Jurnal Teknik Informatika
Vol. 1, No. 1, Februari 2026, pp. 1~5

Kesenjangan antara Pengetahuan dan Perilaku Keamanan Informasi Pengguna Media Sosial dalam Menghadapi Ancaman Rekayasa Sosial

Ratu Bilqis Mantika RO[1], Clinton[2], Dede Pramana Putra[3], Muhammad Gigin Febriano[4], Agung Riyadi[5]
[1,2,3,4,5]Program Studi PJJ Teknik Informatika, Universitas Siber Asia, Indonesia
Email: bilqisirvanro@gmail.com; clintonqq12@gmail.com

ABSTRAK

Meningkatnya penggunaan media sosial beriringan dengan meningkatnya ancaman keamanan informasi, khususnya serangan berbasis rekayasa sosial. Penelitian ini bertujuan untuk menganalisis kesenjangan antara pengetahuan dan perilaku keamanan informasi pengguna media sosial dalam menghadapi ancaman tersebut. Metode penelitian yang digunakan adalah studi literatur dengan pendekatan kualitatif deskriptif terhadap artikel jurnal nasional yang relevan dan diterbitkan dalam rentang tahun 2020–2025. Hasil analisis menunjukkan bahwa sebagian besar pengguna media sosial telah memiliki pengetahuan dan sikap yang cukup baik terkait keamanan informasi, termasuk pemahaman terhadap risiko phishing dan kebocoran data pribadi. Namun, tingkat pengetahuan tersebut belum sepenuhnya tercermin dalam perilaku keamanan yang konsisten, seperti penggunaan kata sandi yang kuat, pembaruan kredensial secara berkala, dan pemanfaatan fitur keamanan platform. Temuan ini mengindikasikan adanya kesenjangan signifikan antara aspek kognitif dan perilaku pengguna. Penelitian ini menegaskan pentingnya pendekatan keamanan informasi yang berorientasi pada perubahan perilaku (human-centered security) sebagai dasar pengembangan strategi edukasi keamanan informasi yang lebih efektif bagi pengguna media sosial.

Kata Kunci: keamanan informasi; media sosial; rekayasa sosial; perilaku pengguna; studi literatur

ABSTRACT

The increasing use of social media is accompanied by increasing information security threats, particularly social engineering-based attacks. This study aims to analyze the gap between social media users' information security knowledge and behavior in dealing with these threats. The research method used is a literature study with a descriptive qualitative approach to relevant national journal articles published between 2020 and 2025. The analysis results indicate that most social media users have fairly good knowledge and attitudes regarding information security, including an understanding of the risks of phishing and personal data leakage. However, this level of knowledge is not fully reflected in consistent security behaviors, such as the use of strong passwords, regular credential updates, and utilization of platform security features. These findings indicate a significant gap between the cognitive and behavioral aspects of users. This study emphasizes the importance of a human-centered approach to information security as the basis for developing a more effective information security education strategy for social media users.

Keyword: information security; social media; social engineering; user behavior; literature review

Corresponding Author:
Ratu Bilqis Mantika RO,
Universitas Siber Asia,
Jalan R.M Harsono No.1 RT09/04 Ragunan, Pasar Minggu, Jakarta Selatan
Lantai 1-2, South Jakarta City, Jakarta 12550, Indonesia
Email: bilqisirvanro@gmail.com

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong peningkatan penggunaan media sosial secara signifikan di berbagai kalangan masyarakat. Berdasarkan laporan *Digital 2025 Global Overview* yang diterbitkan oleh We Are Social dan DataReportal, jumlah akun media sosial aktif di seluruh dunia diperkirakan mencapai lebih dari 5,24 miliar pada tahun 2025, yang menunjukkan tingginya penetrasi media sosial dalam kehidupan masyarakat global. Di Indonesia, penggunaan media sosial juga mengalami pertumbuhan yang pesat. Data pengguna media sosial sekitar 150 juta merupakan angka historis yang dilaporkan dalam riset *Digital 2019* oleh We Are Social, dengan dominasi pengguna pada rentang usia 18–34 tahun.

Penelitian Gunawan (2021) menunjukkan bahwa mahasiswa menjadi salah satu kelompok pengguna media sosial paling aktif karena tingginya intensitas penggunaan internet dalam kehidupan sehari-hari. Meskipun demikian, pengguna media sosial pada umumnya telah memahami pentingnya keamanan informasi, namun sebagian besar belum menerapkan praktik keamanan dasar secara konsisten, seperti mengganti kata sandi secara berkala dan memanfaatkan pengaturan privasi media sosial (Gunawan, 2021). Media sosial dimanfaatkan sebagai sarana komunikasi, penyebaran informasi, hiburan, hingga aktivitas akademik. Tingginya intensitas penggunaan media sosial tersebut berdampak pada meningkatnya potensi risiko terhadap keamanan informasi, sehingga ancaman keamanan informasi menjadi semakin kompleks, salah satunya adalah serangan berbasis rekayasa sosial (*social engineering*).

