



LITERASI DIGITAL SEBAGAI STRATEGI PREVENTIF CYBER CRIME DI KALANGAN MAHASISWA

Nurul Setyawati Handayani¹; Arin Prajawinanti²; Dewi Alifatul Wasi'ah³

^{1,2,3}Universitas Islam Negeri Sayyid Ali Rahmatullah Tulungagung

Korespondensi: arin.prajawinanti@uinsatu.ac.id

ABSTRAK

Transformasi digital dalam pendidikan tinggi meningkatkan ketergantungan mahasiswa pada teknologi sekaligus memperbesar risiko *cyber crime* seperti *phishing*, *impersonation*, *spamming*, dan *malware*. Penelitian ini bertujuan untuk menganalisis pengalaman mahasiswa dalam menghadapi *cyber crime* serta mengkaji literasi digital sebagai strategi preventif. Penelitian ini menggunakan pendekatan kualitatif dengan desain studi kasus pada lima mahasiswa Universitas Islam Negeri Sayyid Ali Rahmatullah Tulungagung yang dipilih secara purposive. Data dikumpulkan melalui wawancara semi terstruktur, observasi, dan dokumentasi, serta dianalisis menggunakan model interaktif Miles, Huberman, dan Saldana. Hasil penelitian menunjukkan bahwa mahasiswa mengalami berbagai bentuk *cyber crime* dengan tingkat kesadaran dan persepsi risiko yang berbeda. Literasi digital berperan sebagai mekanisme protektif dalam meningkatkan kemampuan evaluasi kritis, verifikasi informasi, dan perilaku digital yang aman. Namun, strategi preventif yang dilakukan masih bersifat individual dan belum terintegrasi secara institusional. Kontribusi (*novelty*) penelitian ini terletak pada pendekatan studi kasus yang mengaitkan secara empiris pengalaman nyata mahasiswa dengan literasi digital sebagai strategi preventif *cyber crime*.

Kata kunci: *cyber crime*, literasi digital, strategi preventif, mahasiswa, pendidikan tinggi

DIGITAL LITERACY AS A PREVENTIVE STRATEGY FOR CYBER CRIME AMONG STUDENTS

ABSTRACT

Digital transformation in higher education has increased students' reliance on technology while simultaneously heightening the risk of cyber crime such as *phishing*, *impersonation*, *spamming*, and *malware*. This study aims to analyze students' experiences in dealing with cyber crime and to examine digital literacy as a preventive strategy. This research employs a qualitative approach with a case study design involving five students of Sayyid Ali Rahmatullah State Islamic University of Tulungagung selected through purposive sampling. Data were collected through semi-structured interviews, observation, and documentation, and analyzed using the interactive model of Miles, Huberman, and Saldana. The findings indicate that students experience various forms of cyber crime with differing levels of awareness and risk perception. Digital literacy functions as a protective mechanism in enhancing critical evaluation, information verification, and safe digital behavior. However, the preventive strategies adopted remain individual and are not yet institutionally integrated. The novelty of this study lies in its case study approach that empirically links students' lived experiences with digital literacy as a preventive strategy against cyber crime.

Keywords: *cyber crime*, digital literacy, preventive strategy, higher education, students



Copyright©2019

Riwayat Artikel

1. Diterima : 28 Januari 2026
2. Disetujui : 17 Maret 2026
3. Dipublikasikan : 28 Maret 2026

A. PENDAHULUAN

Transformasi digital dalam pendidikan tinggi meningkatkan intensitas penggunaan teknologi oleh mahasiswa, namun sekaligus memperbesar risiko kejahatan siber seperti penipuan daring, pencurian data, dan peretasan akun yang berdampak pada aspek finansial, psikologis, dan reputasi akademik (Teguh Yudi Cahyono, 2025). Dengan semakin tumbuhnya ketergantungan pada teknologi digital, mahasiswa sebagai pengguna aktif rentan terhadap berbagai bentuk kejahatan siber seperti penipuan daring, pencurian identitas, dan peretasan akun media sosial (Rini et al., 2023). Mahasiswa sebagai kelompok usia produktif dan pengguna aktif media digital sering kali menjadi target utama pelaku kejahatan siber karena tingginya intensitas interaksi digital yang mereka lakukan dalam kehidupan akademik maupun sosial. Kerentanan tersebut semakin diperkuat oleh masih rendahnya tingkat literasi keamanan digital di kalangan mahasiswa. Banyak di antara mereka yang memiliki pemahaman yang rendah tentang keamanan digital serta rentan terhadap risiko digitalisasi (Raissa Pramitha, 2021). Integrasi teknologi digital tersebut tidak hanya meningkatkan efisiensi dan fleksibilitas proses pembelajaran, tetapi juga mendorong terbentuknya pola interaksi akademik dan sosial yang semakin terbuka, cepat, dan tidak dibatasi oleh ruang dan waktu. Dalam konteks ini, mahasiswa dituntut untuk memiliki kemampuan adaptasi yang tinggi terhadap perkembangan teknologi digital sebagai bagian dari kompetensi akademik dan profesional di era masyarakat digital.

