E-ISSN: 3064-5883

Peran Pemahaman Cyber Security untuk Keamanan Akun Media Sosial Instagram Mahasiswa

Adinda Nova Octavia[1], Achmad Fauzi[2], Gilang Aditya Kurniawan[3], Nazwa Febriyana Putri[4], Rama Dwi Alghifari[5], Rasim Rasim[6], Sumarno Manrejo[7], Yusrina Mutiara Adienda[8]
[1]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, adindanova003@gmail.com
[2]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id
[3]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, gilangadit1210@gmail.com
[4]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, wawariyana@gmail.com
[5]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, ramadwialghifari83@gmail.com
[6]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, rasim@dsn.ubharajaya.ac.id
[7]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, sumarno@dsn.ubharajaya.ac.id
[8]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, mutiaradinda2002@gmial.com

Corresponding Author: adindanova003@gmail.com[1]

Abstract**:** *The development of information technology has created new challenges in the form of cybercrime, which is increasing along with the use of social media such as Instagram. This study aims to explore the role of cybersecurity understanding in keeping social media accounts safe among university students. The method used is a literature review, focusing on relevant literature to understand the factors that influence cybersecurity awareness. The results showed that a low understanding of digital security measures, such as the use of strong passwords and two-factor authentication, increases vulnerability to cyberattacks. Therefore, education about online security practices is important to protect personal data and reduce the risk of cybercrime. This research is expected to provide new insights for individuals and educational institutions in designing more effective digital literacy program.*

Keyword: *Cyber Security, Social Media Security, Understanding Security*

Abstrak: *Perkembangan teknologi informasi telah menciptakan tantangan baru dalam bentuk kejahatan siber, yang semakin meningkat seiring dengan penggunaan media sosial seperti Instagram. Penelitian ini bertujuan untuk mengeksplorasi peran pemahaman cybersecurity dalam menjaga keamanan akun media sosial di kalangan mahasiswa. Metode yang digunakan adalah telaah pustaka, dengan fokus pada literatur yang relevan untuk memahami faktor-faktor yang mempengaruhi kesadaran keamanan siber. Hasil penelitian menunjukkan bahwa rendahnya pemahaman tentang langkah-langkah keamanan digital, seperti penggunaan kata sandi yang kuat dan autentikasi dua faktor, meningkatkan kerentanan terhadap serangan siber. Oleh karena itu, edukasi tentang praktik keamanan online menjadi penting untuk melindungi data pribadi dan mengurangi risiko kejahatan siber. Penelitian ini diharapkan dapat memberikan wawasan baru bagi individu dan institusi pendidikan dalam merancang program literasi digital yang lebih efektif.*

Kata Kunci: *Cybersecurity*, Keamanan Media Sosial, Pemahaman *Cybersecurity*

PENDAHULUAN

Perkembangan teknologi dan informasi telah memunculkan ancaman baru di dunia maya, yaitu kejahatan siber. Kejahatan ini muncul sebagai dampak negatif dari kemajuan berbagai aplikasi yang terhubung melalui internet (Rahmawati, 2017). Internet merupakan fenomena yang terus berkembang, yang selalu mengutamakan perlindungan data pribadi maupun data perusahaan (Silalahi, 2022). Di era digital, keamanan siber telah menjadi salah satu tantangan utama yang dihadapi oleh individu dan organisasi. Media sosial seperti Instagram telah menjadi target utama serangan siber karena sifatnya yang sangat terbuka dan penggunaannya yang luas (Arsini et al., 2023). Media sosial merupakan platform berbasis internet yang memungkinkan individu maupun kelompok untuk berinteraksi, berbagi konten, serta berkomunikasi dengan pengguna lainnya. Platform ini menyediakan sarana bagi pengguna untuk membuat, mendistribusikan, dan bertukar informasi, gagasan, pesan, serta berbagai media seperti teks, gambar, video, dan audio secara daring (Puteri et al., 2023). Platform ini juga menyediakan berbagai kemudahan untuk berhubungan, berbagi informasi, dan mengekspresikan diri, sehingga menjadi bagian yang tak terpisahkan dari kehidupan sehari-hari (Naomira et al., 2024). Berdasarkan data yang dirilis oleh berbagai lembaga keamanan siber, jumlah kasus peretasan akun media sosial terus meningkat setiap tahunnya. Salah satu penyebab utama dari meningkatnya ancaman ini adalah rendahnya tingkat kesadaran pengguna terhadap pentingnya menjaga keamanan data pribadi mereka (Arham & Risal, 2023).

Aktivitas penggunaan teknologi digital di Indonesia berpotensi menjadi bagian dari dinamika perang siber (Soesanto et al., 2023). Selama bertahun-tahun, ancaman siber terus berkembang, baik dari segi jumlah maupun tingkat kecanggihannya (Santoso, 2023). Indonesia adalah salah satu dari lima negara teratas di dunia dalam hal penggunaan media sosial, dan memiliki potensi keuntungan dan kerugian dalam hal risiko perang siber. Platform media sosial adalah sumber informasi, alat komunikasi, dan alat pembelajaran digital bagi masyarakat umum, tetapi juga merupakan tantangan bagi kedaulatan negara.. Namun, peluang perang siber tercipta dari penggunaan teknologi digital di Indonesia, karena peretas atau cracker dari negara lain dapat dengan cepat mengakses jaringan informasi, penggunaan teknologi digital di Indonesia membuka peluang terjadinya perang siber., yang meningkatkan risiko kerentanan, terutama dalam penyampaian informasi intelijen melalui dunia maya (Putri et al., 2023).