Rekayasa sosial merupakan teknik serangan yang memanfaatkan manipulasi psikologis untuk mengeksploitasi kelemahan manusia guna memperoleh informasi rahasia atau mendorong pengguna melakukan tindakan yang tidak sah, seperti pencurian data pribadi, kredensial akun, dan akses ilegal terhadap sistem. Serangan ini umumnya muncul dalam bentuk *phishing*, *vishing*, pesan palsu, maupun akun tiruan yang menyerupai pihak resmi (Zein, 2023).

Permasalahan utama dalam keamanan informasi tidak semata-mata terletak pada rendahnya tingkat pengetahuan pengguna, melainkan pada ketidaksesuaian antara pengetahuan yang dimiliki dan perilaku yang diterapkan dalam penggunaan media sosial. Banyak pengguna telah mengetahui risiko kebocoran data pribadi, bahaya *phishing*, serta pentingnya pengaturan privasi, namun dalam praktiknya masih mengabaikan langkah-langkah keamanan dasar. Fenomena ini menunjukkan bahwa kesadaran keamanan informasi tidak selalu berbanding lurus dengan perilaku aman pengguna di lingkungan digital.

Beberapa faktor dapat menjadi penyebab terjadinya kesenjangan antara pengetahuan dan perilaku keamanan informasi. Faktor kenyamanan dan kemudahan penggunaan media sosial sering kali mendorong pengguna untuk mengorbankan aspek keamanan demi efisiensi waktu dan kepraktisan. Selain itu, persepsi risiko yang rendah terhadap ancaman rekayasa sosial menyebabkan pengguna cenderung meremehkan potensi dampak yang ditimbulkan. Kebiasaan penggunaan media sosial yang bersifat berulang dan otomatis juga berkontribusi terhadap terbentuknya perilaku yang kurang memperhatikan aspek keamanan informasi.

Berdasarkan kondisi tersebut, penelitian mengenai kesenjangan antara pengetahuan dan perilaku keamanan informasi menjadi penting untuk dilakukan. Pemahaman yang komprehensif mengenai faktor-faktor penyebab kesenjangan ini diharapkan dapat menjadi dasar dalam merancang strategi edukasi keamanan informasi yang tidak hanya berorientasi pada peningkatan pengetahuan, tetapi juga pada pembentukan kebiasaan dan perilaku aman bagi pengguna media sosial.

2. METODE

Penelitian ini menggunakan metode studi literatur (*literature review*) dengan pendekatan kualitatif deskriptif. Metode ini dipilih untuk menganalisis dan mengkaji secara mendalam temuan-temuan penelitian terdahulu yang berkaitan dengan kesadaran keamanan informasi, perilaku pengguna media sosial, serta ancaman rekayasa sosial. Pendekatan kualitatif digunakan untuk memahami pola, kecenderungan, dan kesenjangan antara pengetahuan dan perilaku keamanan informasi pengguna media sosial berdasarkan hasil penelitian sebelumnya.

A. Sumber Data Penelitian

Sumber data dalam penelitian ini berupa data sekunder yang diperoleh dari artikel jurnal ilmiah nasional yang relevan dengan topik penelitian. Jurnal yang digunakan dipilih berdasarkan kriteria sebagai berikut:

1. Membahas keamanan informasi dan/atau rekayasa sosial.
2. Berfokus pada pengguna media sosial atau aktivitas digital.
3. Berasal dari jurnal nasional terakreditasi atau jurnal ilmiah yang memiliki reputasi baik.
4. Diterbitkan dalam rentang waktu lima tahun terakhir (2020–2025).

B. Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan melalui penelusuran literatur dengan mengakses basis data jurnal nasional, seperti Google Scholar, Garuda, dan portal jurnal perguruan tinggi, serta sumber daring lainnya. Proses penelusuran dilakukan dengan menggunakan kata kunci keamanan informasi, kesadaran keamanan, media sosial, dan rekayasa sosial. Artikel yang diperoleh selanjutnya diseleksi berdasarkan tingkat relevansi dan kesesuaian dengan fokus penelitian.