Selain itu, keterbatasan literasi informasi juga menyebabkan mahasiswa kerap mengalami kesulitan dalam membedakan informasi yang valid dan tidak valid, terutama di tengah banjir informasi digital yang beredar melalui media sosial dan platform daring. Penelitian menunjukkan bahwa mahasiswa kadang bingung membedakan informasi yang sah dan yang tidak, yang menjadi celah bagi pelaku kejahatan untuk melakukan modus penipuan (Ernest & M, 2023). Dampak kejahatan siber yang dialami mahasiswa tidak hanya terbatas pada kerugian finansial, tetapi juga meluas pada aspek psikologis dan reputasi akademik. Kerugian psikologis dapat muncul dalam bentuk kecemasan, rasa tidak aman, hingga menurunnya kepercayaan diri akibat penyalahgunaan data pribadi atau peretasan akun digital, sementara dampak terhadap reputasi akademik dapat terjadi ketika identitas atau akun mahasiswa disalahgunakan untuk tindakan yang merugikan secara akademik maupun sosial (Mariyani, 2023). Situasi ini memunculkan perlunya kesadaran yang lebih akan pentingnya keamanan data dan pengelolaan informasi di ruang digital.

Sejumlah riset menunjukkan bahwa perilaku mahasiswa dalam menggunakan teknologi digital masih cenderung berisiko, terutama dalam praktik berbagi informasi tanpa melalui proses verifikasi yang memadai. Riset juga menunjukkan bahwa kecenderungan untuk berbagi informasi tanpa verifikasi dapat meningkatkan risiko bagi mahasiswa (Adnjani, 2020). Menghadapi kompleksitas ancaman tersebut, literasi digital menjadi faktor kunci dalam upaya pemberdayaan mahasiswa agar mampu mengenali, memahami, dan mengelola risiko yang muncul di dunia maya.

Literasi digital tidak hanya mencakup penguasaan keterampilan teknis dalam penggunaan perangkat dan aplikasi digital, tetapi juga melibatkan kemampuan kognitif dan kritis dalam mengevaluasi informasi, kesadaran etis dalam berinteraksi di ruang digital, serta kompetensi sosial untuk membangun perilaku digital yang aman dan bertanggung jawab (Mustofa, 2023). Pengembangan strategi literasi digital yang komprehensif di lingkungan perguruan tinggi dipandang sebagai langkah strategis untuk menekan tingkat paparan mahasiswa terhadap kejahatan siber. Strategi ini tidak hanya berfokus pada aspek preventif, tetapi juga pada penguatan kapasitas mahasiswa dalam mengantisipasi dan merespons risiko digital secara mandiri. Penelitian menunjukkan bahwa pendekatan literasi digital yang terintegrasi dalam sistem pendidikan tinggi dapat memberikan kontribusi signifikan dalam membentuk perilaku digital yang lebih aman serta meningkatkan ketahanan mahasiswa terhadap berbagai bentuk kejahatan siber (Wutun et al., 2022).

Meskipun berbagai penelitian telah membahas pentingnya literasi digital dan meningkatnya ancaman kejahatan siber, sebagian besar kajian masih berfokus pada aspek konseptual, tingkat literasi digital secara umum, atau perilaku penggunaan media digital mahasiswa. Penelitian yang secara empiris mengaitkan literasi digital dengan pengalaman mahasiswa terhadap *cyber crime*, terutama di perguruan tinggi di Indonesia, masih relatif terbatas (Amna et al., 2024). Penelitian lebih lanjut diperlukan untuk mengeksplorasi hubungan ini dan merumuskan strategi yang lebih efektif dalam mengedukasi mahasiswa tentang keamanan digital sesuai dengan realitas dan tantangan yang mereka hadapi (Teguh Yudi Cahyono, 2025). Selain itu, belum banyak penelitian yang mengidentifikasi bagaimana literasi digital dapat berperan sebagai faktor protektif dalam meminimalisasi risiko kejahatan siber berdasarkan pengalaman nyata mahasiswa. Berdasarkan uraian tersebut, penelitian ini diarahkan untuk menjawab beberapa fokus utama, yaitu: (1) bagaimana bentuk-bentuk *cyber crime* yang dialami mahasiswa dalam aktivitas akademik dan sosial di ruang digital; (2) bagaimana strategi antisipasi yang dilakukan mahasiswa dalam menghadapi berbagai ancaman kejahatan siber; serta (3) bagaimana peran literasi digital dalam membentuk kemampuan mahasiswa untuk mencegah, mengenali, dan merespons risiko kejahatan siber secara efektif. Ketiga fokus ini diharapkan mampu memperjelas keterkaitan antara pengalaman empiris mahasiswa, tingkat literasi digital, dan upaya penguatan keamanan digital di lingkungan pendidikan tinggi.

B. KAJIAN TERDAHULU

Penelitian serupa sudah pernah dilakukan oleh Adila et al. (2019) yang membahas tentang fenomena berita palsu dan “misinformasi” menimbulkan ketakutan, kegelisahan, dan kesalahpahaman di masyarakat. Situasi ini semakin diperparah dengan maraknya ujaran kebencian di dunia digital. Studi tersebut menunjukkan kurangnya literasi media di kalangan masyarakat sehingga menyebabkan pemahaman yang dangkal terhadap informasi yang beredar

di media sosial. Penelitian ini menekankan pentingnya pengembangan model literasi media yang inovatif untuk mengidentifikasi pendekatan misinformasi di media sosial. Dengan mengembangkan model literasi media yang memberdayakan pengguna media sosial (netizen), diharapkan mampu menyaring informasi secara kritis dan menciptakan konten-konten positif dalam memanfaatkan media digital.

Kajian literasi digital juga banyak dikaitkan dengan pendidikan karakter dan pembentukan perilaku digital yang bertanggung jawab. Penelitian Benaziria (2018) yang menunjukkan bahwa penggunaan internet oleh anak dan remaja di Indonesia cenderung berisiko, karena kurangnya pengawasan orang tua dan minimnya kesadaran akan bahaya konten tidak pantas. Penelitian tersebut menegaskan bahwa pelajaran kewarganegaraan mempunyai peran strategis dalam mengembangkan karakter bangsa yang “melek” digital melalui pembelajaran keterampilan digital. Hasil penelitian ini menunjukkan bahwa model pembelajaran VCT efektif dalam mengembangkan keterampilan digital siswa sekaligus nilai moral dalam penggunaan teknologi.

