Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 4, Issue June, 2026 pp. 975-981 http://urj.uin-malang.ac.id/index.php/mij/index

Edukasi digital: Pentingnya meningkatkan kewaspadaan terhadap maraknya kejahatan siber di era digital

Adil Ferhan Nur
Program Studi Teknik Informatika, Universitas Islam Negeri Maulana Malik Ibrahmin Malang
e-mail: vastnigen@gmail.com

Kata Kunci:
Edukasi digital, kejahatan siber, literasi digital, UU PDP, keamanan informasi

Keywords:
Digital education, cybercrime, digital literacy, data protection, cybersecurity

A B S T R A K

Transformasi digital yang berlangsung cepat telah membawa kemudahan dalam berbagai sektor kehidupan, tetapi juga membuka peluang bagi meningkatnya ancaman kejahatan siber. Kasus kebocoran data, penipuan daring, hingga penyalahgunaan identitas menjadi peringatan serius bahwa kesadaran masyarakat terhadap keamanan digital masih rendah. Artikel ini bertujuan untuk mengkaji pentingnya edukasi digital dalam meningkatkan kewaspadaan masyarakat terhadap ancaman siber di era digital. Penelitian dilakukan dengan pendekatan kualitatif deskriptif melalui analisis literatur dari empat jurnal ilmiah relevan serta regulasi nasional seperti UU ITE dan UU Perlindungan Data Pribadi. Hasil kajian menunjukkan bahwa edukasi digital yang terstruktur, kolaborasi lintas sektor, dan peningkatan literasi hukum menjadi fondasi utama dalam membangun ketahanan siber masyarakat. Oleh karena itu, penguatan program literasi digital berbasis komunitas dinilai sebagai langkah strategis dalam menekan risiko kejahatan siber di Indonesia.

A B S T R A C T

The rapid digital transformation has brought significant convenience across various sectors but also increased the risk of cybercrime threats. Data breaches, online fraud, and identity misuse indicate that public awareness of digital security remains low. This article aims to examine the importance of digital education in enhancing public vigilance against cybercrime in the digital era. This study applies a qualitative descriptive approach through literature analysis from four relevant academic journals and national regulations such as the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law). The findings reveal that structured digital education, cross-sector collaboration, and improved legal literacy form the foundation of cyber resilience within society. Therefore, strengthening community-based digital literacy programs is considered a strategic step in mitigating cybercrime risks in Indonesia.

Pendahuluan

Perkembangan teknologi informasi dan komunikasi di Indonesia telah memicu perubahan sosial dan ekonomi secara masif. Aktivitas masyarakat yang sebelumnya dilakukan secara tatap muka kini bergeser ke ruang digital, mulai dari transaksi keuangan, pendidikan, hingga pelayanan publik. Namun, kemajuan ini membawa konsekuensi: meningkatnya ancaman kejahatan siber. Data Badan Siber dan Sandi Negara (BSSN) pada 2022 mencatat lebih dari 800 juta anomali serangan siber, yang sebagian besar menargetkan sektor publik dan layanan digital.

Walaupun pemerintah telah menghadirkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), fakta menunjukkan bahwa serangan dan kebocoran data masih marak. Akar masalahnya tidak hanya pada lemahnya sistem, tetapi juga rendahnya kesadaran dan literasi digital masyarakat.

Beberapa penelitian, seperti yang dilakukan oleh (Siagian et al., 2024) dan (Yudistira, 2023), menegaskan bahwa kebanyakan korban kejahatan siber di Indonesia adalah individu yang kurang memahami cara kerja internet dan keamanan digital. Oleh sebab itu, edukasi digital menjadi garda terdepan dalam membangun kesadaran dan kesiapsiagaan masyarakat terhadap ancaman dunia maya.

