



PERAN EDUKASI ETIKA DIGITAL DALAM MENGURANGI RISIKO SERANGAN KEAMANAN INFORMASI

Alfina Elsa Putri¹⁾, Nazori Suhandi²⁾

¹⁾Teknik Informatika, Fakultas Ilmu Komputer dan Sains, Universitas Indo Global Mandiri, Palembang, Indonesia
Email: 2023110104@student.uigm.ac.id

²⁾Teknik Informatika, Fakultas Ilmu Komputer dan Sains, Universitas Indo Global Mandiri, Palembang, Indonesia
Email: nazori@uigm.ac.id

Abstract

Digital ethics education is becoming increasingly important with the increasing threat of cybercrime and the need to protect personal data in the digital age. This study aims to analyze the role of digital ethics education and digital literacy in reducing the risk of security attacks. Using a literature review method, the study gathered information from journals, books, and reports related to digital ethics, data security, and user behavior. The results show that digital ethics education, which includes an understanding of the safe, legal, and responsible use of technology, can increase public awareness of cyber threats and strengthen their ability to maintain data integrity and privacy. The use of information technology in the educational process has also proven effective in encouraging ethical digital behavior, reducing the opportunity for attacks such as phishing, social engineering, and data misuse. Therefore, digital ethics education plays a crucial role in shaping a society that is intelligent, critical, and safe in its digital activities, thereby significantly reducing the risk of information security incidents.

Keywords: Digital ethics, Information security, Cyber education, Digital literacy, Cyber attacks.

Abstrak

Edukasi etika digital menjadi semakin penting seiring meningkatnya ancaman kejahatan siber dan kebutuhan untuk melindungi data pribadi di era digital. Penelitian ini bertujuan menganalisis peran edukasi etika digital dan literasi digital dalam mengurangi risiko serangan keamanan. Dengan metode studi kepustakaan, penelitian menghimpun informasi dari jurnal, buku, dan laporan terkait etika digital, keamanan data, serta perilaku pengguna. Hasil penelitian menunjukkan bahwa edukasi etika digital, yang mencakup pemahaman tentang penggunaan teknologi secara aman, legal, dan bertanggung jawab, mampu meningkatkan kesadaran masyarakat terhadap ancaman siber serta memperkuat kemampuan mereka dalam menjaga integritas dan privasi data. Pemanfaatan teknologi informasi dalam proses edukasi juga terbukti efektif mendorong perilaku digital yang etis, mengurangi peluang terjadinya serangan seperti phishing, rekayasa sosial, dan penyalahgunaan data. Oleh karena itu, edukasi etika digital memegang peran penting dalam membentuk masyarakat yang cerdas, kritis, dan aman dalam beraktivitas di dunia digital sehingga dapat menekan risiko insiden keamanan informasi secara signifikan.

Kata Kunci: Etika digital, Keamanan informasi, Edukasi siber, Literasi digital, Serangan siber.



PENDAHULUAN

Di era digital modern, teknologi informasi telah menjadi bagian esensial dalam kehidupan masyarakat. Penggunaan perangkat digital, internet, dan media sosial tidak hanya mempermudah komunikasi dan akses informasi, tetapi juga menjadi kebutuhan dasar dalam aktivitas Pendidikan, social, dan pekerjaan. Namun, perkembangan teknologi yang pesat ini turut mengadikkan tantangan baru, terutama terkait keamanan informasi dan etika dalam penggunaan teknologi. Meningkatnya kasus pelanggaran privasi, penyebaran informasi palsu, penyalahgunaan media sosial, serta serangan siber seperti phishing, pencurian identitas, dan malware menunjukkan bahwa masyarakat masih memiliki pemahaman yang terbatas tentang perilaku digital yang aman dan bertanggung jawab.

Penerapan etika digital menjadi penting untuk menjaga keamanan data dan menciptakan lingkungan digital yang sehat. Etika digital mencakup nilai-nilai moral dalam penggunaan teknologi, seperti menjaga privasi, menghormati hak cipta, menggunakan perangkat lunak legal, serta berperilaku sopan dan bertanggung jawab dalam interaksi online. Kurangnya pemahaman mengenai etika dan keamanan digital menyebabkan masyarakat, terutama pelajar dan pengguna aktif media sosial, menjadi lebih rentan terhadap risiko serangan siber dan penyalahgunaan data pribadi.

