most prevalent threats, often exploiting users' psychological vulnerabilities through social engineering techniques. The study also reveals that user behavior, such as weak password management and neglect of security updates, significantly contributes to increased risk. In conclusion, strengthening digital literacy and promoting continuous cybersecurity education are essential to improving user awareness and resilience. The study suggests the need for collaborative efforts among governments, educational institutions, and digital platforms to build a safer and more inclusive digital ecosystem.*

Abstrak: Penelitian ini bertujuan untuk menganalisis tingkat kesadaran keamanan digital pada individu, mengidentifikasi ancaman siber yang dominan, serta merumuskan strategi perlindungan diri yang efektif di era digital. Metode yang digunakan adalah pendekatan kualitatif deskriptif dengan dukungan data kuantitatif sederhana melalui survei online dan wawancara terbatas pada periode Januari–Maret 2026. Hasil penelitian menunjukkan bahwa meskipun penggunaan internet tinggi, tingkat kesadaran keamanan digital pengguna masih rendah, yang disebabkan oleh keterbatasan literasi digital dan kurangnya edukasi formal terkait keamanan siber. Ancaman utama yang dihadapi meliputi phishing, penipuan online, dan peretasan akun yang memanfaatkan kelemahan psikologis pengguna melalui teknik social engineering. Selain itu, perilaku pengguna seperti penggunaan kata sandi lemah dan pengabaian pembaruan sistem turut meningkatkan risiko keamanan. Simpulan penelitian ini menegaskan bahwa peningkatan literasi digital dan edukasi keamanan siber secara berkelanjutan sangat penting dalam membentuk perilaku aman. Oleh karena itu, diperlukan kolaborasi antara pemerintah, institusi pendidikan, dan platform digital untuk menciptakan ekosistem digital yang aman dan berkelanjutan.

PENDAHULUAN

Perkembangan teknologi digital dalam beberapa dekade terakhir telah mengubah secara fundamental cara manusia berinteraksi, bekerja, dan mengakses informasi. Transformasi digital ini tidak hanya memberikan kemudahan dalam berbagai aspek kehidupan, tetapi juga membuka ruang bagi munculnya berbagai ancaman keamanan siber yang semakin kompleks. Fenomena peningkatan kasus kejahatan siber seperti phishing, pencurian data pribadi, penipuan online, dan peretasan akun menjadi indikasi nyata bahwa ruang digital tidak sepenuhnya aman bagi pengguna. Menurut penelitian (Effendy & Oktiani, 2024) intensitas serangan social engineering dan phishing mengalami peningkatan

signifikan seiring dengan tingginya aktivitas masyarakat di dunia digital. Kondisi ini menunjukkan bahwa keamanan digital bukan lagi sekadar isu teknis, melainkan telah menjadi kebutuhan mendasar dalam kehidupan modern yang harus dipahami oleh setiap individu pengguna teknologi.

Di sisi lain, meningkatnya penetrasi internet dan penggunaan perangkat digital tidak selalu diimbangi dengan tingkat literasi keamanan digital yang memadai. Banyak pengguna masih memiliki pemahaman yang terbatas mengenai praktik dasar keamanan, seperti penggunaan kata sandi yang kuat, pengenalan terhadap tautan berbahaya, serta perlindungan data pribadi. Penelitian oleh (Sari & Fitri, 2025) menunjukkan bahwa rendahnya literasi digital berkontribusi terhadap tingginya kerentanan masyarakat terhadap risiko cybercrime, khususnya dalam sektor layanan digital seperti perbankan. Hal ini menegaskan adanya kesenjangan antara adopsi teknologi yang cepat dengan kesiapan pengguna dalam menghadapi ancaman digital, yang pada akhirnya dapat menimbulkan dampak serius baik secara individu maupun sosial.

Sejumlah studi terdahulu telah mengkaji keamanan digital dari berbagai sudut pandang, baik dari aspek teknis maupun perilaku. Pendekatan teknis umumnya berfokus pada pengembangan sistem keamanan seperti enkripsi, firewall, dan autentikasi berlapis, sementara pendekatan sosial lebih menekankan pada pentingnya literasi digital dan kesadaran pengguna. Namun demikian, sebagian besar penelitian masih bersifat parsial dan belum mengintegrasikan kedua aspek tersebut secara komprehensif. Menurut (Istiqomah et al., 2025) literasi digital memiliki pengaruh signifikan terhadap perilaku pencegahan phishing, namun efektivitasnya sangat bergantung pada bagaimana pengguna menerapkan pengetahuan tersebut dalam praktik sehari-hari. Hal ini menunjukkan adanya kebutuhan untuk mengembangkan pendekatan yang lebih holistik dalam memahami keamanan digital sebagai interaksi antara sistem teknologi dan perilaku manusia.

Berdasarkan kondisi tersebut, terdapat celah penelitian yang perlu diisi, khususnya dalam mengkaji keamanan digital secara terpadu dengan mempertimbangkan aspek kesadaran, perilaku, dan strategi perlindungan diri pengguna. Permasalahan utama yang dihadapi adalah masih rendahnya tingkat kesadaran masyarakat terhadap risiko digital serta kurangnya kemampuan dalam menerapkan langkah-langkah perlindungan yang efektif. Banyak pengguna yang masih mengabaikan praktik keamanan dasar, sehingga rentan terhadap berbagai bentuk serangan siber. Oleh karena itu, diperlukan kajian yang tidak hanya mengidentifikasi ancaman yang ada, tetapi juga merumuskan strategi perlindungan diri yang aplikatif dan mudah diterapkan oleh masyarakat luas dalam kehidupan sehari-hari.