C. Teknik Analisis Data

Analisis data dilakukan melalui beberapa tahapan, yaitu:

1. Identifikasi tujuan, metode, dan temuan utama dari masing-masing jurnal yang dianalisis.
2. Klasifikasi temuan penelitian ke dalam tiga dimensi utama, yaitu pengetahuan, sikap, dan perilaku keamanan informasi.
3. Perbandingan antara tingkat pengetahuan dan perilaku keamanan informasi pengguna media sosial untuk mengidentifikasi kesenjangan yang ada.
4. Interpretasi hasil analisis untuk menarik kesimpulan mengenai faktor-faktor yang menyebabkan kesenjangan antara pengetahuan dan perilaku keamanan informasi.

Jurnal yang dianalisis dalam penelitian ini meliputi penelitian oleh Gunawan (2021), Zein (2023), Hartiwi et al. (2024), Setiyawan et al. (2022), serta Tan et al. (2024). Hasil analisis disajikan dalam bentuk narasi deskriptif yang menjelaskan hubungan antara pengetahuan, perilaku, dan tingkat kerentanan pengguna terhadap ancaman rekayasa sosial.

D. Alur Penelitian

Alur penelitian dimulai dari penentuan topik penelitian, pengumpulan jurnal terkait, analisis isi jurnal, hingga penarikan kesimpulan. Penelitian ini tidak melibatkan pengumpulan data primer sehingga tidak memerlukan responden secara langsung.

3. HASIL DAN PEMBAHASAN

A. Hasil Analisis Studi Literatur

Berdasarkan hasil analisis terhadap sejumlah jurnal ilmiah yang membahas kesadaran keamanan informasi dan ancaman rekayasa sosial pada pengguna media sosial, ditemukan pola temuan yang relatif konsisten. Secara umum, sebagian besar pengguna media sosial telah memiliki tingkat pengetahuan yang baik mengenai keamanan informasi. Pengetahuan tersebut mencakup pemahaman terhadap berbagai bentuk serangan rekayasa sosial, seperti *phishing*, *vishing*, dan penipuan berbasis media sosial, serta kesadaran akan risiko kebocoran data pribadi dan penyalahgunaan akun (Gunawan, 2021; Zein, 2023).

Meskipun demikian, hasil studi literatur menunjukkan bahwa tingkat pengetahuan yang relatif baik tersebut belum diikuti oleh perilaku keamanan informasi yang sebanding. Beberapa penelitian mengungkapkan bahwa pengguna masih sering menerapkan praktik penggunaan media sosial yang kurang aman, seperti penggunaan kata sandi yang lemah atau sama pada beberapa akun, jarang melakukan pembaruan kata sandi, serta kurang memanfaatkan fitur keamanan dan pengaturan privasi yang tersedia pada platform media sosial (Setiyawan et al., 2022; Tan et al., 2024). Temuan ini menunjukkan adanya ketidaksesuaian antara pemahaman konseptual pengguna mengenai keamanan informasi dan praktik aktual dalam penggunaan media sosial sehari-hari.

Selain itu, hasil penelitian terdahulu juga memperlihatkan bahwa meskipun pengguna memiliki sikap positif terhadap pentingnya keamanan informasi, sikap tersebut belum sepenuhnya tercermin dalam tindakan nyata. Dimensi perilaku keamanan informasi cenderung berada pada tingkat yang lebih rendah dibandingkan dimensi pengetahuan dan sikap. Kondisi ini mengindikasikan bahwa pengguna media sosial masih berada pada posisi rentan terhadap serangan rekayasa sosial, meskipun secara kognitif telah memahami bentuk dan dampak ancaman yang ada (Hartiwi et al., 2024).

Temuan lain yang muncul dari analisis literatur adalah rendahnya konsistensi perilaku keamanan informasi pengguna dalam aktivitas digital. Pengguna cenderung bersikap waspada pada situasi tertentu, namun mengabaikan aspek keamanan pada kondisi lain, terutama ketika aktivitas media sosial dilakukan secara rutin dan berulang. Pola ini semakin memperkuat indikasi adanya kesenjangan antara pengetahuan, sikap, dan perilaku keamanan informasi pengguna media sosial.