Pembahasan

Dinamika Kejahatan Siber di Indonesia

Kejahatan siber di Indonesia terus menunjukkan tren peningkatan baik dari sisi frekuensi maupun kompleksitas modus operandi. Fenomena ini tidak lagi sebatas aktivitas individu yang iseng atau kelompok kecil semata, melainkan telah menjadi bentuk kejahatan terorganisir lintas negara. Jenis kejahatan siber yang paling sering ditemukan di Indonesia meliputi *phishing*, *malware*, *ransomware*, pencurian identitas digital (*identity theft*), serta penipuan berbasis media sosial dan aplikasi keuangan digital. Berdasarkan laporan Badan Siber dan Sandi Negara (BSSN, 2024), lebih dari 1,1 miliar serangan siber terdeteksi sepanjang tahun 2023, yang menunjukkan peningkatan sekitar 35% dibandingkan tahun sebelumnya. Angka ini menegaskan bahwa Indonesia telah menjadi salah satu target empuk bagi pelaku kejahatan siber di kawasan Asia Tenggara.

Faktor penyebab utama meningkatnya kejahatan siber ini tidak hanya disebabkan oleh kelemahan infrastruktur keamanan digital, tetapi juga oleh rendahnya literasi digital dan kesadaran masyarakat terhadap ancaman dunia maya. Banyak pengguna masih mengabaikan aspek dasar keamanan, seperti penggunaan kata sandi yang kuat, pembaruan perangkat lunak, dan kewaspadaan terhadap tautan mencurigakan. (Siagian et al., 2024) menegaskan bahwa sebagian besar korban serangan siber di Indonesia merupakan pengguna individu yang tidak memahami prinsip dasar keamanan data. Kondisi ini menjadikan mereka sasaran empuk bagi pelaku kejahatan yang memanfaatkan teknik rekayasa sosial (*social engineering*).

Selain itu, perkembangan teknologi seperti *Internet of Things (IoT)* dan kecerdasan buatan (AI) yang belum diimbangi dengan sistem keamanan yang memadai juga memperbesar risiko kebocoran data dan penyalahgunaan identitas digital. Munculnya aplikasi keuangan digital dan *e-commerce* yang tidak memiliki standar keamanan tinggi kerap dijadikan pintu masuk bagi penjahat siber. Di sisi lain, upaya pemerintah dalam membangun kesadaran masyarakat melalui kampanye literasi digital seperti "Indonesia Makin Cakap Digital" yang diluncurkan oleh Kominfo memang menunjukkan hasil positif, namun belum cukup menjangkau seluruh lapisan masyarakat, khususnya di daerah pedesaan. Oleh karena itu, penguatan edukasi digital menjadi langkah fundamental untuk menekan laju peningkatan kejahatan siber di Indonesia.

Di tengah meningkatnya kejahatan siber yang semakin beragam dan sulit diprediksi, mahasiswa menempati posisi yang cukup rawan karena intensitas penggunaan teknologi yang tinggi dalam kehidupan akademik maupun sosial. Kondisi ini menuntut mahasiswa tidak hanya menguasai aspek teknis, seperti menjaga keamanan akun atau perangkat digital, tetapi juga memahami etika digital, pentingnya perlindungan data pribadi, serta cara bersikap aman dalam berinteraksi di ruang daring. (Iskandar et al., 2025) menjelaskan bahwa keamanan siber pada dasarnya tidak dapat dilepaskan dari dimensi moral dan spiritual, karena perilaku seseorang di dunia maya mencerminkan nilai dan kesadarannya sebagai individu. Oleh karena itu, konsep ruhiologi atau spiritualitas dalam dunia digital menjadi relevan untuk membimbing mahasiswa agar menggunakan teknologi secara lebih sadar, bertanggung jawab, dan bermakna. Melalui pendekatan Cyber Smart Campus, perguruan tinggi diharapkan mampu membangun lingkungan pendidikan yang tidak hanya fokus pada kecakapan teknis digital, tetapi juga menumbuhkan kesadaran keamanan siber, etika digital, serta nilai-nilai spiritual, sehingga mahasiswa dapat berkembang menjadi generasi yang cakap secara digital sekaligus bijak dalam memanfaatkan teknologi (Iskandar et al., 2025).