Sejalan dengan hal tersebut, tujuan penulisan artikel ini adalah untuk menganalisis tingkat kesadaran keamanan digital pada individu, mengidentifikasi jenis ancaman digital yang paling dominan, serta merumuskan strategi perlindungan diri yang efektif dalam menghadapi risiko di ruang digital. Secara teoretis, artikel ini diharapkan dapat memperkaya kajian mengenai keamanan digital dengan pendekatan yang lebih integratif antara aspek teknis dan perilaku. Secara praktis, hasil penelitian ini diharapkan dapat menjadi acuan bagi masyarakat dalam meningkatkan literasi keamanan digital serta mendorong terbentuknya perilaku yang lebih bijak dan aman dalam menggunakan teknologi digital di era yang semakin kompleks ini.

METODE PENELITIAN

Metode penelitian yang digunakan dalam kajian ini adalah pendekatan kualitatif deskriptif dengan dukungan data kuantitatif sederhana. Pendekatan ini dipilih untuk memberikan gambaran yang komprehensif mengenai tingkat kesadaran keamanan digital serta perilaku pengguna dalam menghadapi ancaman siber. Subjek penelitian terdiri dari pengguna internet aktif dari berbagai latar belakang usia, pendidikan, dan pekerjaan yang memiliki pengalaman dalam menggunakan media digital, khususnya media sosial dan layanan online. Teknik pengumpulan data dilakukan melalui observasi terhadap perilaku digital dan pengguna umum internet. Selain itu, penelitian ini juga diperkuat dengan studi literatur dari berbagai jurnal ilmiah yang relevan untuk mendukung analisis dan interpretasi data. Teknik analisis data menggunakan analisis deskriptif kualitatif melalui tahapan reduksi data, penyajian data, dan penarikan kesimpulan, serta didukung oleh analisis kuantitatif sederhana berupa persentase guna memperkuat temuan terkait tingkat kesadaran, bentuk ancaman, dan perilaku pengguna dalam mengelola keamanan digital.

HASIL PENELITIAN DAN PEMBAHASAN

Kesadaran Keamanan Digital Pengguna

Tingkat kesadaran pengguna terhadap risiko keamanan digital masih rendah meskipun intensitas penggunaan internet tinggi

Tingkat kesadaran pengguna terhadap risiko keamanan digital menunjukkan kondisi yang relatif rendah, meskipun penggunaan internet terus meningkat secara signifikan di berbagai kalangan. Fenomena ini mengindikasikan adanya ketidakseimbangan antara intensitas pemanfaatan teknologi dengan pemahaman terhadap risiko yang menyertainya. Misalnya, menurut penelitian (Orunsolu et al., 2018), banyak pengguna internet yang memiliki tingkat literasi keamanan rendah sehingga tidak mampu mengenali ancaman seperti phishing dan serangan berbasis rekayasa sosial. Hal ini menyebabkan pengguna tetap rentan terhadap berbagai bentuk kejahatan siber meskipun telah terbiasa menggunakan teknologi dalam kehidupan sehari-hari. Dengan kata lain, penggunaan teknologi yang tinggi tidak secara otomatis meningkatkan kesadaran keamanan digital.

Selain itu, rendahnya kesadaran ini juga dipengaruhi oleh kurangnya pengalaman langsung pengguna terhadap konsekuensi serangan siber, sehingga risiko yang ada sering kali dianggap tidak relevan atau tidak mendesak. Menurut penelitian (Graham & Triplett, 2017), individu dengan tingkat literasi digital yang rendah cenderung memiliki persepsi risiko yang minim terhadap ancaman phishing, sehingga lebih mudah menjadi korban kejahatan siber. Kondisi ini menunjukkan bahwa kesadaran keamanan digital tidak hanya bergantung pada akses teknologi, tetapi juga pada kemampuan kognitif pengguna dalam memahami dan mengantisipasi ancaman. Oleh karena itu, diperlukan upaya sistematis untuk meningkatkan kesadaran pengguna agar sejalan dengan perkembangan teknologi yang semakin kompleks.

Kurangnya edukasi formal dan literasi digital menjadi faktor utama rendahnya pemahaman keamanan

Kurangnya edukasi formal terkait keamanan digital menjadi salah satu faktor utama yang menyebabkan rendahnya pemahaman masyarakat terhadap risiko siber. Dalam banyak kasus, materi mengenai keamanan digital belum terintegrasi secara optimal dalam sistem pendidikan formal maupun program pelatihan masyarakat. Misalnya, menurut penelitian (Istiqomah et al., 2025), literasi digital memiliki peran penting dalam membentuk perilaku pencegahan terhadap phishing, namun masih banyak individu yang belum mendapatkan edukasi yang memadai dalam hal tersebut. Hal ini menyebabkan kesenjangan pengetahuan yang signifikan, terutama di kalangan pengguna yang tidak memiliki latar belakang teknologi informasi.

Lebih lanjut, rendahnya literasi digital juga berdampak pada kemampuan pengguna dalam menginterpretasikan informasi dan mengidentifikasi ancaman digital secara kritis. Tanpa pemahaman yang memadai, pengguna cenderung tidak mampu membedakan antara informasi yang aman dan berbahaya, sehingga meningkatkan risiko terjadinya pelanggaran keamanan. Menurut penelitian (Graham & Triplett, 2017), literasi digital berperan sebagai "perlindungan awal" (capable guardianship) dalam menghadapi ancaman siber, di mana individu yang memiliki literasi tinggi cenderung lebih mampu menghindari serangan phishing. Dengan demikian, peningkatan edukasi formal dan literasi digital menjadi langkah strategis dalam memperkuat keamanan digital masyarakat secara keseluruhan.