Tabel 1. Analisis Komparatif Temuan Penelitian Terdahulu

No	Penelitian	Pengetahuan	Sikap	Perilaku	Bentuk Kesenjangan
1	Gunawan (2021)	Baik: pemahaman *phishing* dan privasi media sosial	Positif	Penggunaan kata sandi lemah; pengaturan privasi diabaikan	Praktik keamanan dasar tidak diterapkan
2	Hartiwi et al. (2024)	Baik: pemahaman risiko *social engineering*	–	Edukasi bersifat parsial dan tidak berkelanjutan	Pengetahuan tidak berujung pada tindakan
3	Setiyawan et al. (2022)	Baik: pemahaman metodologi *MCDA*	–	Skor perilaku rendah akibat banyaknya kriteria	Kompleksitas metode menurunkan praktik

No	Penelitian	Pengetahuan	Sikap	Perilaku	Bentuk Kesenjangan
4	Tan et al. (2024)	Sedang: kesadaran keamanan siber	Positif	Tingkat adopsi *2FA* rendah secara regional	Kesenjangan adopsi teknologi keamanan
5	Zein (2023)	Baik: sistem dan ancaman keamanan informasi	–	Kesadaran dan respons pengguna tidak konsisten	Kesenjangan sistem dan perilaku

Tabel 1 menyajikan analisis komparatif temuan penelitian terdahulu terkait pengetahuan, sikap, dan perilaku keamanan informasi pengguna media sosial.

B. Pembahasan

Hasil analisis studi literatur menunjukkan bahwa kesenjangan antara pengetahuan dan perilaku keamanan informasi merupakan permasalahan utama dalam upaya perlindungan pengguna media sosial dari ancaman rekayasa sosial. Fenomena ini menegaskan bahwa faktor manusia masih menjadi elemen paling rentan dalam sistem keamanan informasi. Pengetahuan yang dimiliki pengguna belum secara otomatis mendorong terbentuknya perilaku keamanan yang konsisten dan berkelanjutan.

Salah satu faktor utama yang berkontribusi terhadap kesenjangan tersebut adalah dominannya orientasi kenyamanan dan efisiensi dalam penggunaan media sosial. Pengguna cenderung mengutamakan kemudahan akses, kecepatan interaksi, dan kenyamanan penggunaan dibandingkan dengan penerapan langkah-langkah keamanan yang dianggap merepotkan. Akibatnya, praktik keamanan dasar sering kali diabaikan meskipun pengguna menyadari potensi risiko yang dapat terjadi (Gunawan, 2021; Tan et al., 2024).

Selain faktor kenyamanan, persepsi risiko yang rendah terhadap ancaman rekayasa sosial juga memengaruhi perilaku keamanan informasi pengguna. Banyak pengguna menganggap bahwa serangan rekayasa sosial hanya berpotensi terjadi pada pihak lain atau dalam situasi tertentu, sehingga tingkat kewaspadaan menjadi menurun. Kondisi ini menyebabkan pengguna kurang berhati-hati dalam merespons pesan, tautan, atau permintaan informasi yang mencurigakan di media sosial (Zein, 2023).

Dalam konteks mahasiswa sebagai pengguna media sosial yang aktif, tingginya intensitas interaksi digital turut memperbesar peluang terjadinya paparan terhadap serangan rekayasa sosial. Meskipun mahasiswa umumnya memiliki tingkat literasi digital yang cukup baik, kebiasaan penggunaan media sosial yang bersifat rutin dan berulang dapat menurunkan tingkat kehati-hatian. Hal ini menunjukkan bahwa literasi digital dan pengetahuan keamanan informasi belum tentu berbanding lurus dengan penerapan perilaku aman dalam aktivitas digital sehari-hari (Tan et al., 2024).

Temuan penelitian ini mengindikasikan bahwa strategi peningkatan keamanan informasi perlu diarahkan pada pendekatan yang lebih berorientasi pada perubahan perilaku. Edukasi keamanan informasi yang hanya menekankan aspek pengetahuan cenderung kurang efektif apabila tidak disertai dengan pembentukan kebiasaan dan penguatan perilaku keamanan. Pendekatan yang bersifat praktis, seperti simulasi serangan rekayasa sosial, pelatihan pengenalan pesan mencurigakan, serta penguatan kebijakan keamanan di lingkungan akademik, dapat menjadi alternatif solusi untuk memperkecil kesenjangan antara pengetahuan dan perilaku keamanan informasi (Hartiwi et al., 2024).

Dengan demikian, pembahasan ini menegaskan pentingnya penerapan pendekatan keamanan informasi yang berpusat pada manusia (*human-centered security*). Pendekatan ini menempatkan perilaku pengguna sebagai fokus utama dalam upaya pencegahan ancaman rekayasa sosial, sehingga perlindungan keamanan informasi tidak hanya bergantung pada teknologi, tetapi juga pada kesadaran dan tindakan nyata pengguna media sosial.

