Journal of Student Development Information System (JoSDIS)
e-ISSN:2774-7948
Volume 6, Nomor 1, November 2025
Program Studi Sistem Informasi
Fakultas Sains dan Teknologi
Universitas Labuhanbatu

Ancaman *Hacker* Dan *Cybercrime* Di Indonesia Dan Pentingnya Pemahaman Untuk Keamanan Akun Media Sosial Instagram Pada Kalangan Mahasiswa

[1]Aji Kurnianto, [2]Alfa Reno Wijaya, [3]Adilillah Assyafii, [4]Indra Gunawan

[1,2,3,4]Teknik Informatika, STIKOM Tunas Bangsa

Email : [1]ajikurnianto31@gmail.com, [2]alfareno1188@gmail.com, [3]adillillah037@gmail.com, [4]indra@amiktunasbangsa.ac.id

Corresponding Author : ajikurnianto31@gmail.com

Abstract

The development of digital technology has increased social media usage among university students, but has also been accompanied by an increase in the threat of hackers and cybercrime. Low awareness of account security has led to many users becoming victims of hacking and personal data theft, particularly on the Instagram platform. This study aims to analyze cybercrime threats in Indonesia and the importance of understanding social media account security for university students. The method used was qualitative descriptive analysis through a review of recent literature. The results indicate that the main factor contributing to user vulnerability lies in a lack of digital literacy and understanding of basic security practices, such as the use of strong passwords and dual authentication. Therefore, increased cybersecurity education on campus is needed to make students more vigilant, responsible, and capable of protecting their personal data in the digital world.

Keywords: *Hackers, Cybercrime, Cybersecurity, Instagram, University Students.*

Pendahuluan

Penggunaan internet di Indonesia terus meningkat dari tahun ke tahun seiring dengan semakin luasnya akses internet dan adopsi teknologi digital di berbagai sektor. Berdasarkan data yang dirilis oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pada tahun 2022, jumlah pengguna internet di Indonesia mencapai sekitar 210 juta orang atau sekitar 78,4% dari total populasi Indonesia yang mencapai 267,7 juta jiwa (Hapsari and Pambayun, 2023).

Fenomena peningkatan kasus *cybercrime* di Indonesia dalam lima tahun terakhir menjadi perhatian serius, terutama di kalangan muda yang aktif menggunakan media sosial seperti Instagram**.** Data dari *Indonesia Cyber Security Report (2024)* menunjukkan bahwa lebih dari 58% serangan siber di Indonesia menargetkan pengguna individu, dengan mahasiswa sebagai kelompok paling rentan karena rendahnya kesadaran terhadap keamanan digital. Menurut Tobondo *et al.*, (2024) ancaman *cyberattack* di Indonesia tidak hanya berasal dari luar negeri tetapi juga dari pelaku domestik yang memanfaatkan kelemahan literasi digital masyarakat.

Instagram, sebagai salah satu platform paling populer di Indonesia, menjadi target empuk para *hacker* dan *social engineer*. Studi Mouncey and Ciobotaru, (2025)

menegaskan bahwa banyak akun Instagram di Indonesia disusupi melalui serangan *phishing*, *brute force*, dan *social engineering*, yang kerap terjadi akibat kurangnya pemahaman pengguna terhadap keamanan digital dasar seperti autentikasi dua faktor dan pengelolaan kata sandi.

Mahasiswa, sebagai pengguna aktif media sosial, sering kali mengabaikan aspek keamanan karena menganggap akun media sosial hanya sebagai sarana ekspresi, bukan aset digital pribadi. Temuan Octavia *et al.*, (2025) memperlihatkan bahwa 72% mahasiswa tidak pernah mengganti kata sandi akun mereka selama lebih dari satu tahun, dan hanya 18% yang mengaktifkan fitur keamanan tambahan di Instagram. Hal ini menunjukkan rendahnya kesadaran siber yang menjadi salah satu penyebab utama meningkatnya kasus pencurian data pribadi, penipuan digital, dan penyalahgunaan identitas daring (Soesanto *et al.*, 2023).