Pengguna cenderung mengabaikan praktik keamanan dasar seperti pengelolaan kata sandi dan privasi akun

Salah satu temuan penting dalam penelitian ini adalah kecenderungan pengguna untuk mengabaikan praktik keamanan dasar, seperti penggunaan kata sandi yang kuat, pengelolaan autentikasi ganda, serta perlindungan privasi akun. Perilaku ini menunjukkan adanya kesenjangan antara pengetahuan dan tindakan, di mana pengguna mungkin mengetahui pentingnya keamanan digital, tetapi tidak menerapkannya dalam praktik sehari-hari. Menurut penelitian (Orunsolu et al., 2018), rendahnya kesadaran keamanan sering kali berbanding lurus dengan perilaku pengguna yang lalai dalam menerapkan langkah-langkah perlindungan dasar. Akibatnya, akun pengguna menjadi lebih mudah diakses oleh pihak tidak bertanggung jawab.

Di sisi lain, faktor kenyamanan dan kemudahan penggunaan teknologi juga menjadi alasan utama pengguna mengabaikan aspek keamanan. Banyak pengguna lebih memilih kemudahan akses dibandingkan dengan keamanan yang lebih kompleks, seperti penggunaan kata sandi unik atau autentikasi dua faktor. Menurut penelitian (Istiqomah et al., 2025) perilaku pengguna dalam keamanan digital sangat dipengaruhi oleh tingkat literasi dan kesadaran yang dimiliki, di mana individu dengan literasi rendah cenderung mengabaikan praktik keamanan dasar. Kondisi ini menegaskan bahwa upaya peningkatan keamanan digital tidak cukup hanya melalui penyediaan teknologi, tetapi juga harus disertai dengan perubahan perilaku pengguna melalui edukasi yang berkelanjutan.

Bentuk Ancaman Digital yang Dihadapi

Phishing dan penipuan online menjadi ancaman paling dominan yang dialami responden

Phishing dan penipuan online merupakan bentuk ancaman digital yang paling dominan dialami oleh pengguna dalam berbagai aktivitas berbasis internet. Ancaman ini umumnya dilakukan melalui email, pesan instan, maupun situs web palsu yang dirancang menyerupai platform resmi untuk mengelabui korban. Misalnya, menurut penelitian (Alkhalil et al., 2021) phishing merupakan salah satu bentuk kejahatan siber paling umum yang memanfaatkan teknik manipulasi untuk memperoleh informasi sensitif seperti kata sandi, nomor kartu kredit, dan data pribadi lainnya. Tingginya prevalensi phishing menunjukkan bahwa metode ini masih sangat efektif karena memanfaatkan kelemahan pengguna, bukan hanya celah teknis dalam sistem. Hal ini menjadikan phishing sebagai ancaman yang sulit dihindari tanpa adanya kesadaran dan kewaspadaan yang tinggi dari pengguna.

Selain itu, perkembangan teknologi juga mendorong evolusi teknik phishing menjadi lebih canggih dan sulit dideteksi. Pelaku kini menggunakan pendekatan yang lebih personal, seperti spear phishing, yang menargetkan individu tertentu dengan informasi yang relevan dan meyakinkan. Menurut penelitian (Ali & Mohd Zaharon, 2024) variasi bentuk penipuan online seperti email scam, lottery fraud, dan financial phishing semakin meningkat seiring dengan digitalisasi layanan keuangan dan komunikasi. Kondisi ini memperkuat temuan bahwa phishing tidak hanya bersifat masif, tetapi juga adaptif terhadap perilaku pengguna. Oleh karena itu, ancaman ini menjadi sangat dominan karena mampu menyesuaikan diri dengan pola interaksi digital masyarakat modern.

Peretasan akun media sosial dan pencurian data pribadi sering terjadi akibat kelalaian penggun

Peretasan akun media sosial dan pencurian data pribadi menjadi ancaman serius yang sering terjadi akibat kelalaian pengguna dalam menjaga keamanan akun mereka. Banyak kasus menunjukkan bahwa penggunaan kata sandi yang lemah, penggunaan ulang kata sandi pada berbagai platform, serta tidak diaktifkannya autentikasi dua faktor menjadi faktor utama yang mempermudah akses tidak sah ke akun pengguna. Menurut penelitian kurangnya pemahaman pengguna terhadap serangan berbasis internet seperti phishing dan malware sering kali menyebabkan akun mereka diretas setelah mengklik tautan berbahaya. Hal ini menunjukkan bahwa kelemahan utama bukan terletak pada sistem, tetapi pada perilaku pengguna itu sendiri.

Lebih lanjut, pencurian data pribadi sering kali menjadi konsekuensi lanjutan dari peretasan akun yang berhasil dilakukan. Data yang dicuri dapat digunakan untuk berbagai tujuan ilegal, seperti penipuan identitas, penyebaran informasi palsu, hingga eksploitasi finansial. Menurut penelitian (Istiqomah et al., 2025) serangan phishing yang berhasil dapat mengarah pada pelanggaran data skala besar yang berdampak luas terhadap korban, baik secara ekonomi maupun psikologis. Kondisi ini menunjukkan bahwa keamanan akun media sosial tidak dapat dipandang sebagai hal sepele, karena data pribadi yang tersimpan di dalamnya memiliki nilai yang tinggi bagi pelaku kejahatan siber. Oleh karena itu, kesadaran dan disiplin pengguna dalam menjaga keamanan akun menjadi faktor kunci dalam mencegah ancaman ini.