Perkembangan ilmu keamanan informasi di dunia era modern 5.0 menghadirkan risiko di dunia siber, yang mencakup ancaman terhadap kerahasiaan dan integritas, baik bagi organisasi maupun individu. Kejahatan tidak lagi terbatas pada tindakan langsung seperti perampokan atau pencurian, melainkan telah berkembang ke ranah maya yang dikenal sebagai kejahatan siber. Jenis kejahatan ini, yang tergolong baru, dilakukan oleh individu dengan keahlian di bidang komputer dan teknologi informasi (Rahayu et al., 2021). Komputer, yang awalnya berfungsi sebagai alat untuk membantu pengumpulan, penyimpanan informasi, serta pekerjaan, tetapi dapat disalahgunakan oleh pihak yang tidak bertanggung jawab untuk melakukan tindak kejahatan (Septasari, 2023). *Cybercrime* merupakan tindakan kriminal yang dilakukan dengan memanfaatkan teknologi komputer sebagai sarana utama untuk melakukan kejahatan, terutama yang berkaitan dengan perkembangan teknologi komputer, khususnya internet (Fadillah et al., 2021).

Mahasiswa, sebagai salah satu kelompok pengguna aktif media sosial, sering kali menjadi sasaran empuk serangan siber (Badrumilah & Rigianti, 2022). Mereka cenderung memiliki aktivitas online yang tinggi, namun tidak diimbangi dengan pemahaman yang memadai tentang langkah-langkah keamanan. Kurangnya pemahaman tentang risiko keamanan digital dapat mendorong perilaku berisiko, seperti membagikan informasi pribadi dengan tidak hati-hati, mengunduh konten berbahaya, dan terlibat dalam aktivitas daring yang dapat menimbulkan kerugian (Sussolaikah et al., 2023). Sebagian besar pengguna media sosial tidak menyadari bahwa kejahatan siber seperti perundungan daring, pengintaian siber, phishing, dan penipuan online dapat berawal dari aktivitas di media sosial (Saizan & Singh, 2018). Faktor-faktor seperti penggunaan kata sandi yang lemah, kurangnya penggunaan autentikasi dua faktor, serta ketidaktahuan dalam mengenali email atau tautan phishing membuat mereka

rentan terhadap serangan. Hal ini diperparah dengan kebiasaan berbagi informasi pribadi secara publik di media sosial tanpa mempertimbangkan risiko yang mungkin timbul. Perlu dipahami bahwa korban peretasan media sosial bukanlah penyebab utama dari peretasan tersebut. Mereka sering menjadi target karena lemahnya sistem keamanan akun atau karena kelalaian dalam menjaga privasi di dunia maya. Oleh sebab itu, edukasi tentang praktik keamanan online serta perlindungan data pribadi menjadi hal yang krusial untuk menekan risiko terjadinya peretasan (Puteri et al., 2023). Langkah tersebut bertujuan melindungi data pribadi guna mengurangi risiko terjadinya kejahatan pelecehan seksual di media sosial (Fikriya et al., 2023).

Literasi digital yang berkaitan dengan cybersecurity di kalangan mahasiswa masih menjadi isu yang memerlukan perhatian. Penelitian-penelitian terdahulu menunjukkan bahwa banyak mahasiswa yang belum memahami konsep dasar keamanan siber, seperti enkripsi data, pengelolaan privasi, serta bagaimana mengenali dan menghindari ancaman siber. Padahal, pemahaman yang baik mengenai keamanan siber dapat membantu mereka melindungi akun media sosial dan data pribadi dari ancaman eksternal. Keamanan siber (cybersecurity) adalah serangkaian kebijakan keamanan yang dirancang untuk melindungi lingkungan dunia maya, organisasi, dan aset penggunanya (Riadi et al., 2023). Keamanan siber (cybersecurity) adalah serangkaian kegiatan dan langkah-langkah yang dilakukan melalui elemen-elemen dunia maya (perangkat keras, perangkat lunak, jaringan komputer) untuk melindungi dari serangan, gangguan, atau ancaman lainnya. Sebagai suatu bidang praktik, tujuan keamanan siber adalah untuk melindungi komputer, jaringan, aplikasi perangkat lunak, sistem kritis, dan data dari potensi ancaman digital (Azzahrah et al., 2024). Struktur manajemen keamanan yang luwes dan mudah beradaptasi memiliki kelebihan dalam menyesuaikan pendekatan pencegahan keamanan siber dengan ancaman yang terus berkembang, sehingga meningkatkan kemampuan respons terhadap serangan siber (Tamima et al., 2024).