Fenomena ini memperlihatkan urgensi penelitian tentang ancaman hacker dan pentingnya pemahaman keamanan siber pada kalangan mahasiswa, khususnya pengguna Instagram, sebagai bagian dari upaya membangun literasi digital dan kesadaran keamanan informasi di era siber.

Landasan Teori

Cybercrime dan *Hacker*

Cybercrime didefinisikan sebagai aktivitas kriminal yang menggunakan komputer atau jaringan digital sebagai sarana utama dalam melakukan kejahatan. Hacker biasanya memanfaatkan kerentanan sistem atau kelalaian pengguna untuk mendapatkan akses ilegal. Di Indonesia, kasus serangan hacker meningkat seiring dengan penggunaan internet yang masif. Tobondo *et al.*, (2024) menyoroti bahwa Indonesia kini masuk dalam 10 besar negara dengan aktivitas siber tertinggi di Asia Tenggara**,** terutama serangan terhadap akun media sosial dan layanan keuangan digital.

Keamanan Akun Media Sosial

Menurut Kurniawan *et al.*, (2023), kesadaran keamanan data pribadi di media sosial masih rendah, terutama di kalangan mahasiswa. Risiko keamanan mencakup pencurian data pribadi, *phishing*, *identity theft*, dan manipulasi psikologis (*social engineering*). Instagram, sebagai platform visual berbasis data pribadi, rentan terhadap serangan tersebut.

Literasi dan Kesadaran Siber

Penelitian Reuben *et al.*, (2023) menyebutkan bahwa tingkat kesadaran siber mahasiswa berhubungan erat dengan pengalaman mereka dalam menghadapi serangan digital. Mahasiswa yang pernah menjadi korban cenderung lebih berhati-hati dibanding yang belum. Kesadaran ini bisa ditingkatkan melalui edukasi keamanan siber dan kampanye digital *awareness*.

Teori Perlindungan Perilaku (*Protection Motivation Theory*)

Teori ini menjelaskan bahwa perilaku perlindungan diri terhadap ancaman digital tergantung pada persepsi risiko dan kemampuan individu untuk mengatasi ancaman tersebut. Menurut Devananta, (2021), mahasiswa yang memahami konsekuensi

kehilangan data pribadi lebih termotivasi untuk menerapkan langkah keamanan seperti *two-factor authentication* dan *password management.*

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode analisis deskriptif**.** Data diperoleh melalui studi literatur terhadap jurnal ilmiah nasional dan internasional periode 2021–2025 yang membahas isu *cybersecurity awareness*, ancaman hacker, dan perilaku pengguna Instagram di Indonesia. Analisis dilakukan dengan menelaah 15 artikel akademik, seperti karya Octavia *et al.*, (2025), Tobondo *et al.*, (2024) dan Reuben *et al.*, (2023), untuk memahami pola kesadaran keamanan di kalangan mahasiswa. Data dikategorikan ke dalam tiga tema utama: (1) bentuk ancaman hacker terhadap Instagram, (2) tingkat kesadaran mahasiswa terhadap keamanan siber, dan (3) strategi perlindungan akun pribadi.

Pendekatan deskriptif kualitatif dipilih karena memungkinkan peneliti menafsirkan data berdasarkan konteks sosial dan perilaku pengguna, bukan sekadar angka statistik. Analisis dilakukan dengan cara *content analysis* terhadap hasil studi terdahulu guna mengidentifikasi kesamaan temuan, perbedaan, dan tren umum yang mencerminkan kondisi nyata di lapangan.