Teknik social engineering dimanfaatkan pelaku untuk mengeksploitasi kelemahan psikologis korban

Social engineering merupakan teknik yang banyak dimanfaatkan oleh pelaku kejahatan siber untuk mengeksploitasi kelemahan psikologis korban, seperti rasa percaya, ketakutan, atau urgensi. Teknik ini tidak bergantung pada kecanggihan teknologi, melainkan pada kemampuan pelaku dalam memanipulasi perilaku manusia agar secara sukarela memberikan informasi sensitif. Misalnya, menurut penelitian (Atkins & Huang, 2013) pelaku social engineering merancang pesan dengan strategi persuasi tertentu yang mampu meyakinkan korban untuk mengikuti instruksi yang diberikan, seperti mengklik tautan atau mengungkapkan data pribadi. Hal ini menunjukkan bahwa aspek psikologis menjadi titik lemah utama dalam sistem keamanan digital.

Selain itu, social engineering sering kali dikombinasikan dengan teknik phishing untuk meningkatkan efektivitas serangan. Pelaku memanfaatkan berbagai skenario, seperti menyamar sebagai pihak resmi, memberikan ancaman palsu, atau menawarkan keuntungan tertentu untuk menarik perhatian korban. Menurut penelitian (Alkhalil et al., 2021) keberhasilan serangan phishing sangat dipengaruhi oleh kemampuan pelaku dalam membangun kepercayaan dan menciptakan situasi yang mendesak bagi korban. Dengan demikian, ancaman social engineering menjadi sangat berbahaya karena sulit dideteksi secara teknis dan lebih bergantung pada respons emosional pengguna. Oleh karena itu, peningkatan kesadaran psikologis dan kemampuan berpikir kritis menjadi langkah penting dalam menghadapi ancaman ini.

Strategi Perlindungan Diri di Era Digital

Penggunaan kata sandi yang kuat dan berbeda untuk setiap akun menjadi langkah perlindungan utama

Penggunaan kata sandi yang kuat dan unik untuk setiap akun merupakan salah satu strategi dasar namun sangat krusial dalam menjaga keamanan digital individu. Kata sandi yang kuat umumnya terdiri dari kombinasi huruf besar, huruf kecil, angka, dan simbol, sehingga sulit ditebak atau diretas melalui teknik brute force. Namun demikian, masih banyak pengguna yang menggunakan kata sandi sederhana atau bahkan sama untuk berbagai akun, yang secara signifikan meningkatkan risiko kebocoran data. Misalnya, menurut penelitian (Effendy & Oktiani, 2024), kelemahan dalam kebijakan penggunaan kata sandi menjadi salah satu faktor utama terjadinya pelanggaran keamanan, terutama ketika pengguna tidak memahami pentingnya kompleksitas dan keunikan kata sandi. Hal ini menunjukkan bahwa praktik sederhana seperti pengelolaan kata sandi memiliki dampak besar terhadap tingkat keamanan akun digital.

Selain itu, penggunaan kata sandi yang berbeda untuk setiap akun juga bertujuan untuk meminimalisir dampak jika terjadi kebocoran pada salah satu platform. Jika satu kata sandi digunakan secara berulang, maka peretas dapat dengan mudah mengakses berbagai akun lain yang dimiliki pengguna. Menurut penelitian (Alkhalil et al., 2021) faktor manusia menjadi aspek paling rentan dalam sistem autentikasi berbasis kata sandi, di mana kebiasaan pengguna dalam memilih dan mengelola kata sandi sering kali tidak mempertimbangkan aspek keamanan. Oleh karena itu, diperlukan kesadaran yang lebih tinggi serta dukungan teknologi seperti password manager untuk membantu pengguna dalam mengelola kata sandi secara aman dan efisien di era digital yang semakin kompleks.

Penerapan autentikasi dua faktor efektif dalam meningkatkan keamanan akun digital

Penerapan autentikasi dua faktor (Two-Factor Authentication/2FA) terbukti menjadi salah satu metode yang efektif dalam meningkatkan keamanan akun digital. Sistem ini menambahkan lapisan verifikasi tambahan selain kata sandi, seperti kode OTP (One-Time Password), biometrik, atau perangkat autentikasi lainnya. Dengan adanya lapisan tambahan ini, akses tidak sah dapat dicegah meskipun kata sandi utama telah berhasil diperoleh oleh pihak lain. Misalnya, menurut penelitian (Ali & Mohd Zaharon, 2024) penerapan multi-factor authentication mampu meningkatkan perlindungan akun secara signifikan dengan mengurangi kemungkinan keberhasilan serangan berbasis pencurian kredensial. Hal ini menunjukkan bahwa keamanan tidak lagi cukup hanya bergantung pada satu faktor autentikasi.

Lebih lanjut, efektivitas autentikasi dua faktor juga terlihat dalam kemampuannya mengurangi tingkat keberhasilan serangan phishing. Ketika pengguna mengaktifkan 2FA, pelaku tidak hanya membutuhkan kata sandi, tetapi juga akses ke faktor kedua yang biasanya bersifat sementara dan personal. Menurut penelitian (Alkhalil et al., 2021) penerapan 2FA dapat menurunkan tingkat keberhasilan phishing secara signifikan karena menambah hambatan bagi pelaku kejahatan siber. Meskipun demikian, implementasi 2FA masih menghadapi tantangan, seperti rendahnya tingkat adopsi oleh pengguna akibat persepsi bahwa sistem ini merepotkan. Oleh karena itu, edukasi mengenai manfaat dan kemudahan penggunaan 2FA perlu terus ditingkatkan.