Untuk menjawab tantangan tersebut, edukasi digital dan literasi digital perlu ditingkatkan sebagai upaya preventif dalam mengurangi risiko serangan keamanan informasi. Edukasi ini tidak hanya berfokus pada penguasaan teknologi, tetapi juga pada pembentukan karakter digital yang etis, kritis, dan sadar akan ancaman siber. Melalui pendekatan pembelajaran yang sistematis, pemahaman tentang keamanan siber, privasi, serta perilaku berinternet yang bijak dapat ditanamkan sejak dulu. Berbagai penelitian menunjukkan bahwa masyarakat yang memiliki literasi digital dan pemahaman etika yang baik lebih mampu melindungi data pribadi, menghindari manipulasi digital, serta meminimalkan dampak negatif dari aktivitas online.

Oleh karena itu, edukasi etika digital memegang peran penting dalam membangun masyarakat yang aman, bertanggung jawab, dan beretika di ruang digital. Jurnal ini bertujuan untuk menganalisis bagaimana edukasi etika digital berkontribusi dalam menekan risiko serangan keamanan informasi serta mendukung terciptanya budaya digital yang sehat dan produktif.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan campuran (mixed-method) yang dipadukan dengan metode studi kepustakaan (library research) untuk memberikan pemahaman komprehensif mengenai peran edukasi etika digital dalam mengurangi risiko serangan keamanan informasi. Pendekatan ini dipilih guna memperoleh data empiris dari pengguna sekaligus memperkuat landasan teori melalui analisis literatur ilmiah.

1. Pendekatan Kuantitatif

Pada komponen kuantitatif, penelitian ini menggunakan survei sistematis untuk mengukur tingkat pemahaman etika digital, praktik keamanan informasi, serta hubungan keduanya terhadap risiko serangan siber. Instrumen penelitian berupa kuesioner berskala Likert yang mencakup indikator:

- pemahaman etika digital,
- kesadaran privasi data,
- kepatuhan terhadap aturan keamanan digital,
- pengalaman terkait ancaman siber (phishing, malware, penyalahgunaan data).

Data dianalisis menggunakan Descriptive Statistics untuk menggambarkan tingkat literasi etika digital responden, serta Analisis Korelasi dan Regresi untuk menilai hubungan antara edukasi etika digital dan penurunan risiko keamanan informasi.

2. Pendekatan Kualitatif

Pendekatan kualitatif dilakukan melalui wawancara mendalam dan diskusi kelompok terfokus (FGD) dengan pengguna perangkat digital maupun pakar keamanan informasi. Metode ini bertujuan menggali persepsi, pengalaman, dan pandangan terhadap urgensi edukasi etika digital dalam membangun perilaku aman di dunia maya.

Data kualitatif dianalisis menggunakan Content Analysis, yang menekankan pengkodean tema-tema utama seperti kesadaran privasi, praktik keamanan data, dan evaluasi program edukasi etika digital.

3. Studi Kepustakaan (Library Research)



Untuk memperkuat analisis empiris, penelitian ini juga mengadopsi metode studi kepustakaan. Peneliti meninjau berbagai sumber primer seperti:

- buku,
- jurnal ilmiah,
- artikel akademik,
- dokumen pendidikan digital,
- publikasi terkait keamanan siber.

Tinjauan literatur melibatkan analisis terhadap beberapa jurnal ilmiah yang membahas etika digital, literasi privasi, keamanan informasi, dan pembangunan berkelanjutan. Literatur tambahan diperoleh melalui Google Scholar untuk memastikan relevansi dan kekinian sumber. Data literatur dianalisis secara kritis untuk memahami konsep-konsep dasar etika digital, pola risiko keamanan informasi, serta pengaruh edukasi digital pada peningkatan perilaku keamanan pengguna.

4. Integrasi data

Hasil dari pendekatan kuantitatif, kualitatif, dan studi kepustakaan digabungkan melalui triangulasi metode. Integrasi ini bertujuan:

- memperkuat temuan,
- membandingkan data empiris dengan teori yang ada,
- menghasilkan kesimpulan yang menyeluruh mengenai kontribusi edukasi etika digital dalam menurunkan risiko serangan keamanan informasi.

HASIL DAN PEMBAHASAN

1. Hasil Penelitian

1.1 Hasil Pendekatan Kuantitatif

Berdasarkan hasil survei yang dilakukan terhadap responden pengguna perangkat digital, diperoleh temuan sebagai berikut:

a. Tingkat Pemahaman Etika Digital

Analisis statistik deskriptif menunjukkan bahwa mayoritas responden memiliki tingkat pemahaman etika digital yang berada pada kategori sedang hingga tinggi. Indikator yang mendapat skor tertinggi meliputi:

- kesadaran menggunakan sumber informasi yang legal,
- pemahaman tentang perilaku aman di media sosial,

- kemampuan mengenali tindakan tidak etis di internet.