Tabel 2. Faktor Penyebab Kesenjangan Pengetahuan dan Perilaku Keamanan Informasi

Faktor	Manifestasi	Bukti Literatur	Implikasi
Comfort Bias	Preferensi terhadap akses cepat dan kemudahan penggunaan dibandingkan penerapan prosedur keamanan	Gunawan (2021): pengabaian autentikasi dua faktor (*2FA*); Setiyawan et al. (2022): faktor kenyamanan dalam pengambilan keputusan	Kebiasaan pengguna lebih dominan dibandingkan pengetahuan keamanan
Low Risk Perception	Anggapan bahwa ancaman hanya terjadi pada pengguna lain	Tan et al. (2024): *overconfidence* pada mahasiswa; Zein (2023): kesadaran keamanan yang tidak konsisten	Penurunan kewaspadaan terhadap potensi risiko
Implementation Gap	Pengetahuan keamanan tidak diikuti praktik yang berkelanjutan	Hartiwi et al. (2024): efek jangka pendek edukasi; Setiyawan et al. (2022): kompleksitas metode	Kegagalan pembentukan perilaku keamanan yang berkelanjutan

Tabel 2 menggambarkan faktor-faktor utama yang menyebabkan kesenjangan antara pengetahuan dan perilaku keamanan informasi, yang meliputi faktor kenyamanan, persepsi risiko, dan kebiasaan penggunaan media sosial.

4. SIMPULAN DAN SARAN

Penelitian ini mengidentifikasi adanya kesenjangan yang signifikan antara pengetahuan dan perilaku keamanan informasi pengguna media sosial dalam menghadapi ancaman rekayasa sosial. Meskipun pengguna media sosial umumnya telah memiliki tingkat pengetahuan yang memadai mengenai keamanan informasi dan bentuk-bentuk ancaman rekayasa sosial, pengetahuan tersebut belum sepenuhnya terimplementasi dalam perilaku keamanan yang konsisten. Praktik penggunaan media sosial yang kurang aman, seperti penggunaan kata sandi yang lemah serta rendahnya pemanfaatan fitur keamanan yang tersedia, masih banyak ditemukan.

Hasil penelitian ini menunjukkan bahwa peningkatan pengetahuan semata tidak cukup untuk mencegah ancaman rekayasa sosial. Diperlukan pendekatan yang lebih komprehensif yang tidak hanya berfokus pada aspek kognitif, tetapi juga pada pembentukan sikap dan perilaku keamanan informasi yang berkelanjutan. Oleh karena itu, strategi peningkatan keamanan informasi perlu diarahkan pada edukasi yang bersifat aplikatif dan berorientasi pada perubahan perilaku pengguna media sosial.

Penelitian ini menegaskan pentingnya penerapan pendekatan keamanan informasi yang berpusat pada manusia (*human-centered security*) sebagai upaya yang efektif dalam mengurangi risiko serangan rekayasa sosial di media sosial. Pendekatan ini menempatkan perilaku pengguna sebagai elemen kunci dalam sistem keamanan informasi, sehingga perlindungan tidak hanya bergantung pada teknologi, tetapi juga pada kesadaran dan tindakan nyata pengguna.

Dalam jangka panjang, penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan strategi keamanan informasi yang lebih efektif serta meningkatkan kesadaran masyarakat mengenai pentingnya penerapan perilaku keamanan informasi dalam penggunaan media sosial.

REFERENSI

Gunawan, H. (2021). Pengukuran kesadaran keamanan informasi dan privasi dalam sosial media. *Jurnal Muara Sains, Teknologi, Kedokteran dan Ilmu Kesehatan, 5*(1), 1–10. https://doi.org/10.24912/jmstkik.v5i1.3456

Hartiwi, Y., Arvita, Y., Purnasari, M., & Nurhayati. (2024). Sosialisasi edukasi bahaya dan upaya pencegahan *social engineering* untuk meningkatkan keamanan informasi. *Jurnal Pengabdian Masyarakat UNAMA, 3*(1), 65–72.

Setiyawan, G. P. B., Helilintar, R., & Wulanningrum, R. (2022). Sistem informasi survei pengukuran tingkat kesadaran keamanan informasi menggunakan metode *multiple criteria decision analysis* (MCDA). in *Seminar Nasional Inovasi Teknologi*.

Tan, T., Sama, H., Wibowo, T., Wijaya, G., & Aboagye, O. E. (2024). Kesadaran keamanan siber pada kalangan mahasiswa universitas di Kota Batam. *Jurnal Teknologi dan Informasi, 14*(2), 163–173. https://doi.org/10.34010/jati.v14i2.12518

Zein, A. (2023). Analisa penyerangan untuk *cyber security social engineering*. *Jurnal Sistem Informasi, 8*(4), 642–648.