Penelitian juga dilakukan oleh Ridwan et al. (2022), yakni untuk menganalisis tentang kepeahaman mahasiswa dalam memahami literasi digital, digital skill, dan digital safety. Penelitian ini dilakukan untuk melihat pemahaman mahasiswa itu sendiri dalam menggunakan perangkat digital dan untuk melihat pemahaman mahasiswa pada digital skill dan digital safety. Temuan dari penelitian ini bahwa mahasiswa UIN Ar-Raniry memiliki pemahaman baik dalam literasi dan keterampilan digital, tetapi masih perlu memperkuat aspek keamanan digital. Penelitian ini merekomendasikan peningkatan intervensi pengembangan kapabilitas digital safety pada mahasiswa.

Hal serupa juga ditemukan dalam penelitian Ramadhan & Nurnawati (2023) yang menunjukkan bahwa mahasiswa memiliki kesadaran terhadap bahaya *Cybercrime*. Penelitian ini menemukan pelajar Indonesia menjadi pengguna teknologi dan internet terbesar yang berisiko menjadi korban kejahatan dunia maya karena kurangnya pendidikan dan kesadaran tentang bahaya internet. Kejahatan dunia maya seperti pencurian identitas dan penipuan online merajalela, namun banyak pengguna yang masih membagikan informasi pribadi di media sosial dan menggunakan Wi-Fi gratis tanpa jaminan. Hasil ini menunjukkan perlunya dukungan dan pelatihan oleh lembaga, departemen, dan program untuk meningkatkan kesadaran dan kewaspadaan siswa dalam penggunaan teknologi digital.

Penelitian lain juga dilakukan oleh Elrayah, M., & Jamil (2023) bahwa pada penelitian ini menyelidiki dampak literasi digital, kewarganegaraan, praktik kurasi, keterhubungan, dan kekhawatiran privasi online terhadap perilaku keamanan siber. Dalam temuannya

mengungkapkan terdapat korelasi yang signifikan antara literasi digital (khususnya hak cipta, kewarganegaraan, kurasi, dan keterhubungan), masalah privasi daring, dan perilaku keamanan siber. Pemahaman tentang keamanan siber secara signifikan memengaruhi tingkat dan lintasan hubungan ini. Pemahaman yang lebih mendalam tentang keamanan siber meningkatkan efek positif literasi digital, termasuk kesadaran hak cipta, kewarganegaraan yang bertanggung jawab, kurasi konten, dan keterhubungan, pada perilaku keamanan siber.

Penelitian ini menempati posisi yang berbeda dan memperkuat celah penelitian (research gap) dengan mengintegrasikan ketiga aspek tersebut literasi digital, pengalaman cyber crime, dan strategi preventif melalui pendekatan kualitatif berbasis studi kasus. Kontribusi utama penelitian ini terletak pada penyajian pemahaman yang lebih kontekstual dan mendalam mengenai bagaimana literasi digital berfungsi sebagai mekanisme protektif yang terbentuk dari pengalaman nyata mahasiswa, sekaligus menawarkan perspektif integratif yang belum banyak dikaji dalam penelitian sebelumnya, khususnya dalam konteks perguruan tinggi di Indonesia. Penelitian ini memberikan kontribusi dengan memosisikan literasi digital sebagai strategi preventif dalam mengantisipasi cyber crime di kalangan mahasiswa, bukan sekadar sebagai kompetensi teknis penggunaan teknologi. Melalui pendekatan kualitatif, penelitian ini mengungkap pengalaman, persepsi risiko, dan strategi antisipasi mahasiswa secara kontekstual dalam budaya akademik perguruan tinggi.

Temuan penelitian ini memperkaya kajian literasi digital dan cyber crime dengan menawarkan kerangka pemahaman yang integratif, edukatif, dan berorientasi pada pencegahan. Penelitian ini berbeda dengan penelitian sebelumnya karena tidak hanya mengukur literasi digital, tetapi juga mengeksplorasi pengalaman mahasiswa dalam menghadapi cyber crime melalui pendekatan kualitatif. Penelitian ini memosisikan literasi digital sebagai strategi preventif yang mencakup aspek teknis, kritis, dan sosial dalam membangun keamanan digital mahasiswa. Dengan demikian, penelitian ini diharapkan dapat memperkaya kajian literasi digital dan cyber crime melalui perspektif yang lebih kontekstual dan preventif.

C. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan desain studi kasus untuk memahami secara mendalam fenomena *cyber crime* yang dialami mahasiswa serta strategi antisipasi yang mereka lakukan. Pendekatan kualitatif dipilih karena penelitian ini berfokus pada makna, pengalaman, persepsi, dan pola perilaku mahasiswa dalam menghadapi ancaman kejahatan siber, yang tidak dapat sepenuhnya dijelaskan melalui data kuantitatif. Penggunaan metode kualitatif memungkinkan peneliti untuk mengeksplorasi konteks sosial dan budaya di mana mahasiswa berada, sehingga memberikan gambaran yang lebih holistik tentang bagaimana mereka

mengidentifikasi dan merespons berbagai bentuk *cyber crime*. Studi kasus sebagai metode memberikan kedalaman pada wawasan yang diperoleh, memungkinkan peneliti untuk mengumpulkan data melalui wawancara mendalam, observasi, dan dokumentasi. Dalam mengumpulkan data lapangan, peneliti bergantung pada informan, karena memiliki peran yang sangat penting sebagai sumber dan pemegang informasi. Dalam penelitian ini terdapat lima mahasiswa dari UIN Sayyid Ali Rahmatullah Tulungagung yang menjadi informan. Pemilihan lima informan dilakukan secara *purposive sampling* berdasarkan kriteria mahasiswa yang aktif menggunakan teknologi digital dan memiliki pengalaman atau potensi terpapar *cyber crime*. Jumlah tersebut dinilai cukup karena penelitian kualitatif menekankan kedalaman data, serta telah mencapai kejenuhan data (*data saturation*) di mana informasi yang diperoleh mulai berulang dan tidak menghasilkan temuan baru.