Kewaspadaan terhadap tautan dan pesan mencurigakan menjadi kunci pencegahan serangan siber

Kewaspadaan terhadap tautan dan pesan mencurigakan merupakan strategi penting dalam mencegah berbagai bentuk serangan siber, khususnya phishing dan social engineering. Banyak serangan siber berhasil dilakukan karena pengguna secara tidak sadar mengklik tautan berbahaya atau memberikan informasi pribadi melalui pesan yang tampak meyakinkan. Oleh karena itu, kemampuan untuk mengenali ciri-ciri pesan mencurigakan, seperti kesalahan tata bahasa, alamat pengirim yang tidak resmi, atau permintaan informasi sensitif secara mendesak, menjadi keterampilan yang sangat penting. Misalnya, menurut penelitian (Van Schaik et al., 2017) kesadaran pengguna dalam mengenali pola phishing memiliki pengaruh signifikan terhadap kemampuan mereka dalam menghindari serangan siber.

Selain itu, kewaspadaan ini juga berkaitan erat dengan kemampuan berpikir kritis dan literasi digital pengguna dalam mengevaluasi informasi yang diterima. Pengguna yang memiliki tingkat kewaspadaan tinggi cenderung tidak mudah terpengaruh oleh manipulasi yang dilakukan oleh pelaku kejahatan siber. Menurut penelitian (Van Deursen & Van Dijk, 2014) faktor manusia menjadi elemen kunci dalam keberhasilan maupun kegagalan serangan phishing, di mana pengguna yang waspada dapat berperan sebagai "lapisan pertahanan terakhir" dalam sistem keamanan digital. Oleh karena itu, selain penerapan teknologi keamanan, peningkatan kesadaran dan kewaspadaan pengguna harus menjadi prioritas utama dalam strategi perlindungan diri di era digital.

Peran Literasi Digital dalam Pencegahan Risiko

Literasi digital berperan penting dalam meningkatkan kesadaran dan kemampuan identifikasi ancaman

Literasi digital memiliki peran yang sangat penting dalam meningkatkan kesadaran individu terhadap berbagai ancaman keamanan siber yang semakin kompleks. Literasi digital tidak hanya mencakup kemampuan menggunakan teknologi, tetapi juga kemampuan memahami risiko, mengevaluasi informasi, serta mengidentifikasi potensi ancaman seperti phishing dan malware. Misalnya, menurut penelitian (Helsper & Eynon, 2013) literasi digital berpengaruh signifikan terhadap perilaku keamanan siber, terutama dalam kemampuan pengguna mengenali ancaman seperti phishing dan praktik perlindungan data pribadi. Hal ini menunjukkan bahwa individu dengan literasi digital yang baik cenderung lebih mampu mendeteksi tanda-tanda serangan siber sejak dini, sehingga dapat menghindari risiko yang lebih besar.

Selain itu, literasi digital juga berfungsi sebagai fondasi dalam membangun kesadaran keamanan yang berkelanjutan. Individu yang memiliki pemahaman yang baik tentang ekosistem digital akan lebih peka terhadap perubahan pola ancaman yang terus berkembang. Menurut penelitian (Istiqomah et al., 2025) tingkat literasi digital yang tinggi berkorelasi positif dengan kemampuan pencegahan phishing, karena pengguna mampu mengenali karakteristik pesan mencurigakan dan tidak mudah terjebak dalam manipulasi digital. Dengan demikian, literasi digital tidak hanya meningkatkan kemampuan teknis, tetapi juga memperkuat aspek kognitif dan analitis dalam menghadapi ancaman siber.

Individu yang memiliki tingkat literasi digital tinggi umumnya menunjukkan perilaku yang lebih berhati-hati dalam melakukan aktivitas di ruang digital. Kehati-hatian ini tercermin dalam kebiasaan seperti memverifikasi sumber informasi, tidak sembarangan mengklik tautan, serta menjaga kerahasiaan data pribadi. Misalnya, menurut penelitian (Graham & Triplett, 2017) individu dengan literasi digital yang baik berperan sebagai "capable guardians" dalam lingkungan digital, di mana mereka mampu melindungi diri sendiri dari ancaman seperti phishing melalui perilaku yang lebih waspada. Hal ini menunjukkan bahwa literasi digital berkontribusi langsung terhadap pembentukan perilaku aman dalam penggunaan teknologi.

Lebih lanjut, tingkat literasi digital juga memengaruhi kemampuan individu dalam mengelola risiko dan اتخاذ keputusan secara rasional di lingkungan digital. Pengguna yang memiliki pemahaman tinggi cenderung tidak mudah terpengaruh oleh manipulasi emosional yang sering digunakan dalam serangan social engineering. Menurut penelitian (Van Schaik et al., 2017) , literasi digital yang tinggi dapat meningkatkan kesadaran privasi dan mendorong perilaku perlindungan data yang lebih baik. Oleh karena itu, literasi digital tidak hanya berdampak pada pengetahuan, tetapi juga pada pembentukan sikap dan perilaku yang lebih adaptif terhadap risiko keamanan digital.