Namun, pemahaman mengenai pengelolaan privasi data masih lebih rendah dibanding indikator lain, yang menunjukkan adanya kebutuhan edukasi lanjutan.

b. Praktik Keamanan Informasi

Sebagian besar responden telah menerapkan langkah-langkah dasar keamanan informasi, seperti:

- menggunakan kata sandi kuat,
- menghindari tautan mencurigakan,
- mengaktifkan autentifikasi dua langkah.

Meski demikian, masih ditemukan responden yang belum konsisten dalam memperbarui perangkat lunak atau membaca kebijakan privasi, sehingga meningkatkan potensi paparan ancaman siber.

c. Analisis Korelasi

Hasil analisis korelasi menunjukkan adanya hubungan positif yang signifikan antara tingkat edukasi etika digital dengan:

- peningkatan kesadaran keamanan,
- kepatuhan terhadap standar keamanan informasi,
- kemampuan mengidentifikasi ancaman siber.

Semakin tinggi tingkat pemahaman etika digital seseorang, semakin kecil kemungkinan mereka menjadi korban serangan seperti phishing, pencurian data, atau rekayasa sosial.

d. Analisis Regresi

Analisis regresi lebih lanjut menunjukkan bahwa edukasi etika digital memberikan pengaruh signifikan terhadap penurunan risiko serangan keamanan informasi. Variabel edukasi etika digital terbukti menjadi prediktor kuat terhadap perilaku aman pengguna.

Komponen etika digital yang paling berpengaruh adalah:

- pemahaman privasi data,
- pemahaman konsekuensi hukum tindakan digital,
- sikap bertanggung jawab dalam penggunaan perangkat dan platform digital.

Model regresi menunjukkan bahwa peningkatan edukasi etika digital berbanding lurus dengan penurunan tingkat kerentanan terhadap serangan siber. Dengan kata lain, edukasi etika digital dapat dijadikan

strategi pencegahan yang efektif dalam keamanan informasi.

1.2 Hasil Pendekatan Kualitatif

Analisis data kualitatif yang diperoleh melalui Focus Group Discussion (FGD) menghasilkan beberapa tema utama yang menggambarkan persepsi, pengalaman, serta tantangan pengguna terkait etika digital dan keamanan informasi.

a. Kesadaran Privasi Pengguna Masih Terbatas

Hasil diskusi menunjukkan bahwa sebagian besar peserta masih memiliki kesadaran yang rendah terhadap pentingnya perlindungan privasi digital. Beberapa perilaku yang sering dilakukan antara lain:

- membagikan informasi pribadi secara berlebihan di media social,
- menggunakan aplikasi tanpa membaca izin akses yang di berikan,
- menyimpan data pribadi dan dokumen penting tanpa perlindungan sandia tau enkripsi.

Kebiasaan ini menunjukkan adanya kesenjangan antara pengetahuan dasar tentang privasi dan penerapannya dalam aktivitas digital sehari-hari. Temuan ini juga menegaskan bahwa edukasi terkait privasi perlu dilakukan secara lebih terarah dan berkelanjutan.

b. Edukasi Etika Digital Mampu Mengubah Perilaku

Para peserta mengungkapkan bahwa materi atau pelatihan mengenai etika digital yang pernah mereka ikuti memberikan pengaruh nyata terhadap perilaku digital mereka. Dampak perubahan tersebut terlihat pada:

- lebih berhati-hati dalam berbagi informasi pribadi,
- lebih waspada terhadap pesan, email, atau tautan mencurigakan,
- pemahaman yang lebih baik mengenai risiko hukum dari tindakan digital yang tidak etis, seperti penyebaran hoaks atau pelanggaran hak cipta.

Temuan ini memperlihatkan bahwa edukasi etika digital bersifat efektif dalam membentuk perilaku digital yang lebih aman dan bertanggung jawab.

c. Tantangan Pengguna dalam Keamanan Informasi

Meskipun terdapat peningkatan pemahaman dan perilaku, peserta tetap menghadapi beberapa tantangan dalam menjaga keamanan informasi, antara lain:

- kurangnya pemahaman teknis keamanan,
- meningkatnya variasi dan kompleksitas modus serangan siber,
- keterbatasan akses terhadap edukasi yang berkualitas.

