Jurnal Komputasi Terdistribusi

Vol.8 No.10, Oktober 2025
ISSN : 27224707

MENINGKATKAN KESADARAN PENGGUNA TERHADAP ANCAMAN SIBER MELALUI PENDIDIKAN TEKNOLOGI INFORMATIKA DAN KOMPUTER

Eric Pardede[1], Oriza Sativa[2], Putri Sihombing[3], Yos Fernandez Purba[4]
Universitas Negeri Medan
E-mail: jojopardede2@gmail.com[1], orizasativamunthe@gmail.com[2],
putrisihombing785@gmail.com[3], yospurba40@gmail.com[4]

Abstrak

Perkembangan teknologi informasi telah membawa dampak positif pada kemudahan akses data, komunikasi, serta transformasi berbagai bidang kehidupan, mulai dari pendidikan, bisnis, hingga layanan publik. Namun, kemajuan ini juga memunculkan beragam ancaman siber yang semakin kompleks, seperti hacking, phishing, malware, ransomware, hingga serangan rekayasa sosial. Ancaman-ancaman tersebut tidak hanya menimbulkan potensi kerugian finansial, tetapi juga berisiko menyebabkan kebocoran data pribadi, kerusakan reputasi, bahkan gangguan serius terhadap operasional sistem yang berakibat pada terganggunya stabilitas organisasi maupun individu. Dalam konteks ini, penelitian berfokus pada analisis peran Pendidikan Teknologi Informatika dan Komputer (PTIK) dalam meningkatkan kesadaran pengguna terhadap bahaya siber. Metode penelitian menggunakan pendekatan deskriptif kualitatif melalui studi literatur dan analisis kebijakan pendidikan keamanan siber. Hasil kajian menunjukkan bahwa integrasi materi keamanan siber ke dalam kurikulum PTIK, pelatihan praktik keamanan digital yang aplikatif, serta pemanfaatan media pembelajaran interaktif dan simulasi serangan siber dapat meningkatkan pemahaman serta sikap waspada pengguna secara signifikan. Temuan ini menegaskan pentingnya pendidikan berbasis teknologi informasi dalam menciptakan ekosistem digital yang aman, cerdas, dan bertanggung jawab, sehingga mampu mempersiapkan generasi yang memiliki literasi digital tinggi sekaligus berdaya tahan menghadapi tantangan siber global.

Kata Kunci — Keamanan Siber, Hacking, Phishing, Malware, PTIK, Edukasi Digital.

Abstract

The development of information technology has brought positive impacts on easier access to data, communication, and the transformation of various aspects of life, ranging from education and business to public services. However, these advancements have also given rise to increasingly complex cyber threats such as hacking, phishing, malware, ransomware, and social engineering attacks. Such threats not only cause potential financial losses but also carry the risk of personal data breaches, reputational damage, and even serious disruptions to system operations, which may affect the stability of organizations as well as individuals. In this regard, the research focuses on analyzing the role of Information and Computer Technology Education (ICTE) in raising user awareness of cyber threats. The research method applies a qualitative descriptive approach through literature review and analysis of cybersecurity education policies. The findings indicate that integrating cybersecurity materials into the ICTE curriculum, conducting practical digital security training, and utilizing interactive learning media and cyber-attack simulations can significantly enhance users' understanding and awareness. These findings emphasize the

importance of technology-based education in creating a digital ecosystem that is safe, intelligent, and responsible, thereby preparing a generation with strong digital literacy and resilience to face global cyber challenges.
Keywords *— Cybersecurity, Hacking, Phising, Malware, PTIK, Digital Education.*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) telah mengubah secara fundamental cara masyarakat berinteraksi, bekerja, dan belajar, menjadikan perangkat digital sebagai kebutuhan primer. Di Indonesia, tingkat adopsi teknologi sangat tinggi, dibuktikan dengan penetrasi pengguna internet yang masif [1]. Namun, akselerasi digital ini membawa konsekuensi serius, yaitu peningkatan eskalasi dan kompleksitas ancaman siber. Serangan seperti phishing, penyebaran malware, dan pencurian data pribadi kini menjadi risiko harian bagi individu dan organisasi, menimbulkan kerugian finansial, reputasi, hingga mengganggu layanan publik [2], [3]. Dalam konteks ini, keamanan siber tidak lagi hanya menjadi tanggung jawab teknisi IT, tetapi menjadi literasi dasar yang harus dimiliki oleh setiap pengguna digital.