Edukasi keamanan digital secara berkelanjutan diperlukan untuk membangun perilaku aman di masyarakat

Edukasi keamanan digital yang dilakukan secara berkelanjutan menjadi kunci dalam membangun perilaku aman di masyarakat. Mengingat ancaman siber yang terus berkembang, pengetahuan yang dimiliki pengguna juga harus diperbarui secara berkala agar tetap relevan dengan kondisi terkini. Program edukasi yang terstruktur, baik melalui pendidikan formal maupun pelatihan nonformal, dapat membantu meningkatkan kesadaran dan keterampilan masyarakat dalam menghadapi risiko digital. Misalnya, menurut penelitian (Istiqomah et al. 2025), edukasi berbasis literasi digital terbukti efektif dalam meningkatkan kemampuan pengguna dalam mencegah serangan phishing dan meningkatkan kesadaran keamanan secara keseluruhan.

Selain itu, edukasi yang berkelanjutan juga berperan dalam membentuk budaya keamanan digital di masyarakat. Ketika individu secara konsisten mendapatkan informasi dan pelatihan terkait keamanan digital, mereka cenderung menginternalisasi perilaku aman sebagai bagian dari kebiasaan sehari-hari. Menurut penelitian (Graham & Triplett, 2017) peningkatan literasi digital melalui edukasi dapat mengurangi tingkat viktimisasi kejahatan siber karena pengguna menjadi lebih siap dan waspada terhadap berbagai bentuk ancaman. Oleh karena itu, edukasi tidak hanya berfungsi sebagai sarana peningkatan pengetahuan, tetapi juga sebagai strategi jangka panjang dalam menciptakan ekosistem digital yang lebih aman dan bertanggung jawab.

Perilaku Pengguna dalam Mengelola Keamanan Akun

Banyak pengguna masih menggunakan kata sandi yang sama untuk berbagai akun digital

Salah satu perilaku yang paling umum ditemukan dalam pengelolaan keamanan akun adalah penggunaan kata sandi yang sama untuk berbagai platform digital. Praktik ini sering dilakukan karena alasan kemudahan dalam mengingat kredensial, terutama ketika pengguna memiliki banyak akun yang harus dikelola. Namun, kebiasaan ini justru meningkatkan risiko keamanan secara signifikan, karena jika satu akun berhasil diretas, maka akun lain dengan kata sandi yang sama juga dapat dengan mudah diakses. Misalnya, menurut penelitian (Gaw & Felten, 2006) sebagian besar pengguna cenderung menggunakan kembali kata sandi yang sama pada berbagai layanan online, meskipun mereka menyadari adanya risiko keamanan. Hal ini menunjukkan adanya kesenjangan antara pengetahuan dan praktik aktual dalam keamanan digital.

Lebih lanjut, penggunaan ulang kata sandi juga berkaitan dengan rendahnya kesadaran pengguna terhadap pentingnya manajemen kredensial yang aman. Dalam banyak kasus, pengguna tidak memahami bahwa serangan seperti credential stuffing memanfaatkan kebiasaan ini untuk mengakses akun secara massal. Menurut penelitian (Florêncio & Herley, 2007), kebiasaan penggunaan ulang kata sandi merupakan fenomena yang meluas dan menjadi salah satu penyebab utama kebocoran akun dalam skala besar. Oleh karena itu, diperlukan upaya edukasi yang lebih intensif serta penggunaan teknologi pendukung seperti password manager untuk membantu pengguna dalam menciptakan dan mengelola kata sandi yang unik dan aman.

Kebiasaan menyimpan informasi sensitif tanpa perlindungan meningkatkan risiko kebocoran data

Kebiasaan menyimpan informasi sensitif tanpa perlindungan yang memadai juga menjadi faktor utama meningkatnya risiko kebocoran data. Banyak pengguna yang menyimpan data penting seperti kata sandi, nomor identitas, atau informasi keuangan dalam perangkat pribadi tanpa enkripsi atau perlindungan tambahan. Praktik ini sering dianggap sebagai solusi praktis, namun justru membuka peluang bagi pelaku kejahatan siber untuk mengakses data tersebut dengan mudah jika perangkat diretas atau hilang. Misalnya, menurut penelitian (Florêncio & Herley, 2007) kelemahan dalam pengelolaan informasi sensitif oleh pengguna sering dimanfaatkan dalam serangan social engineering untuk memperoleh akses ke data penting secara tidak sah.

Selain itu, penyimpanan data tanpa perlindungan juga meningkatkan risiko kebocoran melalui malware atau aplikasi berbahaya yang dapat mencuri informasi dari perangkat pengguna. Dalam konteks ini, kurangnya kesadaran terhadap pentingnya enkripsi dan perlindungan data menjadi masalah utama. Menurut penelitian (Frei et al., 2009) kebocoran data sering kali terjadi bukan karena kelemahan sistem, tetapi karena kelalaian pengguna dalam melindungi informasi sensitif mereka. Oleh karena itu, diperlukan peningkatan pemahaman mengenai pentingnya penggunaan fitur keamanan seperti enkripsi, autentikasi tambahan, serta penyimpanan data yang aman untuk meminimalisir risiko kebocoran.