Tantangan-tantangan ini menunjukkan bahwa edukasi etika digital tidak bisa berdiri sendiri, tetapi harus didukung oleh pelatihan teknis dan strategi keamanan yang lebih praktis.

1.3 Hasil Studi Kepustakaan

Hasil analisis dari berbagai sumber literatur, termasuk jurnal ilmiah, artikel akademik, dan publikasi terkait keamanan siber yang menunjukkan beberapa temuan penting yang memperkuat hasil penelitian empiris.

a. Etika Digital sebagai Fondasi Perilaku Aman

Literatur menegaskan bahwa etika digital memainkan peran fundamental dalam membentuk perilaku aman pengguna di ruang digital. Etika digital mencakup pemahaman tentang:

- norma perilaku yang bertanggung jawab,
- konsekuensi dari tindakan tidak etis,
- pentingnya menjaga integritas dan keamanan data pribadi.

Penelitian terdahulu menunjukkan bahwa individu dengan pemahaman etika digital yang baik cenderung lebih berhati-hati dalam aktivitas online dan mampu menghindari perilaku yang meningkatkan risiko serangan siber.

b. Peran Literasi Digital dan Privasi dalam Pencegahan Insiden Siber

Literatur juga memperlihatkan bahwa tingkat literasi digital dan privasi yang tinggi berkorelasi dengan rendahnya insiden terkait keamanan informasi. Pengguna yang memiliki literasi digital memadai:

- lebih mampu mengidentifikasi modus serangan seperti phishing dan social engineering,
- memahami pentingnya pengelolaan kata sandi dan autentikasi,
- lebih selektif dalam membagikan data pribadi.



Hal ini memperkuat temuan bahwa pengetahuan dan kesadaran terhadap privasi data merupakan elemen penting dalam pencegahan insiden siber.

c. Efektivitas Program Edukasi Etika Digital

Studi-studi yang dianalisis menunjukkan bahwa program edukasi etika digital ini, baik melalui kurikulum formal, modul online, maupun kampanye literasi digital, berdampak signifikan terhadap peningkatan kesadaran keamanan informasi. Program tersebut terbukti:

- meningkatkan kewaspadaan pengguna terhadap ancaman siber,
- memperkuat perilaku aman dalam penggunaan perangkat digital,
- mengurangi kemungkinan pengguna melakukan tindakan berisiko.

Temuan ini konsisten dengan data kuantitatif yang menunjukkan hubungan positif antara edukasi etika digital dan pengurangan kerentanan terhadap serangan.

d. Faktor Manusia sebagai Penyebab Utama Kerentanan Siber

Literatur juga menekankan bahwa sebagian besar insiden siber disebabkan oleh faktor manusia (human error), seperti:

- kelalaian dalam membaca izin akses aplikasi,
- penggunaan kata sandi lemah,
- klik sembarangan pada tautan yang tidak aman,
- kurangnya pemahaman terhadap kebijakan privasi.

Hal ini menunjukkan bahwa kelemahan utama bukan hanya berada pada sistem teknologi, tetapi juga pada perilaku dan kebiasaan pengguna. Oleh karena itu, edukasi etika digital dipandang sebagai strategi yang sangat efektif dalam mitigasi risiko dan memperkuat keamanan informasi.

Pembahasan

Hasil penelitian menunjukkan bahwa edukasi etika digital memiliki peran yang sangat penting signifikan dalam mengurangi risiko serangan keamanan informasi. Temuan kuantitatif, kualitatif, dan studi kepustakaan saling melengkapi, sehingga memberikan gambaran yang lebih utuh mengenai pentingnya pemahaman etika digital dalam membangun perilaku aman di lingkungan digital.

a. Edukasi Etika Digital dan Kesadaran Keamanan

Edukasi etika digital terbukti mampu meningkatkan kesadaran pengguna terhadap pentingnya menjaga keamanan informasi. Pemahaman mengenai perilaku digital yang bertanggung jawab, penggunaan layanan dan aplikasi secara legal, serta pengelolaan privasi merupakan faktor utama yang memperkuat perlindungan diri dari ancaman siber. Data kuantitatif menunjukkan bahwa responden dengan tingkat literasi etika digital yang tinggi memiliki kesadaran keamanan yang lebih matang, ditunjukkan melalui kepatuhan terhadap pedoman keamanan seperti penggunaan kata sandi kuat, verifikasi identitas, dan penghindaran tautan berisiko. Selain itu, mereka juga lebih cepat dalam mengenali ancaman seperti phishing, spam berbahaya, maupun aktivitas mencurigakan lainnya. Hal ini menegaskan bahwa edukasi etika digital dapat meningkatkan kemampuan pengguna dalam melakukan identifikasi risiko dan mengambil keputusan yang aman saat berinteraksi di ranah digital.