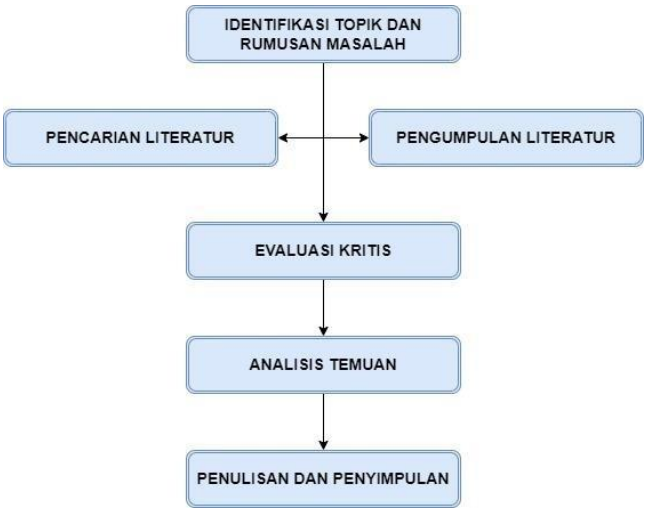
Penelitian ini dilakukan dengan metode kualitatif melalui telaah pustaka dan jurnal untuk memberikan gambaran yang lebih mendalam tentang bagaimana pemahaman terhadap cybersecurity dapat berkontribusi pada keamanan akun media sosial Instagram mahasiswa. Melalui kajian ini, akan dianalisis berbagai faktor yang memengaruhi kesadaran dan perilaku keamanan siber di kalangan mahasiswa, serta strategi yang efektif untuk meningkatkan literasi keamanan. Penelitian ini tidak hanya penting bagi individu, tetapi juga bagi komunitas akademik dan masyarakat luas. Dengan meningkatnya kesadaran akan pentingnya keamanan siber, diharapkan mahasiswa dapat menjadi lebih waspada dan proaktif dalam melindungi data pribadi mereka di dunia digital. Selain itu, hasil penelitian ini juga dapat menjadi acuan bagi institusi pendidikan dan pembuat kebijakan untuk merancang kurikulum atau program literasi digital yang lebih efektif (Muarif et al., 2019).

Oleh karena itu, penelitian ini bertujuan mengkaji peran pemahaman cybersecurity dalam menjaga keamanan akun Instagram mahasiswa serta faktor- faktor yang memengaruhi kesadaran mereka terhadap ancaman siber.

1. Bagaimana ancaman kejahatan siber seperti apa yang dapat menyebabkan konflik siber, seperti peretasan, peretasan, sabotase siber, dan perangkat mata-mata?
2. Apa saja manfaat yang dapat diperoleh dari penggunaan media sosial secara bijak?
3. Strategi apa saja yang dapat dilakukan untuk membangun kesadaran masyarakat mengenai keamanan siber?

METODE

Penelitian ini menggunakan metode telaah pustaka untuk menganalisis peran pemahaman *cybersecurity* dalam menjaga keamanan akun media sosial mahasiswa (Lumanau et al., 2024). Proses dimulai dengan mengidentifikasi topik dan merumuskan masalah penelitian, diikuti oleh pengumpulan literatur yang relevan dari berbagai sumber terpercaya. Literatur yang diperoleh dievaluasi secara kritis untuk menilai kualitas dan relevansinya. Hasil analisis kemudian disintesis guna menemukan pola atau celah penelitian yang signifikan. Akhirnya, temuan tersebut dirangkum dalam kerangka teoretis yang menjelaskan hubungan antara pemahaman *cybersecurity* dan keamanan akun media sosial, diakhiri dengan kesimpulan yang memberikan wawasan baru dalam bidang ini. Berikut adalah gambar diagramnya.



Gambar 1. Diagram langkah-langkah pelaksanaan penelitian

Metode penelitian ini mengumpulkan dan menganalisis informasi dari berbagai sumber tertulis untuk memahami topik penelitian secara mendalam.

HASIL DAN PEMBAHASAN

Hasil

Potensi Ancaman Kejahatan Siber

Ancaman dari kejahatan siber memiliki kemungkinan untuk memicu konflik siber. Berikut adalah beberapa potensi ancaman kejahatan siber yang perlu diperhatikan (Putri et al., 2023):

1. Peretasan

   Peretasan adalah salah satu elemen yang berkontribusi pada serangan siber, yang dapat disebabkan oleh apa pun, mulai dari penolakan pemerintah hingga upaya yang tidak disengaja untuk menguji keamanan. Selama pemilihan presiden 2014, misalnya, dilaporkan bahwa peretas telah membobol situs web KPU. Menurut referensi, ada masalah dengan akses yang menyebabkan situs web KPU tidak tersedia untuk sementara waktu.

2. *Cracking*

   Peretasan sering dilakukan di Indonesia oleh pihak-pihak yang dikenal sebagai "carder." Mereka menggunakan metode ini untuk mencuri informasi kartu kredit dengan cara mengakses data pelanggan. Setelah mendapatkan informasi tersebut, para peretas berusaha untuk mengakses data sensitif dan simpanan nasabah di bank demi kepentingan kriminal yang sangat merugikan bagi kedua belah pihak yaitu pihak bank dan nasabah.

3. Sabotase Dunia Maya

   Tindakan yang disengaja untuk mengganggu, merusak, atau menghancurkan jaringan komputer atau sistem informasi yang terhubung ke Internet dikenal sebagai sabotase siber. Bagi banyak bisnis besar di seluruh dunia, perilaku ini telah menjadi salah satu mimpi terburuk mereka.

4. Perangkat Mata-Mata

   Perangkat mata-mata merujuk pada program perangkat lunak yang secara diam- diam mencatat aktivitas jaringan, termasuk cookie dan informasi pendaftaran. Setelah dikumpulkan, data tersebut dapat dijual atau diberikan kepada bisnis atau orang tertentu, yang mungkin menggunakannya untuk mendistribusikan virus berbahaya atau menampilkan iklan yang tidak diinginkan. Sayangnya, Indonesia menemukan 24 wabah malware yang terkait dengan internet banking.