Kurangnya kebiasaan memperbarui sistem dan aplikasi menyebabkan celah keamanan tetap terbuka

Kurangnya kebiasaan pengguna dalam memperbarui sistem operasi dan aplikasi merupakan salah satu faktor yang menyebabkan celah keamanan tetap terbuka dan mudah dieksploitasi oleh pelaku kejahatan siber. Pembaruan perangkat lunak biasanya mencakup perbaikan bug dan patch keamanan yang dirancang untuk menutup kerentanan yang telah ditemukan. Namun, banyak pengguna yang menunda atau bahkan mengabaikan pembaruan tersebut karena dianggap tidak penting atau mengganggu aktivitas penggunaan. Misalnya, menurut penelitian (Frei et al., 2009) terdapat hubungan yang signifikan antara keterlambatan dalam melakukan pembaruan sistem dengan meningkatnya risiko eksploitasi kerentanan oleh pihak tidak bertanggung jawab.

Selain itu, rendahnya kesadaran terhadap pentingnya pembaruan sistem juga menunjukkan kurangnya pemahaman pengguna terhadap dinamika ancaman siber yang terus berkembang. Banyak pengguna tidak menyadari bahwa perangkat lunak yang tidak diperbarui menjadi target empuk bagi serangan malware dan eksploitasi keamanan. Menurut penelitian (Van Deursen & Van Dijk, 2014) perilaku pengguna dalam mengelola pembaruan perangkat lunak sangat dipengaruhi oleh persepsi mereka terhadap risiko dan manfaat pembaruan tersebut. Oleh karena itu, diperlukan edukasi yang lebih efektif untuk meningkatkan kesadaran pengguna agar secara rutin melakukan pembaruan sistem dan aplikasi sebagai bagian dari praktik keamanan digital yang baik.

Tantangan dan Upaya Peningkatan Keamanan Digital

Minimnya kesadaran masyarakat terhadap pentingnya perlindungan data pribadi menjadi hambatan utam

Minimnya kesadaran masyarakat terhadap pentingnya perlindungan data pribadi merupakan salah satu tantangan utama dalam upaya meningkatkan keamanan digital. Banyak individu yang masih menganggap data pribadi sebagai informasi yang tidak memiliki nilai strategis, sehingga cenderung membagikannya secara bebas di berbagai platform digital. Padahal, data pribadi seperti nomor identitas, alamat email, hingga informasi keuangan dapat dimanfaatkan oleh pelaku kejahatan siber untuk berbagai tujuan ilegal. Misalnya, menurut penelitian (Acquisti et al., 2015) rendahnya kesadaran privasi menyebabkan individu sering kali mengabaikan risiko jangka panjang dari penyebaran data pribadi di internet. Hal ini menunjukkan bahwa masalah utama bukan hanya pada aspek teknis, tetapi juga pada persepsi dan sikap pengguna terhadap pentingnya perlindungan data.

Selain itu, kurangnya kesadaran ini juga berdampak pada rendahnya adopsi praktik keamanan dasar, seperti pengaturan privasi akun dan penggunaan fitur keamanan tambahan. Banyak pengguna yang tidak memahami bagaimana data mereka dikumpulkan, disimpan, dan digunakan oleh platform digital. Menurut penelitian (Orunsolu et al., 2018) kompleksitas kebijakan privasi dan kurangnya transparansi dari penyedia layanan digital turut memperparah rendahnya kesadaran pengguna terhadap perlindungan data pribadi. Oleh karena itu, diperlukan pendekatan edukatif yang tidak hanya menekankan aspek teknis, tetapi juga meningkatkan pemahaman masyarakat tentang nilai dan risiko terkait data pribadi dalam ekosistem digital.

Keterbatasan akses terhadap edukasi keamanan digital di beberapa kalangan memperlebar kesenjangan literasi

Keterbatasan akses terhadap edukasi keamanan digital menjadi faktor yang memperlebar kesenjangan literasi di masyarakat. Tidak semua kelompok memiliki kesempatan yang sama untuk memperoleh pengetahuan dan keterampilan terkait keamanan digital, terutama masyarakat di daerah terpencil atau dengan tingkat pendidikan yang rendah. Kondisi ini menyebabkan adanya ketimpangan dalam kemampuan menghadapi ancaman siber, di mana kelompok dengan akses terbatas cenderung lebih rentan terhadap kejahatan digital. Misalnya, menurut penelitian (Van Deursen & Van Dijk, 2014) kesenjangan digital tidak hanya berkaitan dengan akses teknologi, tetapi juga mencakup perbedaan dalam keterampilan dan literasi digital yang dimiliki oleh individu.

Lebih lanjut, keterbatasan ini juga berdampak pada rendahnya partisipasi masyarakat dalam program edukasi keamanan digital yang tersedia. Banyak individu yang tidak menyadari pentingnya literasi digital atau tidak memiliki sumber daya untuk mengakses pelatihan yang relevan. Menurut penelitian (Helsper & Eynon, 2013) faktor sosial ekonomi, usia, dan tingkat pendidikan memiliki pengaruh signifikan terhadap kemampuan individu dalam mengakses dan memanfaatkan teknologi digital secara aman. Oleh karena itu, upaya peningkatan keamanan digital harus mempertimbangkan aspek inklusivitas agar seluruh lapisan masyarakat dapat memperoleh edukasi yang memadai dan relevan.

Kolaborasi antara pemerintah, institusi pendidikan, dan platform digital diperlukan untuk meningkatkan keamanan ekosistem digita

Upaya meningkatkan keamanan digital tidak dapat dilakukan secara individual, melainkan membutuhkan kolaborasi antara berbagai pihak, termasuk pemerintah, institusi pendidikan, dan platform digital. Pemerintah memiliki peran dalam merumuskan kebijakan dan regulasi yang melindungi data pengguna, sementara institusi pendidikan berperan dalam mengintegrasikan literasi digital ke dalam kurikulum. Di sisi lain, platform digital bertanggung jawab untuk menyediakan sistem keamanan yang kuat dan transparan bagi penggunanya. Misalnya, menurut penelitian (Graham & Triplett, 2017) pendekatan multi-stakeholder menjadi strategi yang efektif dalam mengatasi tantangan keamanan digital yang bersifat kompleks dan lintas sektor.