Teknik pengumpulan data diperoleh melalui observasi dan wawancara semi terstruktur, dan dokumentasi. Pertama, Observasi (Observation) atau pengamatan dalam penelitian ini menggunakan pengamatan langsung terhadap objek yang menjadi fokus penelitian. Objek pada penelitian ini yakni Mahasiswa UIN Sayyid Ali Rahmatullah Tulungagung. Teknik ini diterapkan untuk memperoleh informasi yang lebih mendalam dan komprehensif terkait data penelitian. Dalam proses observasi, media yang digunakan meliputi perekam video, perekam suara, dan kamera untuk dokumentasi foto. Kedua, wawancara (Interview) merupakan kegiatan tanya jawab yang dilakukan peneliti untuk memperoleh informasi lengkap mengenai fokus penelitian bagi seorang informan. Wawancara dalam penelitian ini menggunakan wawancara semi-terstruktur. Ketiga, Dokumentasi merupakan teknik pengumpulan data yang objeknya berbentuk tulisan, gambar, maupun karya.

Teknik analisis data menggunakan model analisis interaktif, dimana proses pengumpulan, interpretasi dan penyimpulan data dilakukan secara berulang hingga hasil interpretasi bersifat informatif dan komprehensif. Miles et al. (2014), menyebutkan bahwa analisis data dapat dilakukan dengan tiga tahapan yaitu (1) *data reduction* (reduksi data), dilakukan dengan melakukan mengubah hasil wawancara/observasi menjadi teks untuk memahami konteks dan gambaran umum dengan memberikan kode pada bagian data yang relevan dengan fokus penelitian. Mengelompokkan kode yang memiliki kesamaan makna dan membuang data yang tidak relevan; (2) *data display* (penyajian data), melakukan proses mengorganisasikan dan menampilkan data yang telah direduksi ke dalam matriks atau tabel, diagram hubungan antar kategori, narasi deskriptif dan peta konsep atau tema penelitian; dan (3) *conclusion/verification* (penarikan kesimpulan), dilakukan dengan menarik kesimpulan dengan melakukan triangulasi sumber data, mengkonfirmasi ulang kepada informan, kemudian membandingkan dengan teori.

Triangulasi data dalam penelitian ini dilakukan untuk menjamin kredibilitas dan validitas temuan melalui triangulasi sumber, teknik, waktu, dan teori. Triangulasi sumber dilakukan dengan membandingkan data antar informan terkait pengalaman *cyber crime* dan strategi antisipasi yang

dilakukan. Triangulasi teknik dilakukan dengan mengonfirmasi kesesuaian data hasil wawancara, observasi, dan dokumentasi. Triangulasi waktu dilakukan melalui pengumpulan data pada waktu yang berbeda untuk memastikan konsistensi informasi, disertai klarifikasi ulang apabila ditemukan perbedaan. Selain itu, peneliti juga melakukan member check dengan mengonfirmasi hasil interpretasi kepada informan, serta triangulasi teori dengan membandingkan temuan penelitian dengan konsep dan hasil studi terdahulu yang relevan (Miles et al., 2014).

D. HASIL DAN PEMBAHASAN

Pengalaman Mahasiswa Menghadapi *Cyber Crime*

Berdasarkan hasil penelitian menunjukkan bahwa pengalaman mahasiswa dalam menghadapi cyber crime bersifat berulang dan beragam, baik dari sisi bentuk kejahatan maupun dampak yang ditimbulkan. Hal ini diungkapkan oleh informan 2 bahwa:

“Pernah menjadi korban penipuan melalui Instagram saat membeli produk dari akun penjual yang ternyata palsu. Pelaku meminta korban melanjutkan transaksi melalui WhatsApp hingga korban melakukan transfer pembayaran. Setelah itu, pelaku meminta denda tambahan dengan alasan pengiriman barang bermasalah dan mengancam akan melapor ke polisi. Korban kemudian melapor ke pihak keluarga dan kepolisian. Kasus tersebut menimbulkan kerugian sekitar Rp700.000–Rp800.000 serta meningkatkan kewaspadaan korban terhadap transaksi digital” (LS).

Hal ini diperkuat oleh pendapat informan 2 yang pernah mengalami tindakan kejahatan melalui beberapa jenis media yakni:

“Tindakan kejahatan yang dilakukan dengan menggunakan teknologi komunikasi, seperti komputer, gadget atau alat elektronik lainnya” (HA).

Temuan wawancara menunjukkan bahwa sebagian besar informan pernah menerima pesan atau informasi digital yang mencurigakan, terutama melalui aplikasi pesan instan dan media sosial. Bahkan beberapa pesan-pesan tersebut sering kali dikemas dalam konteks yang relevan dengan kehidupan akademik mahasiswa, seperti informasi beasiswa, kegiatan kampus, administrasi akademik, atau permintaan bantuan atas nama dosen dan institusi (Broadhurst et al., 2020).