Peran *Cybersecurity* Terhadap Keamanan Media Sosial Instagram

A. Dimensi Peran *Cybersecurity*

Berdasarkan teori peran, dimensi peran dapat mencakup peran sebagai kebijakan, alat, penyelesaian sengketa, atau peran sebagai terapi kejut (Siagian et al., 2018).

1. *Cybersecurity* sebagai Kebijakan

Dalam menangani konten negatif di dunia maya di Indonesia, pemerintah melalui Direktorat Jenderal Aptika Kominfo RI menerapkan kebijakan yang mencakup penanganan dari hulu hingga hilir.

2. *Cybersecurity* sebagai Instrumen atau Alat

Cybersecurity berfungsi sebagai alat untuk mengatasi serangan siber dengan memanfaatkan teknologi aplikasi Nawala dan sistem *crawling*.

3. *Cybersecurity* sebagai Terapi Kejut

Tindakan pemblokiran dan filtrasi konten memberikan efek terapi kejut yang signifikan.

4. *Cybersecurity* sebagai Penyelesaian Sengketa

Cybersecurity juga berperan dalam menyelesaikan sengketa yang muncul akibat masalah di dunia maya.

Dengan pendekatan ini, peran *cybersecurity* dapat membantu mengatasi berbagai tantangan yang dihadapi dalam menjaga keamanan siber di Indonesia.

B. Peningkatan Keamanan Data Pribadi

Kebocoran data adalah risiko yang terkait dengan keamanan dan data pribadi. Penggunaan komunikasi digital tidak dapat dipisahkan dari penggunaan big data, karena dunia saat ini sangat bergantung pada data, yang menjadi dasar dari segala hal. Setiap hari, sejumlah besar data dikumpulkan dan dihasilkan, memberikan berbagai peluang analitis bagi organisasi untuk menemukan informasi yang berguna bagi operasional mereka. Keamanan digital merupakan hal yang sangat penting untuk dipertimbangkan sebelum mulai membagikan data di lingkup internet (M et al., 2023). Meskipun internet tidak selalu berbahaya, menggunakannya dengan bijak akan memberikan manfaat, seperti:

1. Menjaga Kerahasiaan Privasi

Kerahasiaan informasi pribadi, seperti email, kata sandi, nama ibu, dan nomor identitas, dapat dijaga dengan menjaga keamanan digital. Hanya pemilik data atau pihak tertentu, seperti lembaga pemerintah atau lembaga pendidikan, yang boleh mengakses informasi sensitif.

2. Menghindari Ancaman Kejahatan Siber

Terdapat banyak jenis kejahatan siber, dan pencurian serta penyalahgunaan data adalah beberapa di antaranya. Dengan memahami pentingnya menjaga keamanan digital, ancaman tersebut dapat dihindari, sehingga dapat berselancar di dunia maya dengan lebih aman.

3. Membangun Kebudayaan *Cybersecurity*

Strategi untuk membangun pertahanan digital dalam keamanan siber sangat penting, mengingat ancaman kejahatan siber yang semakin serius dan kompleks (Yudhanto, 2024). Berbagai serangan dunia maya, termasuk pencurian identitas, peretasan, kegagalan sistem komputer, dan pelanggaran keamanan jaringan, dapat membahayakan. Orang-orang dapat lebih memahami dan membantu mengatasi masalah ini dengan mengembangkan pertahanan digital dalam keamanan siber.

Untuk meningkatkan kesadaran akan etika keamanan siber, ada beberapa taktik yang bisa digunakan. Berikut ini adalah beberapa pendekatan yang dapat digunakan (Gunawan et al., 2024).

a. Pendidikan dan *Awareness*

Mendidik dan mengedukasi masyarakat tentang etika digital dan keamanan siber. Membantu masyarakat memahami nilai keamanan siber dan cara menangani serangan adalah tujuannya.

b. Gamifikasi

Mengimplementasikan gamifikasi untuk mendorong masyarakat agar lebih sadar akan masalah keamanan siber.

c. Pengembangan *Chatbot*
Menciptakan *chatbot* untuk menjadi sumber daya tunggal bagi pengguna online yang mencari informasi tentang teknologi, keamanan siber, dan internet.

d. Pelatihan Sumber Daya Manusia
Menawarkan kursus pelatihan keamanan siber kepada para profesional SDM di industri keamanan siber.

e. Pengembangan Kode Etik
Membuat dan menerapkan kode etik yang relevan untuk institusi, bisnis, dan komunitas dalam konteks keamanan siber.

Dengan menerapkan strategi-strategi ini, diharapkan etika dan kesadaran keamanan siber akan meningkat secara dramatis, risiko kejahatan siber akan menurun, dan masyarakat yang lebih mampu dan tangguh akan tercipta untuk menghadapi isu-isu digital yang semakin kompleks.

Menurut Rahmawati (2017) (dalam Azzahrah et al., 2024) ancaman kejahatan siber dapat ditangani melalui empat tahapan dalam manajemen risiko yang dapat diterapkan. Tahapan tersebut adalah sebagai berikut:

1) Identifikasi
Proses identifikasi risiko kejahatan siber harus dilakukan secara rutin. Tujuannya adalah untuk menemukan penyebab terjadinya kejahatan. Dalam tahap ini, semua aspek yang berpotensi menyebabkan kerugian perlu diperiksa dengan cermat. Setelah itu, semua risiko yang telah diidentifikasi akan diukur berdasarkan probabilitas dan dampaknya.