Meskipun infrastruktur digital terus dikembangkan, celah keamanan terbesar seringkali terletak pada faktor manusia (human factor). Berbagai penelitian menunjukkan bahwa tingkat kesadaran keamanan siber di kalangan pengguna, termasuk pelajar dan mahasiswa, masih tergolong rendah atau belum memadai [4], [5]. Kurangnya pemahaman tentang praktik keamanan dasar, seperti pentingnya kata sandi yang kuat, konfigurasi privasi, dan identifikasi tautan berbahaya membuat mereka rentan terhadap rekayasa sosial dan serangan siber sederhana. Kerentanan ini diperburuk oleh kurangnya materi edukasi keamanan siber yang terstruktur dan terintegrasi dalam kurikulum pendidikan formal. Hal ini menunjukkan urgensi untuk mengintervensi dengan solusi pendidikan yang proaktif dan berkelanjutan.

Menanggapi krisis kesadaran siber ini, Pendidikan Teknologi Informatika dan Komputer (TIK) memiliki peran strategis sebagai fondasi untuk membangun literasi digital aman. Pendidikan TIK adalah wahana yang tepat untuk tidak hanya mengajarkan keterampilan teknis, tetapi juga menanamkan etika, tanggung jawab, dan kewaspadaan digital sejak dini [6]. Program edukasi TIK yang efektif terbukti mampu meningkatkan pemahaman siswa mengenai bahaya digital dan membekali mereka dengan tindakan proaktif [7], [8]. Oleh karena itu, penelitian ini bertujuan untuk menganalisis secara mendalam peran TIK.

Berdasarkan latar belakang tersebut, penelitian ini merumuskan beberapa pertanyaan kunci untuk panduan analisis. Pertama, bagaimana pendekatan deskriptif kualitatif dan studi literatur dapat mengidentifikasi tantangan dan hambatan utama dalam upaya peningkatan kesadaran pengguna terhadap ancaman siber di Indonesia? Kedua, apa peran strategis dan bentuk implementasi Pendidikan TIK, termasuk konten dan metodologi pembelajarannya, yang paling efektif dalam meningkatkan literasi dan kesadaran keamanan siber pengguna? Dan ketiga, bagaimana kebijakan-kebijakan pemerintah terkait keamanan siber dan pendidikan TIK (seperti UU PDP dan Strategi Nasional) mendukung atau perlu diselaraskan untuk mengoptimalkan upaya peningkatan kesadaran pengguna?

Sejalan dengan rumusan masalah yang telah ditetapkan, penelitian ini memiliki tiga tujuan utama yang hendak dicapai. Tujuan pertama adalah menganalisis dan mengidentifikasi tantangan utama dalam peningkatan kesadaran keamanan siber pengguna melalui kajian literatur yang komprehensif. Tujuan kedua adalah merumuskan model atau kerangka strategis implementasi Pendidikan TIK yang efektif, yang dapat diadaptasi oleh institusi pendidikan untuk menanamkan pemahaman dan keterampilan keamanan siber.

Sementara itu, tujuan terakhir adalah menganalisis kebijakan yang relevan sebagai landasan untuk merekomendasikan langkah-langkah peningkatan kesadaran keamanan siber secara holistik dan berkelanjutan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif yang bertujuan untuk menggambarkan dan menganalisis peran Pendidikan Teknolgi Informatika dan Komputer (PTIK) dalam meningkatkan kesadaran pengguna terhdapat ancaman siber. Metode ini dipilih karena sesuai untuk memperoleh pemahaman mendalam melalui kajian literatur dan analisis kebijakan yang relevan.

Peneliti menggunakan metode studi literatur dengan mengumpulkan dan menelaah berbagai jurnal, artikel, dan dokumen kebijakan terkait keamanan siber, ancaman hacking, phising, malware, serta peran pendidikan teknologi ingormatika dalam meningkatkan kesadaran keamanan digital. Sumber-sumber yang digunakan meliputi publikasi nasional dan internasional yang kredibel.

ahapan penelitian dimulai dengan proses pengumpulan literatur dari berbagai sumber terpercaya. Literatur yang dikaji dipilih berdasarkan relevansi, kebaruan, dan kredibilitas penulis atau lembaga penerbitnya. Selanjutnya, dilakukan proses identifikasi konsep-konsep utama seperti ancaman siber, kesadaran keamanan digital, serta strategi pendidikan TIK yang berperan dalam meningkatkan pemahaman pengguna.