Penelitian ini mengidentifikasi beberapa pola cyber crime yang dominan di kalangan mahasiswa dengan beberapa jenis penipuan yakni modus *phishing* menjadi bentuk kejahatan yang paling sering ditemui, baik melalui tautan palsu maupun permintaan data sensitif (Broadhurst et al., 2019). Hal ini diungkapkan oleh informan 1 bahwa:

“Sejauh ini berdasarkan pengalaman saya, cyber crime itu seperti kejahatan khususnya di media sosial. Seperti kemarin itu contohnya kasus penipuan yang bermula dari hack akun media sosial instagram yang berujung pada melakukan transaksi transfer” (NK)

Selain itu, modus impersonation juga banyak ditemukan, khususnya yang mengatasnamakan dosen, organisasi kemahasiswaan, atau pihak administrasi kampus, dengan

memanfaatkan relasi hierarkis yang ada (Bergh & Junger, 2018). Spamming dan penyebaran malware juga menjadi ancaman yang cukup sering dialami mahasiswa. Sesuai pendapat informan 3 bahwa:

“Sangat besar jika mahasiswa sering menghiraukan informasi-informasi melalui internet dan sering buka laman-laman tidak resmi. Bahkan bisa juga sering upload data pribadi melalui media sosial, sehingga bisa jadi sangat rentan mengalami penipuan dalam bentuk apapun” (HA).

Informan mengungkapkan bahwa pesan spam sering kali diabaikan, padahal berpotensi menjadi pintu masuk malware atau penipuan lanjutan. Temuan ini menunjukkan bahwa rendahnya sensitivitas terhadap risiko digital dapat memperbesar peluang terjadinya kejahatan siber (Bhandari, 2025).

Mahasiswa memiliki persepsi risiko yang berbeda-beda terhadap cyber crime. Hal ini diungkapkan oleh informan 2 bahwa:

“Antisipasi saya lakukan untuk melindungi dan menjaga akun digital saya itu dengan mengganti email ataupun mengganti password pada akun digital secara berkala” (LS)

Hal ini juga dipertegas dari jawaban informan 3 bahwa:

“Sangat penting, karena perlindungan data pribadi menjadi suatu kerahasiaan tersendiri yang harus dijaga. Sehingga perlunya keamanan akun atau data pribadi dengan sering melakukan penggantian password atau bisa memanfaatkan aplikasi get contact untuk mengantisipasi penipuan dengan nomor baru. Contoh chat nomor baru dan tidak dikenal mungkin bisa langsung di blokir. Sekarang saya kalau ada nomor baru yg tidak dikenal langsung saya senyapkan” (NA)

Sebagian informan menunjukkan kesadaran tinggi akan bahaya kejahatan siber, namun sebagian lainnya menganggap risiko tersebut sebagai hal yang wajar dan sulit dihindari (Sestani et al., 2022). Perbedaan persepsi ini berkaitan erat dengan tingkat literasi digital yang dimiliki mahasiswa. Mahasiswa dengan literasi digital yang lebih baik cenderung memiliki sikap waspada, melakukan verifikasi informasi, dan membatasi pembagian data pribadi, sebaliknya mahasiswa dengan literasi digital yang rendah lebih rentan menjadi korban karena kurang memahami pola kejahatan siber. Strategi antisipasi yang dilakukan mahasiswa masih bersifat individu dan tidak terstruktur. Beberapa mahasiswa mengembangkan strategi berdasarkan pengalaman pribadi, seperti mengabaikan pesan mencurigakan, memeriksa ulang identitas pengirim, atau berkonsultasi dengan teman (Bhandari, 2025). Namun, strategi ini belum didukung oleh pemahaman konseptual yang memadai mengenai keamanan siber. Temuan ini menunjukkan bahwa strategi antisipasi cyber crime memerlukan pendekatan yang lebih sistemik melalui pendidikan literasi digital yang terencana (Sestani et al., 2022).

Perguruan tinggi memiliki peran strategis dalam membentuk perilaku aman mahasiswa di ruang digital. Namun berdasarkan hasil wawancara terkait edukasi khusus terkait *cyber crime* dengan informan 1 menunjukkan bahwa:

“Untuk secara khusus belum ada. Namun kemungkinan ada beberapa mata kuliah yang topiknya sedikit menyinggung terkait cyber crime itu tadi” (NK)

Namun sebagian mahasiswa mengikuti pelatihan tentang keamanan digital melalui media sosial, hal ini diungkapkan oleh informan bahwa:

“Belum pernah kalau di kampus, pernahnya saat scroll tiktok tentang edukasi keamanan digital atau mengikuti akun media sosial. Salah satunya mengikuti konten kreator membahas edukasi keamanan data. Salah satunya mas hafiz dan mbak mahira. Sejak semester 2” (HA)

Berdasarkan hasil penelitian menunjukkan bahwa perguruan tinggi belum melakukan sosialisasi terkait keamanan digital. Hal ini sependapat bahwa belum semua institusi menyediakan panduan resmi terkait komunikasi digital dan keamanan siber, sehingga pembekalan mahasiswa mengenai pentingnya keamanan informasi masih minim (Arora & Dadhania, 2024).