2) Penilaian
Tujuan dari penilaian risiko adalah untuk mengevaluasi tingkat risiko yang terkait dengan kejahatan siber. Ancaman ini dapat muncul dari berbagai aspek kehidupan, termasuk pertahanan negara. Penilaian risiko tidak dapat dilakukan secara langsung; untuk mengukurnya, digunakan tabel matriks yang memberikan gambaran mengenai tingkat probabilitas dan dampak setelah identifikasi.

3) Penanganan
Penanganan dilakukan dengan cara menghentikan secara paksa tindakan dan respons yang terkait dengan risiko kejahatan siber. Risiko yang telah ditetapkan kemudian dapat diterima, dialihkan, diminimalkan, atau dihindari. Dalam kasus pencurian informasi atau data, baik secara individu maupun lembaga, langkah ini sangat penting untuk meminimalkan risiko.

4) Pengendalian
Pada tahap ini, pengendalian melibatkan pemantauan dan penyesuaian yang penting untuk menilai seberapa baik keberhasilan manajemen risiko bekerja. Mereka yang bertanggung jawab atas keamanan, seperti Kementerian Pertahanan Indonesia, harus memiliki sistem peringatan dini agar solusi dapat menghentikan ancaman kejahatan siber.

Ancaman kejahatan siber dapat dikelola melalui empat tahapan manajemen risiko: identifikasi, penilaian, penanganan, dan pengendalian. Proses ini melibatkan identifikasi risiko secara berkala, evaluasi tingkat risiko, penanganan untuk mengurangi atau menghindari risiko, serta pemantauan untuk memastikan efektivitas langkah- langkah yang diambil. Dengan pendekatan sistematis ini, organisasi dapat lebih baik dalam mencegah dan mengatasi ancaman kejahatan siber.

Tabel 1. Penelitian terdahulu

No	Judul dan Penulis	Persamaan	Perbedaan
1	Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia (Najwa, 2024).	Membahas upaya meningkatkan keamanan siber terhadap ancaman digital	Tidak menitikberatkan kepada penegakan hukum siber di Indonesia
2	Peningkatan Keterampilan	Keduanya berfokus pada	Tidak berfokus pada mahasiswa dan

	Keamanan Siber bagi Pengelola Situs Desa Baros	peningkatan keamanan siber.	media sosial, tetapi berfokus pada pengelola situs desa.
3	Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) (Aji, 2022).	Sama-sama membahas keamanan siber dan perlindungan data pribadi.	Tidak fokus kepada mahasiswa dan media sosial, melainkan kepada kedaulatan data dan ekonomi politik
4	Analisis Pentingnya Edukasi Keamanan Siber bagi Pengguna Mahasiswa (Azizi et al., 2024).	Sama-sama membahas pentingnya edukasi atau pemahaman keamanan siber bagi mahasiswa.	Fokus pertama pada keamanan akun media sosial Instagram, sedangkan yang kedua lebih umum pada edukasi keamanan siber.
5	Peran Keamanan Siber dalam Mengatasi Konten Negatif Guna Mewujudkan Ketahanan Informasi Nasional (Siagian et al., 2018).	Sama-sama membahas peran keamanan siber dalam melindungi dari ancaman digital.	Fokus pertama pada mahasiswa dan media sosial, sementara yang kedua pada konten negatif dan ketahanan informasi nasional.
6	Mitigasi Ancaman Resiko Keamanan Siber Di Masa Pandemi Covid-19 (Herdiana et al., 2021).	Membahas keamanan siber dan perlindungan dari ancaman digital	Tidak membahas pada mitigasi risiko keamanan siber selama pandemi COVID-19.
7	Tantangan Pertahanan dan Keamanan Data Cyber dalam Era Digital : Studi Kasus dan Implementasi (Azzahrah et al., 2024).	Saling membahas keamanan siber dan perlindungan data.	Tidak membahas tantangan dan implementasi pertahanan data siber di era digital.
8	Modal Sosial Masyarakat Digital dalam Diskursus Keamanan Siber (Rachman & Susan, 2021).	Sama-sama membahas peran keamanan siber.	Fokus pertama pada mahasiswa dan media sosial, sementara yang kedua pada konten negatif dan ketahanan informasi nasional.
9	Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di	Keduanya membahas keamanan siber dan perlindungan terhadap ancaman digital.	Tidak membahas tata kelola dan diplomasi siber Indonesia dalam konteks kelembagaan.
10	Inisiatif Siber dalam Konteks Keamanan Siber di Filiphina (Simbolon, 2017).	Keduanya membahas keamanan siber.	Tidak berfokus pada tata kelola dan diplomasi siber Indonesia.
11	Pelatihan Media Edukasi Kesadaran keamanan Siber di SDN 01 Pandean kota Madiun (Sussolaikah et al., 2023).	Keduanya membahas keamanan siber dan perlindungan terhadap ancaman digital.	Tidak membahas tata kelola dan diplomasi siber Indonesia.
12	Peran dan Tantangan Cyber Security di Era Society 5.0 (M. F. Saputra & Wibawa, 2022).	Keduanya membahas peran keamanan siber dalam menghadapi ancaman digital.	Tidak membahas peran dan tantangan keamanan siber dalam konteks era Society 5.0.
13	Membangun Benteng Digital Untuk Memperkuat Etika Cyber Security Melawan Ancaman Cyber Crime (Gunawan et al., 2024).	Keduanya membahas keamanan siber dalam melindungi dari ancaman digital.	Tidak membahas secara mendalam tentang upaya membangun etika dan pertahanan digital untuk melawan ancaman cybercrime.
14	Strategi Indonesia Membentuk Cyber Security dalam Menghadapi Ancaman Cyber Crime melalui Badan Siber dan Sandi Negara (Ginanjar, 2022).	Keduanya membahas keamanan siber dan perlindungan terhadap ancaman cybercrime.	Tidak membahas strategi Indonesia dalam membentuk sistem keamanan siber untuk menghadapi ancaman cybercrime melalui Badan Siber dan Sandi Negara.
15	Perlindungan Data Pribadi Bagi Pengguna Media	Keduanya membahas perlindungan data pribadi dalam	Tidak membahas lebih umum membahas perlindungan data