Analisis data dalam penelitian ini menggunakan pendekatan deskriptif-analitis. Setiap informasi yang diperoleh dari literatur disintesiskan untuk menemukan pola, hubungan, serta rekomendasi strategis yang dapat diterapkan dalam konteks pendidikan. Hasil analisis kemudian disusun dalam bentuk uraian sistematis, sehingga dapat memberikan gambaran yang komprehensif mengenai pentingnya pendidikan TIK sebagai upaya meningkatkan kesadaran pengguna terhadap ancaman siber

ANALISIS KEBIJAKAN

Analisis kebijakan bersumber pada regulasi yang menjadi landasan wajib peningkatan kesadaran siber Pendidikan TIK wajib menjadi medium utama untuk mengimplementasikan strategi ini, memastikan pengguna dibekali tindakan proaktif menghadapi ancaman Tantangan kebijakan terletak pada harmonisasi kurikulum TIK formal. Kebijakan harus memastikan TIK fokus pada kompetensi Digital Safety dan yang terstruktur, bukan hanya keterampilan teknis [8]. Berbagai inisiatif Literasi Digital Nasional telah membuktikan edukasi digital safety efektif meningkatkan kesadaran siswa [5], [7]. Namun, perlu standardisasi dan alokasi sumber daya untuk integrasi materi keamanan siber secara seragam di semua jenjang pendidikan, sehingga sejalan dengan tuntutan hukum dan prioritas keamanan nasional.

TAHAPAN PENELITIAN

Penelitian ini menggunakan Pendekatan Deskriptif Kualitatif dengan Studi Literatur (Literature Review) sebagai metode utama. Pendekatan ini bertujuan untuk mengumpulkan, menganalisis, dan mensintesis data dari berbagai sumber pustaka untuk menghasilkan deskripsi mendalam mengenai peran Pendidikan TIK dalam meningkatkan kesadaran siber. Penelitian ini menggunakan Pendekatan Deskriptif Kualitatif dengan metodologi utama Studi Literatur (Literature Review). Tahapan penelitian dimulai dengan:

1. Perumusan Fokus dan Desain, : Fokus penelitian dikunci pada peran Pendidikan TIK dalam meningkatkan kesadaran keamanan siber, serta menetapkan rumusan masalah dan tujuan yang jelas.
2. Pengumpulan Data Pustaka yang dilakukan secara sistematis : Proses ini melibatkan

penelusuran basis data akademik bereputasi (seperti IEEE, Scopus, dan jurnal terakreditasi SINTA) dan dokumen kebijakan resmi pemerintah menggunakan kata kunci yang relevan, seperti cybersecurity awareness, TIK education, literasi digital, dan analisis terhadap undang-undang kunci seperti UU PDP dan Strategi BSSN [3], [9].

3. Seleksi dan Kredibilitas Sumber : Sumber yang telah dikumpulkan kemudian disaring berdasarkan kriteria inklusi (relevansi topik, metode penelitian kualitatif/deskriptif, dan kredibilitas publikasi), untuk memastikan data yang digunakan memiliki validitas tinggi, seperti temuan mengenai tingkat kesadaran di kalangan mahasiswa dan siswa [4], [5].
4. Analisis Data (Sintesis Kualitatif) : Teknik yang digunakan adalah Content Analysis dan Thematic Synthesis, di mana temuan dari literatur dikelompokkan dan dibandingkan ke dalam tema-tema utama: deskripsi ancaman siber, analisis kebijakan terkait (UU ITE dan UU PDP), dan model implementasi Pendidikan TIK yang efektif [7], [8].
5. Inferensi dan Penulisan Laporan Akhir, dilakukan dengan menginterpretasikan hasil sintesis untuk menjawab rumusan masalah secara komprehensif, merumuskan kesimpulan, dan memberikan saran rekomendasi model edukasi TIK yang proaktif.

HASIL DAN PEMBAHASAN

Hasil kajian literatur menunjukkan bahwa ancaman siber bersifat semakin kompleks dan multidimensi, mulai dari pencurian identitas, phishing yang menargetkan data pribadi, hingga penyebaran malware melalui aplikasi tidak resmi. Ancaman ini secara langsung mengganggu kerahasiaan, integritas, dan ketersediaan informasi sebagai pilar utama keamanan siber. Rendahnya tingkat kesadaran dan literasi keamanan digital, khususnya di kalangan pelajar dan masyarakat umum, masih menjadi celah terbesar yang dimanfaatkan oleh pelaku kejahatan siber. Kurangnya pemahaman terhadap risiko ini dapat berujung pada kerugian serius seperti pencurian data maupun penipuan. Temuan studi literatur konsisten menegaskan bahwa peningkatan literasi digital yang mencakup aspek pemahaman keamanan siber mampu menurunkan risiko kejahatan digital secara signifikan.