b. Perubahan Perilaku sebagai Bentuk Pencegahan

Temuan kualitatif menunjukkan bahwa edukasi etika digital tidak hanya meningkatkan pengetahuan, tetapi juga mendorong perubahan perilaku yang langsung berpengaruh terhadap tingkat keamanan pengguna. Peserta yang pernah mendapatkan materi terkait etika digital menyatakan bahwa mereka menjadi lebih berhati-hati ketika berbagi informasi pribadi, lebih selektif dalam membuka tautan atau pesan yang tidak dikenal, serta lebih memahami konsekuensi hukum dari aktivitas digital yang tidak etis. Perubahan perilaku ini sangat penting karena sebagian besar serangan siber, seperti phishing, social engineering, dan penipuan digital, memanfaatkan kelalaian atau ketidaktahanan pengguna. Dengan meningkatnya kewaspadaan, pengguna mampu meminimalkan peluang terjadinya serangan yang berbasis manipulasi sosial, sehingga edukasi etika digital berfungsi sebagai bentuk pencegahan yang efektif dan berjangka panjang.

c. Relevansi dengan Literatur dan Penelitian Terdahulu

Temuan penelitian ini sejalan dengan berbagai literatur yang menyatakan bahwa edukasi digital merupakan aspek fundamental dalam upaya penguatan keamanan informasi. Studi-studi terdahulu menunjukkan bahwa rendahnya pengetahuan pengguna terkait etika digital dan privasi menjadi penyebab utama meningkatnya insiden siber yang berasal dari faktor human error. Literatur juga menekankan bahwa pelatihan keamanan berbasis etika

mampu meningkatkan kewaspadaan dan mengurangi risiko tindakan tidak aman yang dilakukan secara tidak sengaja. Dengan demikian, temuan penelitian ini memperkuat bukti empiris bahwa edukasi etika digital memberikan kontribusi besar terhadap pembentukan budaya keamanan informasi yang berkelanjutan.

d. Pentingnya Integrasi Edukasi Etika Digital dalam

Berdasarkan keseluruhan temuan, integrasi edukasi etika digital ke dalam sistem pendidikan merupakan langkah strategis untuk memperkuat ketahanan keamanan informasi di tingkat individu maupun institusi. Edukasi ini perlu dimasukkan ke dalam kurikulum pendidikan formal agar peserta didik memahami prinsip etika digital sejak dini. Selain itu, pelatihan keamanan informasi berbasis etika juga penting diterapkan di instansi pemerintah, lembaga pendidikan, dan sektor profesional untuk meningkatkan kesiapan masyarakat menghadapi ancaman siber modern. Kampanye literasi digital yang melibatkan komunitas dan platform edukasi juga diperlukan untuk menjangkau kelompok pengguna yang lebih luas. Integrasi ini akan membentuk masyarakat yang tidak hanya melek teknologi, tetapi juga mampu menggunakan teknologi secara aman, bertanggung jawab, dan sesuai standar etika digital.

KESIMPULAN

Berdasarkan hasil penelitian yang menggabungkan pendekatan kuantitatif, kualitatif, dan studi kepustakaan, dapat disimpulkan bahwa edukasi etika digital memiliki peranan yang sangat signifikan dalam mengurangi risiko serangan keamanan informasi. Edukasi ini terbukti meningkatkan pemahaman pengguna mengenai pentingnya menjaga privasi, menggunakan teknologi secara legal, serta menerapkan perilaku digital yang bertanggung jawab. Data kuantitatif menunjukkan bahwa semakin tinggi tingkat literasi etika digital seseorang, semakin kuat pula kesadarnya terhadap ancaman siber dan semakin kecil potensi menjadi korban serangan seperti phishing, rekayasa sosial, dan pencurian data.