	Sosial (Arham & Risal, 2023).	konteks keamanan siber.	pribadi bagi pengguna media sosial secara luas.
16	Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di *Platform* Sosial (Ardy et al., 2024).	Keduanya membahas ancaman di dunia maya, khususnya terkait keamanan siber pada media sosial	Tidak berfokus pada identifikasi dan pencegahan ancaman phishing di platform sosial.
17	Upaya Membangun Kesadaran Keamanan Siber pada Konsumen *E-commerce* di Indonesia (Rohmah, 2022).	Keduanya membahas upaya meningkatkan kesadaran keamanan siber.	Tidak berfokus pada kesadaran keamanan siber bagi konsumen *e-commerce* di Indonesia.
18	Penerapan Manajemen *Security* Terhadap *Cyber Crime* di Kominfo (F. Saputra et al., 2024).	Keduanya membahas keamanan siber dan perlindungan terhadap ancaman *cybercrime*.	Tidak membahas penerapan manajemen keamanan untuk menangani *cybercrime* di Kementerian Komunikasi dan Informatika (Kominfo).
19	Analisis Bibliometrik Perkembangan Strategi Komunikasi di Media Sosial pada Instansi Pemerintahan dalam Keamanan Siber (Hakiki et al., 2024).	Keduanya membahas aspek keamanan siber dalam konteks media sosial.	Tidak membahas taktik komunikasi di media sosial terkait keamanan siber pada instansi pemerintahan.
20	Peran *Cyber Security* Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus : *Hacker* Bjorka) (Indah et al., 2022).	Kedua penelitian ini membahas peran keamanan siber dalam melindungi data dan akun dari ancaman digital.	Tidak membahas peran keamanan siber dalam melindungi data penduduk Indonesia dari ancaman seperti peretasan (*hacker*).

Berdasarkan tabel *literature review*, dapat disimpulkan bahwa semua penelitian membahas berbagai aspek keamanan siber dan perlindungan data pribadi, dengan fokus yang berbeda- beda sesuai konteksnya. Beberapa penelitian menyoroti pentingnya edukasi atau pemahaman keamanan siber, seperti di kalangan mahasiswa atau masyarakat digital, sementara yang lain lebih menekankan pada aspek kebijakan, tata kelola, dan strategi dalam menghadapi ancaman digital, baik di Indonesia maupun secara global. Perbedaan utama terletak pada fokus spesifik, misalnya perlindungan data pribadi, mitigasi ancaman, atau penerapan kebijakan dan strategi keamanan siber di berbagai sektor, seperti pemerintahan, *e-commerce*, dan media sosial. Beberapa studi juga lebih terfokus pada analisis kasus spesifik, seperti ancaman dari *hacker* atau tantangan dalam era digital dan *Society* 5.0.

KESIMPULAN

Keamanan siber memainkan peran yang sangat penting dalam melindungi data pribadi dan menjaga integritas sistem media sosial seperti Instagram. Ancaman kejahatan siber, seperti peretasan, cracking, sabotase dunia maya, dan penggunaan perangkat mata-mata, terus berkembang dan memerlukan perhatian serius. Upaya untuk mengelola ancaman ini melalui kebijakan, alat, terapi kejut, dan penyelesaian sengketa yang berbasis pada *cybersecurity* sangat penting. Peningkatan kesadaran masyarakat mengenai pentingnya menjaga privasi dan keamanan data pribadi, serta pembangunan kebudayaan *cybersecurity*, akan mengurangi risiko terhadap kejahatan siber dan menciptakan lingkungan digital yang lebih aman.

Untuk menghadapi ancaman kejahatan siber yang semakin kompleks, disarankan agar masyarakat terus meningkatkan literasi digital mereka dengan mengikuti program pelatihan keamanan siber dan menggunakan alat keamanan yang tersedia. Selain itu, pengembangan kebijakan yang lebih komprehensif dan penerapan teknologi canggih untuk mendeteksi ancaman siber perlu diperkuat. Pemerintah dan lembaga terkait harus melibatkan lebih banyak pihak dalam menyebarkan informasi tentang pentingnya menjaga data pribadi dan memperkenalkan langkah-langkah preventif dalam menghadapi potensi ancaman siber di dunia

maya.