Selain itu, kolaborasi ini juga penting dalam menciptakan ekosistem digital yang aman dan berkelanjutan. Dengan adanya kerja sama yang sinergis, berbagai pihak dapat saling melengkapi dalam mengatasi kelemahan yang ada, baik dari segi teknis maupun edukatif. Menurut penelitian (Acquisti et al., 2015) perlindungan privasi yang efektif memerlukan kombinasi antara regulasi yang kuat, teknologi yang aman, serta kesadaran pengguna yang tinggi.

SIMPULAN DAN SARAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan, dapat disimpulkan bahwa keamanan digital merupakan isu krusial yang dipengaruhi oleh interaksi antara tingkat kesadaran pengguna, literasi digital, serta perilaku dalam mengelola keamanan akun. Temuan menunjukkan bahwa rendahnya kesadaran dan literasi digital masih menjadi faktor utama kerentanan terhadap ancaman seperti phishing, peretasan akun, dan social engineering, meskipun intensitas penggunaan teknologi terus meningkat. Misalnya, menurut penelitian (Istiqomah et al., 2025) serta (Helsper & Eynon, 2013) peningkatan literasi digital terbukti berkontribusi signifikan dalam membentuk perilaku pencegahan terhadap serangan siber dan meningkatkan kewaspadaan pengguna. Oleh karena itu, implikasi dari penelitian ini menekankan pentingnya integrasi edukasi keamanan digital secara berkelanjutan, penguatan kebijakan perlindungan data, serta penerapan teknologi keamanan seperti autentikasi dua faktor. Selain itu, diperlukan kolaborasi lintas sektor antara pemerintah, institusi pendidikan, dan platform digital untuk menciptakan ekosistem yang aman dan inklusif. Untuk penelitian selanjutnya, disarankan agar mengkaji lebih dalam faktor psikologis pengguna, efektivitas program edukasi keamanan digital, serta pengembangan model pendekatan holistik yang mengintegrasikan aspek teknis dan perilaku dalam menghadapi ancaman siber yang terus berkembang.

DAFTAR REFERENSI

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*. https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full

Ali, M. M., & Mohd Zaharon, N. F. (2024). Phishing—A cyber fraud: The types, implications and governance. *Journal of Educational Reform*. https://journals.sagepub.com/doi/abs/10.1177/10567879221082966

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences*. https://pdfs.semanticscholar.org/e868/fb7f1ea53fd018689a64a0cdef8fc76f75b3.pdf

Effendy, M. Y., & Oktiani, H. (2024). Literasi digital keamanan siber pada remaja menghadapi social engineering. *Wacana Publik*. http://wacanapublik.stisipoldharmawacana.ac.id/index.php/politik/article/view/67

Florêncio, D., & Herley, C. (2007). A large-scale study of web password habits. *Proceedings of the 16th International World Wide Web Conference*. https://dl.acm.org/doi/10.1145/1242572.1242661

Frei, S., May, M., Fiedler, U., & Plattner, B. (2009). Large-scale vulnerability analysis. *Proceedings of the 2009 SIGCOMM Workshop*. https://dl.acm.org/doi/10.1145/1592665.1592667

Gaw, S., & Felten, E. W. (2006). Password management strategies for online accounts. *Proceedings of the 2nd Symposium on Usable Privacy and Security*. https://dl.acm.org/doi/10.1145/1143120.1143127

Graham, R., & Triplett, R. (2017). Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Deviant Behavior*. https://www.academia.edu/download/51484772/Capable_Guardians_in_the_Digital_Environment_The_Role_of_Digital_Literacy_in_Reducing_Phishing_Victimization.pdf

Helsper, E. J., & Eynon, R. (2013). Distinct skill pathways to digital engagement. *European Journal of Communication, 28*(6), 696–713. https://doi.org/10.1177/0267323113499113

Istiqomah, N. A., Lorenza, N. A., & Mutia, F. (2025). The impact of digital literacy on phishing prevention behaviour: A literature review. *Pustakaloka*. https://jurnal.iainponorogo.ac.id/index.php/pustakaloka/article/download/10495/4257

Orunsolu, A. A., Afolabi, O., & Sodiya, A. S. (2018). A users' awareness study and influence of socio-demography perception of anti-phishing security tips. *Acta*

Informatica.
https://pdfs.semanticscholar.org/f181/c4e58e3266ffc121b2d83c26aef5fdba887a.pdf

Sari, S. N., & Fitri, A. O. (2025). Analisis persepsi masyarakat terhadap keamanan dan risiko cyber crime dalam perbankan digital. *Inflasi: Jurnal Ekonomi, Manajemen*. https://ejurnal.faaslibsmedia.com/index.php/inflasi/article/view/128

Van Deursen, A. J., & Van Dijk, J. A. (2014). The digital divide shifts to differences in usage. *New Media & Society, 16*(3), 507–526. https://doi.org/10.1177/1461444813487959

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Persepsi risiko keamanan siber dan perilaku kehati-hatian. *Komputer dalam Perilaku Manusia* , *75* , 547-559. https://www.sciencedirect.com/science/article/abs/pii/S074756321730359X