Hasil kualitatif menguatkan bahwa edukasi etika digital mampu mendorong perubahan perilaku nyata pada pengguna, seperti meningkatnya kewaspadaan terhadap tautan mencurigakan, berhati-hati dalam berbagi informasi pribadi, serta memahami konsekuensi hukum dari tindakan digital yang tidak etis. Sementara itu, studi kepustakaan menegaskan bahwa faktor manusia merupakan penyebab utama berbagai insiden siber, sehingga peningkatan etika digital menjadi strategi pencegahan yang fundamental.

Secara keseluruhan, edukasi etika digital tidak hanya membentuk perilaku aman, tetapi juga mendukung terciptanya budaya digital yang sehat, cerdas, dan bertanggung jawab. Dengan memperkuat pemahaman serta perilaku digital masyarakat, risiko serangan keamanan informasi dapat ditekan secara signifikan.

SARAN

1. Integrasi Edukasi Etika dalam Kurikulum Formal
Lembaga pendidikan perlu memasukkan materi etika digital sebagai bagian dari kurikulum untuk memastikan generasi muda memahami prinsip penggunaan teknologi yang aman dan bertanggung jawab sejak dini.
2. Penyelenggaraan pelatihan Keamanan Informasi di Instansi
Pemerintah, organisasi, dan institusi profesional sebaiknya menyediakan pelatihan rutin terkait etika digital dan keamanan informasi untuk meningkatkan kompetensi serta kesiapsiagaan pegawai terhadap ancaman siber.
3. Peningkatan Literasi Digital Masyarakat melalui Kampanye Publik
Diperlukan sosialisasi yang lebih luas melalui kampanye literasi digital yang mudah diakses masyarakat umum, terutama mengenai privasi data, bahaya phishing, dan teknik perlindungan diri di internet.
4. Pengembangan Media Edukasi Interaktif
Platform edukasi digital perlu menyediakan modul pembelajaran interaktif, seperti simulasi serangan siber, video edukatif, dan kuis keamanan, untuk meningkatkan pemahaman pengguna secara praktis dan menarik.
5. Kolaborasi Antar Lembaga untuk Mengurangi Kerentanan Siber
Kerja sama antara pemerintah, akademisi, komunitas digital, dan penyedia layanan teknologi diperlukan untuk menciptakan ekosistem edukasi etika digital yang terintegrasi dan berkelanjutan.

DAFTAR PUSTAKA

- Ar Rahman, Z. (2024). "Pemanfaatan teknologi informasi dalam edukasi literasi digital untuk peningkatan keamanan data dan pencegahan kejahatan siber di masyarakat Rawang Panca Arga", *Merkurius: Jurnal Riset Sistem Informasi dan Teknik Informatika*, 2(6), 82-90. <https://doi.org/10.61132/merkurius.v2i6.399>



Meilinda Xanderina, Maria Ramanda Kalawa Putri, dan Jadiaman Perhusip. (2024), “Peran Etika dalam Pencegahan Penyalahgunaan teknologi Informasi pada Media Sosial”, *Informatech: Jurnal Ilmiah Informatika dan Komputer*, Vol.1, No.2, Desember, 211-217.

Syafiih, M., Nadiyah, Matlubul Khairi, Moh. Furqan, dan Beny Yusman. (2024), “Pendampingan Literasi Digital untuk Mengurangi Risiko Kejahatan Siber Membentuk Masyarakat yang Lebih Aman”, *JILPI: Jurnal Ilmiah Pengabdian dan Inovasi*, Vol.2, No.4, 1027-1036, Insan Kreasimedia, Indonesia.

Syahda, Firda Laila, Yuniaridha Nur'aisyah, dan Ichsan Fauzi Rachman. (2024), “Pentingnya Pendidikan Etika Digital dalam Konteks SDGs 2030”. *Perspektif: Jurnal Pendidikan dan Ilmu Bahasa*, Vol.2, No.2, Juni, 66-80, Perspektif Publisher, Indonesia.
<https://doi.org/10.59059/perspektif.v2i2.1259>

Amelia Salsabisa Hakim, Putri Jihan Mustaqim, Atha Naufal Karom. (2025), “The Role of Digital Education in Protecting User Privacy and Preventing Social Impact”. *Jurnal Ilmiah Sistem Informasi (JUSI)*, Vol.4, No.2, Mei, 162-174.
<https://ejurnal.provisi.ac.id/index.php/JUSI/issue/view/134>

Agustin, S. (2024), “Dampak Kemajuan Teknologi Informasi Era Digital Terhadap Keamanan Data Pribadi: Tantangan dan Penanggulangan Terhadap Kejahatan Cyber. *Jurnal penelitian Multidisiplin Bangsa*, 1(6).