Keamanan siber memainkan peran yang sangat penting dalam melindungi data pribadi dan menjaga integritas sistem media sosial seperti Instagram. Ancaman kejahatan siber, seperti peretasan, cracking, sabotase dunia maya, dan penggunaan perangkat mata-mata, terus berkembang dan memerlukan perhatian serius. Upaya untuk mengelola ancaman ini melalui kebijakan, alat, terapi kejut, dan penyelesaian sengketa yang berbasis pada *cybersecurity* sangat penting. Peningkatan kesadaran masyarakat mengenai pentingnya menjaga privasi dan keamanan data pribadi, serta pembangunan kebudayaan *cybersecurity*, akan mengurangi risiko terhadap kejahatan siber dan menciptakan lingkungan digital yang lebih aman. Untuk menghadapi ancaman kejahatan siber yang semakin kompleks, disarankan agar masyarakat terus meningkatkan literasi digital mereka dengan mengikuti program pelatihan keamanan siber dan menggunakan alat keamanan yang tersedia. Selain itu, pengembangan kebijakan yang lebih komprehensif dan penerapan teknologi canggih untuk mendeteksi ancaman siber perlu diperkuat. Pemerintah dan lembaga terkait harus melibatkan lebih banyak pihak dalam menyebarkan informasi tentang pentingnya menjaga data pribadi dan memperkenalkan langkah-langkah preventif dalam menghadapi potensi ancaman siber di dunia maya.

REFERENSI

Anam, K. (2018). Analisa Dan Perancangan Sistem Informasi Akademik Berbasis Web Pada Mi Al-Mursyidiyyah Al-'Asyirotussyafi'Iyyah. *Jurnal Teknik Informatika*, *11*(2), 207–217. https://doi.org/10.15408/jti.v11i2.8867

Andini, D. Y. A., & Anisa, C. (2022). *Analisis Penilaian Resiko Keamanan Sistem Informasi Akademik Security Risk Assessment Analysis Academic Information System*. *1*(1), 1–7.

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Ariyadi, T., Widodo, T. L., Apriyanti, N., & Kirana, F. S. (2023). Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP. *Techno.Com*, *22*(2), 418–429. https://doi.org/10.33633/tc.v22i2.7562

Azhari, F., Sumarno, S., Fauzi, A., & Pratama, D. R. (2024). *Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-wallet*. *2*(2), 138–147.

Budi, D. S., & Tarigan, A. (2018). 1) Jl. Ring Road Utara, Condong Catur, Sleman 55283 2) Jl. Margonda Raya 100. *Tahun*, *2*(1), 53–64.

Cahyono, D., Fahrudin, R., Sinclair, A., Informatika, F. T., Info, A., Data, K., Banking, M., Multifactor, A., & Pengguna, E. (2024). *Pentingnya Edukasi dalam Mengatasi Keamanan Data Mobile Banking di Indonesia*. *3*(1), 81–89.

Chalifa, C. (2015). *Jurnal Informasi Volume VII*. *VII*(1), 58–82. https://informasi.stmik-im.ac.id/wp-content/uploads/2016/05/03-Haryoso-Wicaksono.pdf

Damayanti, S., Elysia, Y. G., Purba, O. A. P., & Prawira, I. F. A. (2021). Pengaruh Penggunaan Sistem Informasi Akademik Di Lingkungan Pendidikan Tinggi. *Jurnal MANAJERIAL*, *20*(1), 43–53. https://doi.org/10.17509/manajerial.v20i1.25095

Destrianto, F. R., Armys, M., & Sitorus, R. (2017). *Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE*. *9*(1), 35–47.

Emi, S. E., & Farizy, S. (2021). Sistem Informasi Manajemen. In *Tangerang Selatan* (Issue 1). www.unpam.ac.id

Fachrudin, R., Respaty, E., Adilah, I. S., & Sinlae, F. (2024). *Multidisciplinary Science Peranan Penting Manajemen Sekuriti di Era Digitalisasi*. *2*(1), 94–102.

Hariono, T., Iqbal, M., Yaqin, N., & Hilyah, A. (2019). Web-Based Academic Information System. *IOP Conference Series: Materials Science and Engineering*, *662*(2). https://doi.org/10.1088/1757-899X/662/2/022042

Hariyanto, S. (2018). Sistem Informasi Manajemen. *Sistem Informasi Manajemen*, *9*(1), 80–85. https://jurnal-unita.org/index.php/publiciana/article/viewFile/75/69

Homaidi, A. (2015). Tijd van slapen: Verstoring van de biologische klok door nacht-en wisse