Pembahasan akan berfokus pada sintesis temuan dari studi literatur, mendeskripsikan ancaman siber, dan menjelaskan peran strategis Pendidikan TIK.

Deskripsi Ancaman Siber dan Urgensi Kesadaran Pengguna

Ancaman siber saat ini bersifat multidimensi, mulai dari pencurian identitas, phishing yang menargetkan data pribadi, hingga penyebaran *malware* melalui aplikasi tidak resmi (Mod APK) [3], [9]. Ancaman ini mengancam kerahasiaan, integritas, dan ketersediaan informasi pengguna, yang merupakan pilar utama keamanan siber [6]. Tingkat kesadaran keamanan siber yang tidak memadai di kalangan pengguna, terutama pelajar dan masyarakat umum, terbukti menjadi celah terbesar yang dieksploitasi oleh pelaku kejahatan siber [4], [5]. Rendahnya pengetahuan tentang bahaya ini dapat menyebabkan risiko serius seperti pencurian data dan penipuan [2]. Hasil penelitian menunjukkan secara konsisten bahwa peningkatan literasi digital, yang mencakup pemahaman yang kuat tentang keamanan siber, dapat secara signifikan mengurangi risiko kejahatan siber [8]

Peran Strategis Pendidikan TIK dalam Meningkatkan Kesadaran

Pendidikan TIK memiliki peran fundamental sebagai benteng digital yang proaktif. Berbeda dengan pendekatan reaktif, edukasi TIK menawarkan solusi pencegahan jangka panjang[9]. Implementasi yang efektif mencakup:

1. Integrasi Kurikulum : Materi TIK harus menyertakan modul wajib tentang Cyber Security dan Digital Safety sejak dini. Kurikulum harus berfokus pada aspek praktis, seperti cara membuat kata sandi yang kuat, mengidentifikasi tautan phishing, dan memahami konsep two-factor authentication [5], [9].
2. Edukasi Literasi Digital : Pendidikan TIK berfungsi sebagai wahana edukasi literasi digital yang lebih luas, yaitu kemampuan untuk menggunakan teknologi secara aman dan bertanggung jawab[2]. Ini melibatkan pemahaman etika bermedia digital dan cara menjaga keamanan data pribadi di dunia maya.
3. Metode Pembelajaran Interaktif : Studi literatur menunjukkan bahwa program edukasi yang melibatkan ceramah interaktif, diskusi, dan sesi tanya jawab, seperti yang diterapkan pada siswa, efektif dalam meningkatkan pemahaman siswa mengenai ancaman keamanan siber [7]. Penggunaan studi kasus nyata dan simulasi ancaman siber dapat meningkatkan kesadaran secara signifikan.

Model Peningkatan Kesadaran (Sintesis Studi Literatur)

Berdasarkan kajian literatur, model peningkatan kesadaran siber melalui Pendidikan TIK harus didasarkan pada tiga pilar utama:

1. Pengetahuan (Kognitif) : Menyediakan informasi yang akurat tentang jenis-jenis ancaman dan cara kerjanya [5].
2. Sikap (Afektif) : Menumbuhkan kesadaran diri dan rasa tanggung jawab untuk melindungi data pribadi dan orang lain (mendorong perilaku proaktif) [1].
3. Keterampilan (Psikomotorik) : Memberikan panduan praktis dalam mengkonfigurasi privasi, menggunakan perangkat lunak keamanan, dan merespons insiden siber [7].
4. Peran TIK adalah sebagai medium dan konten pembelajaran yang mampu menyalurkan ketiga pilar ini secara efisien kepada pengguna, memastikan bahwa masyarakat yang teredukasi lebih mampu menghadapi tantangan keamanan siber[10].

KESIMPULAN

Penelitian ini menyimpulkan bahwa metode studi literatur deskriptif kualitatif berhasil mengidentifikasi urgensi dan kerangka solusi untuk meningkatkan kesadaran pengguna terhadap ancaman siber. Tantangan utama terletak pada rendahnya pengetahuan dasar dan ketidakpatuhan pengguna terhadap praktik keamanan digital yang aman. Pendidikan Teknologi Informatika dan Komputer (TIK) memiliki peran strategis sebagai solusi jangka panjang dan berkelanjutan. Pemanfaatan TIK, melalui integrasi kurikulum yang berfokus pada literasi dan keamanan digital serta didukung oleh regulasi nasional, terbukti efektif dalam membangun tiga pilar kesadaran: pengetahuan, sikap proaktif, dan keterampilan praktis dalam menjaga data dan informasi.