Hasil Dan Pembahasan

Penelitian oleh Octavia *et al.*, (2025) secara spesifik menyoroti peran pemahaman keamanan siber terhadap perlindungan akun Instagram mahasiswa. Dalam studi tersebut ditemukan bahwa banyak mahasiswa tidak menyadari potensi kebocoran data pribadi yang mereka bagikan secara terbuka di media sosial. Lebih dari 60% responden mengaku tidak menggunakan fitur keamanan tambahan seperti *two-factor authentication (2FA)*, dan sebagian besar menggunakan kata sandi yang sama untuk beberapa platform digital. Rendahnya kesadaran ini memperbesar peluang peretasan akun melalui teknik manipulasi psikologis dan pencurian kredensial.

Sementara itu Kurniawan *et al.*, (2023), dalam risetnya mengenai kesadaran keamanan data pribadi di kalangan mahasiswa Indonesia, menemukan bahwa hanya sekitar 35% mahasiswa yang memiliki tingkat kesadaran tinggi terhadap privasi daring. Sebagian besar menganggap ancaman siber sebagai hal yang tidak terlalu serius atau "tidak akan terjadi pada diri mereka sendiri." Fenomena ini dikenal sebagai *optimism bias*, yakni persepsi keliru bahwa risiko digital hanya menimpa orang lain. Kondisi ini menyebabkan mahasiswa seringkali lengah dalam mengamankan akun, misalnya dengan membagikan informasi login kepada teman dekat atau menggunakan jaringan Wi-Fi publik tanpa pengamanan tambahan.

Selain itu, Reuben *et al.*, (2023) menunjukkan bahwa kampanye edukasi siber dan pelatihan keamanan digital berperan penting dalam meningkatkan kewaspadaan terhadap serangan sosial (*social engineering*). Mahasiswa yang pernah mengikuti pelatihan keamanan digital lebih cenderung mengadopsi kebiasaan aman seperti mengganti kata sandi secara berkala, menghindari tautan mencurigakan, dan berhati-hati dalam membagikan informasi pribadi. Penelitian ini sejalan dengan hasil Razak *et al.*,(2022), yang menemukan bahwa pengguna media sosial yang memiliki literasi keamanan digital tinggi cenderung lebih mampu mengenali pola penipuan dan serangan daring.

Dari hasil sintesis berbagai penelitian tersebut dapat disimpulkan bahwa ancaman hacker di Indonesia tidak semata berasal dari kelemahan sistem teknologi, tetapi lebih banyak dipicu oleh faktor manusia (human error). Mahasiswa yang kurang paham akan pentingnya literasi digital menjadi target utama pelaku kejahatan siber. Rendahnya kesadaran untuk menjaga keamanan akun pribadi di Instagram seperti tidak menggunakan verifikasi ganda atau membagikan data pribadi sembarangan menciptakan celah yang mudah dieksploitasi oleh peretas (Vera et al., 2024).

Secara umum, hasil pembahasan memperkuat argumen bahwa peningkatan pemahaman keamanan siber harus menjadi prioritas dalam dunia pendidikan tinggi. Universitas perlu berperan aktif melalui penyuluhan, seminar, dan program literasi digital agar mahasiswa tidak hanya mampu menggunakan teknologi, tetapi juga memahami risiko dan strategi perlindungan data pribadi. Hal ini penting untuk menciptakan lingkungan digital yang aman, bertanggung jawab, dan beretika di kalangan generasi muda Indonesia (Nabila and Refania, 2024).

Kesimpulan

Penelitian ini menyimpulkan bahwa ancaman *hacker* dan *cybercrime* di Indonesia**,** khususnya terhadap akun Instagram mahasiswa, terus meningkat seiring dengan pertumbuhan pengguna aktif media sosial dan rendahnya kesadaran keamanan digital. *Data warehouse* digital pribadi berupa akun media sosial kini menjadi sasaran empuk bagi peretas yang memanfaatkan kelemahan perilaku pengguna.