Meningkatnya variasi dan kompleksitas kejahatan siber tidak terlepas dari karakteristik sistem informasi modern yang menyimpan semakin banyak data sensitif pengguna. (Prakasa, 2020) menjelaskan bahwa perkembangan sistem informasi secara langsung diikuti oleh peningkatan intensitas serangan, karena sistem tersebut memuat informasi krusial seperti nomor telepon, Nomor Induk Kependudukan, tanggal lahir, hingga data perbankan. Data-data ini memiliki nilai tinggi dan sangat rentan disalahgunakan oleh pihak yang tidak bertanggung jawab. Lebih lanjut, hasil penelitiannya menunjukkan bahwa serangan siber tidak hanya menargetkan satu titik tertentu, melainkan dapat terjadi pada setiap komponen penyusun sistem informasi. Temuan ini menegaskan bahwa keamanan harus menjadi pertimbangan utama sejak tahap perancangan dan pengembangan sistem, sekaligus memperlihatkan bahwa ancaman siber bersifat menyeluruh dan tidak dapat ditangani hanya dengan pendekatan teknis semata, tanpa diimbangi peningkatan kesadaran dan literasi keamanan bagi para penggunanya (Prakasa, 2020).

Peran Regulasi dan Implementasi UU PDP

Keberadaan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) menjadi tonggak penting dalam perlindungan hak privasi warga negara Indonesia di ruang digital. Regulasi ini hadir sebagai respon atas banyaknya kasus kebocoran data yang melibatkan institusi publik maupun swasta, seperti kebocoran data pelanggan telekomunikasi, lembaga finansial, hingga platform digital besar. Namun, penerapan UU PDP dalam praktik masih menghadapi sejumlah tantangan yang signifikan, terutama pada aspek penegakan hukum dan kesadaran kelembagaan terhadap pentingnya tata kelola data yang baik (*data governance*).

Berdasarkan hasil evaluasi Kominfo (2023), masih banyak instansi pemerintah dan perusahaan swasta yang belum memiliki *Data Protection Officer (DPO)* sebagaimana diamanatkan oleh UU PDP. Hal ini menyebabkan lemahnya pengawasan terhadap proses pengumpulan, penyimpanan, dan penghapusan data pribadi. Selain itu, kendala lain terletak pada pemahaman masyarakat yang masih minim mengenai hak-hak mereka

sebagai pemilik data. Banyak pengguna internet belum mengetahui bahwa penyalahgunaan data pribadi tanpa izin dapat dikenakan sanksi hukum. (Change, 2021) menyoroti bahwa keberhasilan penerapan regulasi perlindungan data tidak hanya bergantung pada perangkat hukum, tetapi juga pada kesiapan sosial dan budaya masyarakat dalam menghargai privasi digital.

Dibandingkan dengan negara-negara maju, implementasi perlindungan data di Indonesia memang masih dalam tahap awal. Misalnya, Uni Eropa telah lama menerapkan General Data Protection Regulation (GDPR) yang mewajibkan setiap institusi memiliki sistem keamanan data yang ketat serta mekanisme transparansi kepada pengguna. Sementara di Indonesia, sosialisasi UU PDP masih terbatas di lingkungan pemerintahan dan akademik. Untuk memperkuat efektivitas regulasi ini, diperlukan langkah strategis berupa sinergi antara pemerintah, lembaga penegak hukum, dan sektor pendidikan guna memperluas pemahaman masyarakat terhadap hak perlindungan data pribadi. Dengan demikian, regulasi tidak hanya menjadi dokumen hukum formal, tetapi juga pedoman etis bagi seluruh pelaku digital di tanah air.

Edukasi Digital sebagai Pertahanan Sosial

Edukasi digital berperan sebagai garda terdepan dalam membangun ketahanan masyarakat terhadap kejahatan siber. Pendidikan mengenai keamanan siber tidak boleh berhenti pada aspek teknis seperti penggunaan perangkat lunak keamanan atau pengaturan kata sandi, tetapi juga harus menyentuh aspek nilai, etika, dan kesadaran moral dalam berteknologi. (Asnawi, 2023) menekankan bahwa program literasi digital yang berhasil adalah yang mampu menginternalisasi pemahaman bahwa keamanan digital merupakan tanggung jawab bersama, bukan hanya tanggung jawab pemerintah atau penyedia layanan.