ldiensten. *Nederlands Tijdschrift Voor Geneeskunde*, *159*(51–52), 17–23.
Hutapea, Y., Fauzi, A., Dwiyanti, A., Alifah, F. A., Andina, N., & Jati, S. M. D. (2024). *Peran Manajemen Sekuriti Dalam Mencegah Resiko Kerugian Terhadap Keuangan Digital*. *2*(2).
Intan Mafiana, A., Hanum, L., Ilmi, H. M., & Febriliani, S. (2023). Implementasi Manajemen Keamanan Informasi Berbasis Iso 27001 Pada Sistem Informasi Akademik. *Journal of Digital Business and Innovation Management*, *2*(2), 139–163. https://doi.org/10.26740/jdbim.v2i2.57580
Irawan, C. R., Fauzi, A., Sanjaya, F., & Ramadhan, A. (2024). *Pengaruh Efektivitas Manajemen Sekuriti Dalam Keamanan Perusahaan*. *3*(1), 59–68.
Islami, D. C., I.H, K. B., & Candiwan, C. (2016). Kesadaran Keamanan Informasi pada Pegawai Bank x di Bandung Indonesia. *Jurnal INKOM*, *10*(1), 19. https://doi.org/10.14203/j.inkom.428
Kurniawan Ritonga, R., & Firdaus, R. (2024). Pentingnya Sistem Informasi Manajemen Dalam Era Digital the Importance of Management Information Systems in the Digital Era. *JICN: Jurnal Intelek Dan Cendikiawan Nusantara* , *1*(3), 4353–4358. https://jicnusantara.com/index.php/jicn
Mahameru, D. E., Nurhalizah, A., Wildan, A., Haikal, M., & Rahmadia, M. H. (2023). *Implementasi Uu Perlindungan Data*. *5*(20), 115–131.
Maulana, G. R., Aqila, S. W., Sakinah, N. H., Wulandari, N. I., & Nurhayati, I. (2023). *PENGAMANAN DATA PRIBADI MAHASISWA PRODI AKUNTANSI UNIVERSITAS TRUNOJOYO MADURA*. *9*(2), 89–96.
Mewengkang, R., Tumbel, G., Mamonto, F., & Joufree, V. N. (2021). *YUME : Journal of Management Implementasi Kebijakan Sistem Informasi Manajemen Akademik Di Universitas Negeri Manado*. *4*(2), 318–339. https://doi.org/10.37531/yume.vxix.234
Milafebina, R., Lesmana, I. P., & Syailendra, M. R. (2023). Perlindungan Data Pribadi terhadap Kebocoran Data Pelanggan E-commerence di Indonesia. *Jurnal Tana Man*, *4*(1), 158–169. https://ojs.staialfurqan.ac.id/jtm/
Ramayani, Y., & Oktarina, T. (2022). *Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA)*. 289–296.
Saraswati, E. (2013). Sistem Informasi Akademik Berbasis WEB Pada Sekolah Menengah Pertama N 3 Pringkulu. *Indonesia Jurnal on Networking and Security*, *2*(2), 58–63.
Satoto, K. I. (2008). Analisis Keamanan Sistem Informasi Akademik Berbasis Web Di Fakultas Teknik Universitas Diponegoro Oleh : Ir . Kodrat Iman Satoto , MT Program Studi Sistem Komputer Fakultas Teknik Universitas Diponegoro. *Seminar Nasional Aplikasi Sains Dan Teknologi ISSN:1979-911X*, *13 Desember*, 175–186.
Setiawan, A., & Yulianto, E. (2020). *Keamanan Dalam Media Digital* (Edisi Pert). Informatika Bandung.
Sharipuddin. (2014). *SISTEM INFORMASI AKADEMIK (STUDI KASUS PADA STIKOM DINAMIKA BANGSA)*. *9*(2), 132–140.
Siagian, S. H. T., & Effiyaldi. (2018). *AKADEMIK PADA STIKES PRIMA JAMBI*. *3*(4), 1282–1291.
Silvia, A. F., Saputra, W., Sunaryo, H., Sinlae, F., & Info, A. (2024). *Multidisciplinary Science Analisis Keamanan Data Pribadi pada Pengguna BPJS Kesehatan : Ancaman , Risiko , Strategi*. *2*(1), 201–207.
Sugiartono, A. M., Yasril, A., Sumantry, D. H., Nugraha, D. A., Arif, I. N., Nugroho, P. B., Fauzan, R., & Saepudin, T. H. (2024). *No Title*. *2*(7), 742–747.
Susanto, E., Moses, H., Ramadan, R., & Deanova, S. (2023). Analisis dan Pengembangan Sistem Manajemen Sekuriti pada PT. Denso Manufacturing Indonesia. *Jurnal Ilmiah Wahana Pendidikan*, *9*(13), 225–236.
Taylor, B., & Bean, H. (2013). The handbook of communication history. In *The Handbook of Communication History*. Taylor & Francis. https://doi.org/10.4324/9780203149119
Ujung, A. M., Irwan, M., & Nasution, P. (2023). Pentingnya Sistem Keamanan Database untuk melindungi data pribadi. *JISKA: Jurnal Sistem Informasi Dan Informatika*, *1*(2), 44.

http://jurnal.unidha.ac.id/index.php/jteksis

Wahyu Hidayat M, Nurhayi Musdira, Natatsa Rasyid, Miftahul Khairi S, & Muh Juharman. (2023). Analisis Ancaman Terhadap Keamanan Data Pribadi pada Email. *Jurnal Pendidikan Terapan*, *01*, 7–12. https://doi.org/10.61255/jupiter.v1i2.73

Waruwu, M. (2022). Motivasi Belajar Dan Prestasi Belajar Pada Mata Pelajaran Ppkn Di Indonesia: Kajian Analisis Meta. *Bhineka Tunggal Ika: Kajian Teori Dan Praktik Pendidikan PKn*, *9*(2), 99–113. https://doi.org/10.36706/jbti.v9i2.18333

Wijoyo, A., Fatimah, S., Toni, Widianti, Y., & Fadillah, M. (2023). *Keamanan Data dalam Sistem Informasi Manajemen : Risiko dan Strategi Perlindungan*. *1*(2), 1–7.

Yel, M. B., & Nasution, M. K. M. (2022). Keamanan Informasi Data Pribadi Pada Media Sosial. *Jurnal Informatika Kaputama (JIK)*, *6*(1), 92–101. https://doi.org/10.59697/jik.v6i1.144

Zahwani, S. T., & Nasution, M. I. P. (2024). *Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital*. *2*(2), 105–109.