Integrasi literasi digital dan keamanan siber ke dalam kurikulum, penyediaan kanal komunikasi resmi, serta sosialisasi berkala mengenai modus *cyber crime* menjadi langkah penting dalam upaya pencegahan kejahatan siber. Berdasarkan hasil wawancara dengan informan 3 bahwa:

“Peran kampus mungkin seharusnya sesekali atau bahkan dijadwalkan untuk membuat program pelatihan atau sosialisasi secara khusus mengenai bahayanya penggunaan teknologi digital yang tidak bijak dan pentingnya memahami isu terkait cyber crime” (NA)

Temuan penelitian ini menguatkan pandangan bahwa literasi digital merupakan faktor kunci dalam membentuk perilaku aman mahasiswa di ruang digital. Dalam perspektif teori literasi digital, lemahnya aspek kritis dan etis menjadi celah utama yang dimanfaatkan pelaku *cyber crime*. Oleh karena itu, strategi antisipasi *cyber crime* perlu dirancang secara komprehensif dengan mengintegrasikan literasi digital ke dalam proses pendidikan tinggi (Ignasia Helena Waleng Kumanireng, 2023). Penelitian ini menunjukkan bahwa mahasiswa merupakan kelompok yang rentan terhadap berbagai bentuk *cyber crime* akibat intensitas penggunaan teknologi digital yang tinggi dan belum meratanya pemahaman mengenai keamanan digital.

Jenis *cyber crime* yang paling banyak ditemui oleh mahasiswa meliputi *phishing*, *impersonation*, *spamming*, dan *malware*. Literasi digital terbukti memiliki peran strategis sebagai upaya preventif dalam mengantisipasi kejahatan siber. Oleh karena itu, penguatan

literasi digital yang komprehensif dan berkelanjutan perlu menjadi prioritas dalam kebijakan dan praktik pendidikan tinggi guna menciptakan lingkungan digital yang aman dan beretika bagi mahasiswa.

Temuan penelitian ini menunjukkan bahwa intensitas penggunaan teknologi digital yang tinggi menjadikan mahasiswa sebagai kelompok yang rentan terhadap cyber crime. Kondisi ini memperlihatkan bahwa transformasi digital dalam pendidikan tinggi tidak hanya menciptakan peluang pembelajaran yang lebih fleksibel, tetapi juga menghadirkan risiko keamanan digital yang signifikan. Hasil penelitian ini sejalan dengan temuan Sestani et al. (2022) yang menyatakan bahwa tingkat kesadaran risiko digital memengaruhi perilaku keamanan pengguna dalam menghadapi ancaman siber.

Penelitian ini menginterpretasikan bahwa kerentanan mahasiswa terhadap cyber crime tidak hanya disebabkan oleh keterbatasan keterampilan teknis, tetapi juga lemahnya kemampuan kritis dan etis dalam memverifikasi informasi digital. Temuan ini menguatkan perspektif literasi digital yang menekankan integrasi aspek teknis, kognitif, dan sosial dalam membangun perilaku digital yang aman (Ignasia Helena Waleng Kumanireng, 2023). Dalam konteks ini, literasi digital tidak hanya berfungsi sebagai kemampuan penggunaan teknologi, tetapi juga sebagai mekanisme protektif dalam menghadapi ancaman cyber crime.

Berdasarkan berbagai jenis kejahatan siber, mahasiswa menunjukkan kerentanan yang signifikan terhadap praktik-praktik ini. Hal ini disebabkan oleh beberapa faktor:

1. Penggunaan Internet yang Tinggi: Mahasiswa adalah pengguna aktif internet, mengakses informasi melalui media sosial, email, dan situs web, meningkatkan kemungkinan mereka terpapar oleh kejahatan siber.
2. Kurangnya Kesadaran akan Keamanan Digital: Banyak mahasiswa yang belum sepenuhnya memahami risiko terkait aktivitas online mereka. Ketidaktahuan ini menyebabkan mereka lebih mudah terjebak dalam modus kejahatan (Iloanya, 2024).
3. Perilaku Digital yang Tidak Stabil: Generasi muda cenderung lebih impulsif dalam berbagi informasi pribadi. Tindakan ini dapat mengakibatkan kebocoran data yang membahayakan mereka (Jefri Susanto Manik, 2022).
4. Lingkungan Akademik yang Rentan: Perguruan tinggi sering kali memiliki sistem keamanan yang mungkin tidak cukup untuk melindungi data mahasiswa dari ancaman *cyber* (Dwinugroho, 2024).

Untuk mengatasi masalah ini, sangat penting untuk meningkatkan literasi digital di kalangan mahasiswa. Pendidikan literasi digital harus mencakup pengetahuan tentang jenis-jenis *cyber crime*, cara melindungi diri dari risiko, dan strategi untuk memperkuat keamanan

secara keseluruhan dalam berinteraksi di dunia maya (Topik Hidayat, Jeffry A. Ch. Likadja, 2023). Perguruan tinggi dapat berperan aktif dengan memasukkan modul tentang keamanan siber dalam kurikulum atau melalui program-program sosialisasi yang rutin. Namun demikian, penelitian ini mengungkap bahwa strategi perlindungan yang dilakukan mahasiswa masih bersifat individual dan belum terintegrasi dalam sistem pendidikan tinggi. Selain itu, penelitian ini menegaskan bahwa perguruan tinggi memiliki peran strategis dalam membangun budaya keamanan digital melalui integrasi literasi digital dalam kurikulum, penyediaan pedoman komunikasi digital, serta pelaksanaan sosialisasi keamanan siber secara berkelanjutan. Temuan ini didukung oleh pernyataan Arora dan Dadhania (2024) bahwa institusi pendidikan tinggi tidak hanya berperan sebagai penyedia teknologi pembelajaran, tetapi juga sebagai agen pembentukan perilaku digital yang aman dan bertanggung jawab. Dengan demikian, literasi digital merupakan faktor kunci dalam strategi preventif *cyber crime* di lingkungan perguruan tinggi.