Program-program literasi digital di Indonesia telah mulai berkembang pesat dalam beberapa tahun terakhir. Salah satu inisiatif penting adalah Gerakan Nasional Literasi Digital (GNLD) "Siberkreasi" yang digagas oleh Kominfo dan berbagai mitra strategis. Melalui gerakan ini, masyarakat diberikan pelatihan dan sosialisasi terkait keamanan data, etika berinternet, serta cara mengenali hoaks dan penipuan daring. Namun, efektivitas program ini masih bergantung pada keberlanjutan dan jangkauan implementasinya. Banyak pelatihan literasi digital masih berfokus di kota besar, sedangkan masyarakat pedesaan yang rentan terhadap penipuan daring sering kali belum tersentuh oleh kegiatan serupa.

Selain pelatihan berbasis komunitas, lembaga pendidikan juga memiliki peran vital dalam menanamkan kesadaran digital sejak usia dini. Pendidikan formal seperti sekolah dan perguruan tinggi perlu mengintegrasikan materi literasi digital ke dalam kurikulum pembelajaran. Hal ini sejalan dengan pandangan (UNESCO, 2023) yang menegaskan bahwa literasi digital harus menjadi bagian dari kompetensi dasar abad ke-21, sejajar dengan kemampuan membaca, menulis, dan berhitung. Dengan demikian, edukasi digital dapat menjadi instrumen sosial yang tidak hanya melindungi masyarakat dari ancaman siber, tetapi juga membentuk karakter generasi yang bijak dan bertanggung jawab dalam menggunakan teknologi.

Studi Lapangan dan Dampak Edukasi Masyarakat

Salah satu bukti empiris efektivitas edukasi digital dapat dilihat dari kegiatan pengabdian masyarakat yang dilakukan oleh Siagian et al. (2024) di Desa Cengkring, Kabupaten Batubara. Sebelum pelaksanaan program, masyarakat di desa tersebut sangat rentan terhadap berbagai bentuk penipuan online, seperti investasi bodong, phishing, dan penyebaran hoaks melalui media sosial. Setelah dilakukan serangkaian pelatihan dan sosialisasi mengenai cara mengenali ciri-ciri kejahatan siber, mengelola kata sandi, serta menjaga kerahasiaan data pribadi, terjadi peningkatan signifikan dalam perilaku digital masyarakat. Mereka menjadi lebih berhati-hati dalam memberikan informasi pribadi dan lebih aktif melaporkan aktivitas mencurigakan di dunia maya.

Peningkatan ini membuktikan bahwa edukasi digital memiliki dampak nyata dalam membentuk perilaku preventif terhadap ancaman siber. Program serupa dapat diadaptasi di berbagai daerah dengan melibatkan aktor lokal seperti perangkat desa, guru, dan tokoh masyarakat agar pesan literasi digital lebih mudah diterima. Selain itu, keberhasilan pelatihan di Desa Cengkring juga menunjukkan pentingnya pendekatan partisipatif, di mana masyarakat tidak hanya menjadi objek sosialisasi tetapi juga subjek aktif dalam menjaga keamanan digital lingkungannya.

Lebih jauh lagi, kolaborasi antara akademisi, lembaga pemerintah, dan komunitas lokal perlu terus diperkuat untuk menciptakan model pemberdayaan masyarakat yang berkelanjutan. Ketika masyarakat memahami bahwa keamanan digital adalah bagian dari keamanan sosial, maka terciptalah bentuk "pertahanan semesta" di ranah siber yang berbasis pada kesadaran kolektif. Dengan kata lain, semakin tinggi tingkat edukasi digital masyarakat, semakin kuat pula daya tahan bangsa terhadap ancaman kejahatan siber di masa depan.