Saran

Untuk meningkatkan kesadaran pengguna terhadap ancaman siber, disarankan agar pendidikan mengenai keamanan digital diintegrasikan secara sistematis ke dalam kurikulum sekolah maupun perguruan tinggi serta dilengkapi dengan pelatihan berkelanjutan yang menyesuaikan perkembangan ancaman terbaru. Selain itu, diperlukan kolaborasi antara akademisi, praktisi teknologi, dan industri dalam menyusun materi pembelajaran yang relevan, praktis, dan mudah dipahami. Penyampaian materi hendaknya tidak hanya bersifat teoritis, tetapi juga aplikatif melalui simulasi maupun praktik langsung, seperti mengenali email phishing, mengelola kata sandi dengan aman, dan melindungi data pribadi. Upaya sosialisasi dapat diperluas dengan memanfaatkan media digital, kampanye daring, maupun platform interaktif agar menjangkau masyarakat luas. Terakhir, setiap program pendidikan keamanan siber perlu dievaluasi secara berkala untuk menilai efektivitasnya dan menyesuaikan dengan perkembangan teknologi serta pola serangan siber yang terus berubah.

DAFTAR PUSTAKA

Yulisa Gardenia, Fitria Risyda, Muryan Awaludin, and Yoke Lucia Renica Rehatalanit, "Sosialisasi Pentingnya Cyber Security untuk Meningkatkan Kesadaran Bahaya Siber di Era Digital," J. Bakti Dirgant., vol. 2, no. 1, pp. 14–19, 2025, doi: 10.35968/3e2zfj52.

M. Ancaman et al., "BERKELANJUTAN," vol. 2, no. 6, pp. 707–711, 2025.

R. A. Permana, R. Anindita, Z. Zainol, and A. Quinn, "Analisis Metode dan Teknologi untuk Perlindungan Data dan Informasi dari Ancaman Siber," J. MENTARI Manajemen, Pendidik. dan Teknol. Inf., vol. 3, no. 2, pp. 137–146, 2025, doi: 10.33050/mentari.v3i2.744.

A. F. Mahendra, P. Hatta, and Y. H. Aristyagama, "Analisis Tingkat Kesadaran Keamanan Cyber di Media Sosial Instagram: Studi Kasus pada Siswa SMK Negeri 1 Banyudono," Bina Insa. Ict J., vol. 11, no. 1, p. 86, 2024, doi: 10.51211/biict.v11i1.2963.

T. Tan, H. Sama, T. Wibowo, G. Wijaya, and O. E. Aboagye, "Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam," J. Teknol. dan Inf., vol. 14, no. 2, pp. 163–173, 2024, doi: 10.34010/jati.v14i2.12518.

M. Wathoni et al., "Kesadaran Keamanan Siber (Cyber Security Awareness) Pada Smp Labschool Fip Umj," Pros. Semin. Nas. LPPM UMJ, pp. 1–5, 2023, [Online]. Available: http://jurnal.umj.ac.id/index.php/semnaskat

Y. Ceng Giap, M. Prawira Gunawan, D. Erickwitopo, J. Allexandro Kebaowolo, J. Valentino Salim, and M. Dandi Cahyadi, "Peningkatan Literasi Digital Melalui Edukasi Keamanan Siber di Kalangan Siswa Sekolah Menengah," J. Igakerta, vol. 1, no. 3, pp. 6–10, 2024, doi: 10.70234/7xv09h64.

Zulfa Ar Rahman, "Pemanfaatan Teknologi Informasi dalam Edukasi Literasi Digital untuk Peningkatan Keamanan Data dan Pencegahan Kejahatan Siber di Masyarakat Rawang Panca Arga," Merkurius J. Ris. Sist. Inf. dan Tek. Inform., vol. 2, no. 6, pp. 82–90, 2024, doi: 10.61132/merkurius.v2i6.399.

F. B. Santoso, R. Pujianto, and T. Ramadhan, "Smishing Guard: Strategi Pengembangan Sistem Deteksi Dan Respons Ancaman Sms Phishing," J. Inf. Inf. Secur., vol. 5, no. 2, p. 88955882, 2024, [Online]. Available: http://ejurnal.ubharajaya.ac.id/index.php/jiforty

E. S. B. Herawati, Z. Mustofa, M. N. Sari, N. R. P. Mirsa, A. P. Widiyan, and Y. Astuti, "Edukasi Digital Safety Dalam Meningkatkan Kecakapan Bermedia Digital Siswa," Lamahu J. Pengabdi. Masy. Terintegrasi, vol. 3, no. 1, pp. 47–54, 2024, doi: 10.37905/ljpmt.v3i1.24090.