Hasil penelitian juga menunjukkan bahwa mahasiswa yang memiliki literasi digital lebih baik cenderung memiliki kesadaran risiko yang lebih tinggi serta mampu menerapkan strategi perlindungan data secara mandiri. Temuan ini sesuai dengan penelitian Broadhurst et al. (2019) yang menyatakan bahwa pemahaman terhadap pola kejahatan siber berkontribusi terhadap peningkatan perilaku keamanan digital pengguna. Penguatan literasi digital yang komprehensif dan berkelanjutan diperlukan untuk menciptakan ekosistem digital pendidikan tinggi yang aman, kritis, dan beretika.

E. KESIMPULAN

Penelitian ini menunjukkan bahwa mahasiswa merupakan kelompok yang rentan terhadap berbagai bentuk kejahatan siber akibat tingginya intensitas penggunaan teknologi digital serta belum meratanya pemahaman mengenai keamanan dan etika digital. Bentuk *cyber crime* yang paling sering dialami mahasiswa meliputi *phishing*, *impersonation*, *spamming*, dan *malware* yang berdampak pada kerugian finansial, psikologis serta reputasi akademik. Temuan penelitian ini menegaskan bahwa literasi digital memiliki peran strategis sebagai upaya preventif dalam mengantisipasi kejahatan siber di lingkungan perguruan tinggi. Mahasiswa dengan literasi digital yang lebih baik cenderung memiliki kemampuan untuk mengenali pola kejahatan siber, melakukan verifikasi informasi, serta mengelola dan melindungi data pribadi secara lebih aman. Secara kontribusi, penelitian ini memperkuat dan memperluas kajian literasi digital dengan memosisikannya secara empiris sebagai strategi preventif berbasis pengalaman mahasiswa, bukan sekadar kompetensi teknis. Selain itu, penelitian ini menawarkan perspektif kontekstual tentang

hubungan antara literasi digital, persepsi risiko, dan perilaku keamanan digital di lingkungan perguruan tinggi Indonesia.

Secara teoritis, penelitian ini memperluas kajian literasi digital dengan menempatkannya sebagai pendekatan preventif terhadap cyber crime berbasis pengalaman mahasiswa. Secara praktis, penelitian ini merekomendasikan integrasi literasi digital dan keamanan cyber crime secara eksplisit ke dalam kurikulum, penguatan kebijakan perlindungan data, serta pelaksanaan edukasi keamanan digital secara berkelanjutan di perguruan tinggi. Penelitian ini terbatas pada lingkup subjek tertentu, sehingga penelitian selanjutnya disarankan menggunakan pendekatan dan cakupan responden yang lebih luas. Di sisi lain, penelitian ini belum mengeksplorasi peran kebijakan institusi secara langsung melalui data dari pihak pengelola atau pembuat kebijakan kampus.

DAFTAR PUSTAKA

- Adila, I., Weda, W., & Tamitiadini, D. (2019). Pengembangan Model Literasi Dan Informasi Berbasis Pancasila Dalam Menangkal Hoaks. *WACANA, Jurnal Ilmiah Ilmu Komunikasi*, 18(1), 101–111. <https://doi.org/10.32509/wacana.v18i1.721>
- Adnjani, M. D. (2020). Strategi Sinergitas Wartawan Dan Akademisi Dalam Gerakan Sosial Literasi Digital Di Jawa Tengah. *SOSFILKOM*, XIV(01), 47–55. <https://doi.org/https://doi.org/10.32534/jsfk.v14i01.1527>
- Amna, F. A., Saibi, E. A., & Wahyuni, U. (2024). *Motivasi atas Sikap Mahasiswa Generasi Milenial terhadap Literasi Digital di Prodi Kemas STIKES Syedza Saintika*. 14(1), 242–249. <https://doi.org/10.33087/dikdaya.v14i1.629>
- Arora, M. S., & Dadhania, P. J. (2024). *Threats , Effects , and Awareness of Cybercrime : A Survey*. 1–10. <https://doi.org/10.55041/IJSREM32833>
- Benaziria, B. (2018). Pengembangan Literasi Digital pada Warga Negara Muda dalam Pembelajaran PPKn melalui Model VCT. *Jupiis: Jurnal Pendidikan Ilmu-Ilmu Sosial*, 10(1), 11. <https://doi.org/10.24114/jupiis.v10i1.8331>
- Bergh, C. M. M. R. Van Den, & Junger, M. (2018). Victims of cybercrime in Europe : a review of victim surveys. *Crime Science*. <https://doi.org/10.1186/s40163-018-0079-3>
- Bhandari, B. (2025). Cybersecurity Awareness amongst University Students: Legal Remedies and Policies to Mitigate Risks. *Unity Journal*, 6(1), 120–135. <https://doi.org/https://doi.org/10.3126/unityj.v6i1.75557>
- Broadhurst, R., Skinner, K., Sifniotis, N., & Matamoros-macias, B. (2020). Phishing Risks In A University Student Community. *Australian Institute of Criminology, February*(587), 1–16.
- Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-macias, B., & Ipsen, Y. (2019). Phishing and Cybercrime Risks in a University Student Community Phishing and Cybercrime Risks in a University Student Community. *International Journal of Cybersecurity Intelligence and Cybercrime*, 2(1), 4–23. <https://doi.org/https://www.doi.org/10.52306/02010219RZEX445>