Mahasiswa umumnya belum memahami sepenuhnya pentingnya menjaga keamanan akun, baik melalui autentikasi dua faktor, pengelolaan kata sandi, maupun deteksi aktivitas mencurigakan. Oleh karena itu, pemahaman tentang keamanan siber perlu ditanamkan sejak dini**,** baik melalui kurikulum pendidikan tinggi maupun kampanye digital nasional. Dengan demikian, mahasiswa tidak hanya menjadi pengguna teknologi, tetapi juga agen yang berperan aktif dalam membangun ekosistem digital yang aman dan beretika.

Daftar Pustaka

Adinda Nova Octavia *Et Al.* (2025) 'Peran Pemahaman Cyber Security Untuk Keamanan Akun Media Sosial Instagram Mahasiswa', *Orbit : Jurnal Ilmu Multidisiplin Nusantara*, 1(2), Pp. 89–99. Doi: 10.63217/Orbit.V1i2.80.

Devananta, A. (2021) 'Implikasi Cybercrime Pada Bisnis Digital Di Indonesia', *Jurnal Litbang Polri*, 24(3), Pp. 139–146. Doi: 10.46976/.V24i3.157.

Hapsari, R. D. And Pambayun, K. G. (2023) 'Ancaman Cybercrime Di Indonesia: Sebuah Tinjauan Pustaka Sistematis', *Jurnal Konstituen*, 5(1), Pp. 1–17. Doi: 10.33701/Jk.V5i1.3208.

Kurniawan, Y. *Et Al.* (2023) 'Analysis Of Higher Education Students' Awareness In Indonesia On Personal Data Security In Social Media', *Sustainability (Switzerland)*, 15(4). Doi: 10.3390/Su15043814.

Mouncey, E. And Ciobotaru, S. (2025) 'Phishing Scams On Social Media: An Evaluation Of Cyber Awareness Education On Impact And Effectiveness', *Journal Of Economic Criminology*. Elsevier, 7(October 2024), P. 100125. Doi: 10.1016/J.Jeconc.2025.100125.

Nabila Aulia Agustin And Refania Meilani Firdos (2024) 'Studi Literatur : Ancaman Cybercrime Di Indonesia Dan Pentingnya Pemahaman Akan Fenomena Kejahatan Digital', *Jurnal Mahasiswa Teknik Informatika*, 3(1), Pp. 126–131. Doi: 10.35473/Jamastika.V3i1.2841.

Razak, N. A. *Et Al.* (2022) 'A Comprehensive Study Of Privacy And Security Risk Awareness Among Mobile Internet Users For Social Networks Sites In Malaysia', *International Journal Of Business And Technology Management*, 3(1), Pp. 2682–7646. Available At: Http://Myjms.Mohe.Gov.My/Index.Php/Ijbtm.

Reuben, N. *Et Al.* (2023) 'Raising Cyber Security Awareness To Reduce Social Engineering Through Social Media In Indonesia', *Proceedings - 2023 3rd International Conference On Electronic And Electrical Engineering And Intelligent System: Responsible Technology For Sustainable Humanity, Ice3is 2023*, (August 2023), Pp. 138–141. Doi: 10.1109/Ice3is59323.2023.10335454.

Soesanto, E. *Et Al.* (2023) 'Analisis Dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman Dan Solusi Dalam Lingkungan Digital Untuk Mengamankan Objek Vital Dan File', *Sammajiva: Jurnal Penelitian Bisnis Dan Manajemen*, 1(2), Pp. 172–191.

Tobondo, Y. A. *Et Al.* (2024) 'Analysis Of Cybersecurity Implementation In Indonesia Based On The Framework Of Administrative Law', *Interdisciplinary Journal (Ide)*, 2(2), Pp. 83–94. Doi: 10.61254/Idejournal.V2i2.55.

Vera, N., Morisrona, M. And Nurohman, H. A. (2024) 'Keamanan Informasi Pada Media Sosial Instagram', *Seminar Nasional Teknologi Informasi Dan Bisnis (Senatib) 2024*, Pp. 511–517.