Temuan empiris tersebut menunjukkan bahwa edukasi digital tidak hanya berdampak pada peningkatan pengetahuan, tetapi juga mampu mendorong perubahan perilaku nyata dalam menghadapi ancaman siber. Keberhasilan program di Desa Cengkring memperlihatkan bahwa ketika masyarakat dibekali pemahaman yang sederhana, praktis, dan dekat dengan aktivitas sehari-hari, kesadaran akan keamanan digital dapat tumbuh secara perlahan namun berkelanjutan. Pendekatan semacam ini sebenarnya juga relevan diterapkan di lingkungan pendidikan tinggi, terutama bagi mahasiswa yang kesehariannya sangat lekat dengan teknologi digital. Penelitian (Iskandar et al., 2024) menunjukkan bahwa meskipun literasi digital mahasiswa berada pada tingkat sedang, penguatan edukasi yang lebih terarah—khususnya pada kemampuan komunikasi digital, kolaborasi, dan pembuatan konten—dapat meningkatkan kesiapan mereka dalam menghadapi berbagai risiko siber. Dengan demikian, baik pengalaman edukasi digital berbasis komunitas maupun temuan akademik sama-sama menegaskan bahwa literasi digital yang disusun secara partisipatif dan kontekstual menjadi fondasi penting dalam membangun perilaku preventif serta ketahanan siber, baik di tingkat masyarakat maupun di lingkungan kampus.

Kesimpulan dan Saran

Kejahatan siber di Indonesia merupakan ancaman nyata yang tidak dapat diabaikan. Meski pemerintah telah menghadirkan regulasi seperti UU ITE dan UU PDP, keberhasilan penanggulangan tetap bergantung pada kesadaran masyarakat sebagai pengguna teknologi. Edukasi digital muncul sebagai solusi kunci dalam membangun kesadaran kolektif terhadap risiko dunia maya. Dengan memperkuat edukasi digital yang berorientasi pada nilai, etika, dan hukum, masyarakat tidak hanya menjadi pengguna yang cerdas, tetapi juga penjaga keamanan informasi di lingkungannya. Sinergi antara pemerintah, lembaga pendidikan, dan komunitas menjadi langkah strategis dalam mewujudkan ekosistem digital yang aman dan berkelanjutan.

Saran

1. Pemerintah perlu memperluas jangkauan program literasi digital hingga ke daerah terpencil dengan pendekatan berbasis komunitas.
2. Lembaga pendidikan sebaiknya mengintegrasikan materi literasi digital ke dalam kurikulum formal sejak tingkat dasar.
3. Penegakan hukum terhadap kejahatan siber harus dilakukan tegas, transparan, dan lintas lembaga.
4. Masyarakat perlu diberdayakan menjadi agen kesadaran digital dengan melibatkan media dan komunitas lokal.

Dengan langkah-langkah tersebut, Indonesia dapat membangun pertahanan siber berbasis edukasi dan kesadaran, menciptakan masyarakat digital yang tangguh dan beretika.

Daftar Pustaka

Asnawi, A. (2023). *Cybercrime sebagai tantangan global di era digitalisasi. Jurnal Teknologi dan Informasi*. 145–155.

Change, R. (2021). *Perlindungan data dan privasi dalam era transformasi digital. Jurnal Informasi dan Komunikasi*.

Iskandar, I., Putra, D. D., Yasin, A. I., & Khairan, K. (2025). *Cyber Smart Campus: Cakap Digital & Aman Siber*. PT. Sonpedia Publishing Indonesia. https://repository.uin-malang.ac.id/25350/

Iskandar, I., Yasin, A. I., Putra, D. D., & Khairan, K. (2024). *Analisis korelasi kemampuan literasi digital dan kesadaran keamanan siber mahasiswa di PTKI se Indonesia*. https://repository.uin-malang.ac.id/22166/

Prakasa, J. E. W. (2020). Peningkatan keamanan sistem informasi melalui klasifikasi serangan terhadap sistem informasi. *Jurnal Ilmiah Teknologi Informasi Asia*, *14*(2), 75–84. https://repository.uin-malang.ac.id/5506/

Siagian, Y., Syah, A. Z., & Irawati, N. (2024). Peningkatan Kesadaran dan Kewaspadaan Terhadap Ancaman Cybercrime Bagi Masyarakat di Era Digital. *Jurnal Pengabdian Masyarakat Mitra Kreasi Cendekia (MKC)*, *2*(2), 164–169.

UNESCO. (2023). *Digital literacy for lifelong learning. United Nations Educational, Scientific and Cultural Organization*.

Yudistira, M. (2023). *Analisis efektivitas edukasi digital terhadap pencegahan kejahatan siber di kalangan masyarakat. Jurnal Teknologi Informasi dan Edukasi, 4(3), 3802–3815.*