- Dwinugroho, Y. B. (2024). Transformation Strategy: Indonesian National Police in Coordinating Crime in The Digital Era. *International Journal of Integrated Science and Technology (IJIST)*, 2(5), 374–383. <https://doi.org/https://doi.org/10.59890/ijist.v2i5.1904>
- Elrayah, M., & Jamil, S. (2023). Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour: The Moderating Role of Cybersecurity Awareness. *International Journal of Cyber Criminology*, 17(2), 166–187. <https://doi.org/https://doi.org/10.5281/zenodo.4766711>
- Ernest, I. Z., & M, M. D. P. (2023). The Use of Google Sites-based Electronic Modules in Science Learning Against Digital Literacy of Junior High School Students. *Jurnal Pendidikan Indonesia Volume*, 12(2), 293–304. <https://doi.org/https://doi.org/10.23887/jpiundiksha.v12i2.56311> The
- Ignasia Helena Waleng Kumanireng, R. B. U. (2023). Pengaruh Literasi Keuangan, Literasi Pajak Dan Literasi Digital Terhadap Minat Investasi Mahasiswa Universitas Mercu Buana Yogyakarta. *JAE: Jurnal Akuntansi Dan Ekonomi*, 8(3), 11–22. <https://doi.org/10.29407/jae.v8i3.20566>
- Iloanya, K. O. (2024). Effect of Cybercrime on the Academic Performance of Students of Tertiary Institutions in Enugu State, Nigeria Kenneth O. Iloanya. *Journal of Policy and Development Studies (JPDS)*, 15(1), 126–144. <https://doi.org/https://www.ajol.info/index.php/jpds/article/view/267154>
- Jefri Susanto Manik. (2022). Peran Guru dalam Menjaga E-Safety Peserta Didik di Era Teknologi Digital di Indonesia. *Edukatif: Jurnal Ilmu Pendidikan*, 4(4), 5098–5108. <https://doi.org/https://doi.org/10.31004/edukatif.v4i4.3085> Copyright
- Mariyani, T. (2023). Profil literasi digital mahasiswa di era digitalisasi. *Bhineka Tunggal Ika: Kajian Teori Dan Praktik Pendidikan PKN*, 10(1), 50–57. <https://doi.org/https://jbt.ejournal.unsri.ac.id/index.php/jbti/article/view/78/40>
- Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative data Analysis: A Methods Sourcebook* (3rd ed.). Sage Publications.
- Mustofa, F. I. (2023). Ekologi Literasi Kampus sebagai Pilar Menyongsong Merdeka Belajar – Kampus Merdeka. *Alinea: Jurnal Bahasa, Sastra, Dan Pengajaran*, 12(1), 40–52. <https://doi.org/https://jurnal.unsur.ac.id/ajbsi/article/view/2031>
- Raissa Pramitha, Y. D. A. (2021). Hubungan Kesejahteraan Psikologis dengan Kesepian pada Mahasiswa yang Merantau di Yogyakarta. In *Jurnal Sosial dan Teknologi (SOSTECH)* (Vol. 1, Issue 10). <https://doi.org/https://doi.org/10.59188/jurnalsostech.v1i10.211>
- Ramadhan, I. H., & Nurnawati, E. K. (2023). Analisis Kesadaran Mahasiswa Terhadap Bahaya Cybercrime Di Media Sosial. *JTKSI (Jurnal Teknologi Komputer Dan Sistem Informasi)*, 6(1), 38. <https://doi.org/10.56327/jtksi.v6i1.1342>
- Ridwan, Yusran, Y., & Maulidia, C. A. (2022). Analisis Pemahaman Literasi Digital Pada Mahasiswa Uin Arraniry Terhadap Digital Skill Dan Digital Safety. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, 6(2), 142. <https://doi.org/10.22373/cj.v6i2.15433>

- Rini, H. M., Nabhan, S., & Info, A. (2023). Exploring Critical Digital Literacy In A Higher Education EFL Classroom: Teachers' Views And Practices. *Journal of English Language Teaching*, 6(1), 216–228. <https://doi.org/https://doi.org/10.15294/elt.v12i3.69160>
- Sestani, R. A., Septiana, A. C., Puspita, X., Setiawan, P., & Muhid, A. (2022). *Edukasi Literasi Digital untuk Meningkatkan Self Regulated Learning pada Mahasiswa*. 6(2), 202–211. <https://doi.org/10.26623/philanthropy.v6i2.5299>
- Teguh Yudi Cahyono, U. M. (2025). The Role Of Academic Libraries In Improving Digital Literacy Postgraduate Students Of State University Of Malang. *Jurnal Perpustakaan Universitas Airlangga: Media Informasi Dan Komunikasi Kepustakawanan*, 15(1), 29–38. <https://doi.org/https://doi.org/10.20473/jpua.v15i1.2025.29-38>
- Topik Hidayat, Jeffry A. Ch. Likadja, P. E. D. (2023). Perlindungan Hukum Data Pribadi Konsumen Dalam Perdagangan Elektronik. *Journal of Comprehensive Science*, 2(5), 1087–1103. <https://doi.org/https://doi.org/10.59188/jcs.v2i5.323>
- Wutun, M., Daga, L. L., Swan, M. V. D. P., Meilawati, F. T., & Lada, H. L. L. (2022). Kampanye Literasi Media ‘ Diet Televisi ’ Bagi Mahasiswa Di Kota Kupang. *Meskipun Pentingnya Literasi Digital Telah Diakui, Masih Terdapat Kekurangan Dalam Penelitian Yang Secara Empiris Mengaitkan Literasi Digital Dengan Pengalaman Mahasiswa Terhadap Cyber Crime, Terutama Di Perguruan Tinggi Di Indonesia (Pramitha & Astuti, 2, 14(1), 28–35*. <https://doi.org/https://dikdaya.unbari.ac.id/index.php/dikdaya/article/view/629/604>