JURNAL KOMPREHENSIF
E ISSN: 3031-0970 | Vol. 4 No. 1 2026 | pp. 741-755
Available online at: https://ejournal.edutechjaya.com/index.php/komprehensif

Analisis Keamanan Akun Instagram Mahasiswa Terhadap Ancaman *Phishing*

Vinna Olymphyani[1], Anggi Putri Khatami Simbolon[2], Gilang Kurnia Rambe[3], Ridwan Hafiz Ritonga[4], Sahat Parulian Sitorus[5]

[1,2,3,4,5]Universitas Labuhanbatu, Indonesia

Email: vinnaolymphyani07@gmail.com

ABSTRAK

Perkembangan penggunaan media sosial, khususnya Instagram, di kalangan mahasiswa telah meningkatkan risiko terjadinya berbagai ancaman keamanan siber, salah satunya *phishing*. Penelitian ini bertujuan untuk menganalisis tingkat keamanan akun Instagram mahasiswa terhadap ancaman *phishing* dengan meninjau aspek pengetahuan *phishing*, kemampuan mengenali tautan mencurigakan, kesadaran keamanan digital, penggunaan kata sandi yang kuat, autentikasi dua faktor (2FA), dan perlindungan data pribadi. Metode penelitian yang digunakan adalah kuantitatif deskriptif dengan pengumpulan data melalui kuesioner berbasis skala Likert yang disebarkan kepada mahasiswa pengguna Instagram. Data dianalisis menggunakan statistik deskriptif untuk mengukur tingkat keamanan akun dan tingkat kerentanan terhadap *phishing*. Hasil penelitian menunjukkan bahwa bentuk ancaman *phishing* yang paling sering ditemukan meliputi pesan palsu, tautan *phishing*, akun tiruan, dan penawaran hadiah palsu. Tingkat keamanan akun mahasiswa berada pada kategori tinggi sebesar 42%, kategori sedang sebesar 38%, dan kategori rendah sebesar 20%. Selain itu, ditemukan hubungan berbanding terbalik antara tingkat keamanan akun dan risiko menjadi korban *phishing*. Semakin baik penerapan praktik keamanan digital, semakin rendah risiko serangan *phishing*. Penelitian ini menyimpulkan bahwa peningkatan literasi keamanan digital dan pemanfaatan fitur keamanan akun secara optimal sangat penting untuk melindungi akun Instagram mahasiswa dari ancaman *phishing*.
Kata Kunci: Instagram, Keamanan Akun, *Phishing*, Keamanan Digital, Mahasiswa.

ABSTRACT

The rapid growth of social media usage, particularly Instagram, among university students has increased the risk of cybersecurity threats, especially phishing attacks. This study aims to analyze the security of students' Instagram accounts against phishing threats by examining several factors, including phishing awareness, the ability to identify suspicious links, digital security awareness, strong password usage, Two-Factor Authentication (2FA), and personal data protection. The research employed a descriptive quantitative approach, with data collected through a Likert-scale questionnaire distributed to active Instagram users among university students. The collected data were analyzed using descriptive statistical methods to assess account security levels and vulnerability to phishing attacks. The findings reveal that the most common forms of phishing threats include fake direct messages, phishing links, fake accounts, and fraudulent giveaway offers. The results indicate that 42% of respondents have a high level of account security, 38% fall into the moderate category, and 20% are categorized as having low account security. Furthermore, an inverse relationship was identified between account security levels and the risk of becoming a phishing victim. The better the implementation of digital security practices, the lower the risk of phishing attacks. This study concludes that improving digital security literacy and optimizing the use of account security features are essential measures for protecting students' Instagram accounts from phishing threats.
Keywords: Instagram, Account Security, Phishing, Digital Security, University Students.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan yang signifikan dalam berbagai aspek kehidupan masyarakat. Kemajuan internet dan teknologi digital memungkinkan individu untuk berkomunikasi, memperoleh informasi, melakukan transaksi, serta berinteraksi tanpa dibatasi oleh ruang dan waktu. Di era digital saat ini, penggunaan media sosial menjadi salah satu aktivitas yang paling dominan dalam kehidupan sehari-hari. Media sosial tidak hanya berfungsi sebagai sarana komunikasi, tetapi juga digunakan untuk kegiatan pendidikan, bisnis, hiburan, pemasaran, serta pengembangan identitas digital pengguna. Seiring dengan meningkatnya ketergantungan masyarakat terhadap teknologi digital, muncul berbagai tantangan baru yang berkaitan dengan keamanan informasi dan perlindungan data pribadi pengguna (Satrio & Syafaat, 2025).

Salah satu platform media sosial yang memiliki tingkat penggunaan tinggi adalah Instagram. Platform ini memungkinkan pengguna untuk berbagi foto, video, pesan, maupun berbagai bentuk informasi lainnya secara cepat dan mudah. Di kalangan mahasiswa, Instagram telah menjadi bagian penting dari aktivitas sehari-hari karena digunakan untuk berkomunikasi, membangun jaringan pertemanan, mengikuti perkembangan informasi, mendukung kegiatan akademik, hingga membangun personal branding. Tingginya intensitas penggunaan Instagram menyebabkan platform ini menyimpan berbagai informasi penting milik pengguna, seperti alamat email, nomor telepon, foto pribadi, lokasi, riwayat aktivitas, dan berbagai data lainnya yang memiliki nilai bagi pihak-pihak yang tidak bertanggung jawab. Kondisi tersebut menjadikan Instagram sebagai salah satu target yang menarik bagi pelaku kejahatan siber (Amanda Ardelia et al., 2024).

Peningkatan penggunaan media sosial secara masif juga diikuti dengan meningkatnya berbagai ancaman keamanan siber (*cybersecurity threats*). Ancaman tersebut meliputi pencurian identitas, peretasan akun, penyalahgunaan data pribadi, penyebaran malware, hingga serangan *phishing*. Berbeda dengan serangan yang memanfaatkan kelemahan teknis pada sistem, sebagian besar serangan modern justru memanfaatkan kelemahan manusia sebagai target utama. Oleh karena itu, keamanan akun media sosial tidak hanya bergantung pada teknologi yang digunakan oleh penyedia layanan, tetapi juga dipengaruhi oleh tingkat kesadaran, pengetahuan, dan perilaku pengguna dalam menjaga keamanan akun mereka (Adinda Nova Octavia et al., 2025).

Phishing merupakan salah satu bentuk kejahatan siber yang paling sering digunakan untuk memperoleh informasi sensitif milik korban. *Phishing* dilakukan dengan cara menyamar sebagai pihak yang terpercaya untuk meyakinkan korban agar memberikan informasi penting seperti nama pengguna (*username*), kata sandi (*password*), kode verifikasi, maupun data pribadi lainnya. Serangan *phishing* dapat dilakukan melalui berbagai media, seperti email, pesan singkat, aplikasi perpesanan, maupun media sosial. Dalam konteks Instagram, pelaku *phishing* sering menggunakan akun palsu, pesan langsung (*direct message*), tautan berbahaya, atau halaman login

tiruan yang menyerupai tampilan resmi Instagram. Ketika korban memasukkan informasi login pada halaman palsu tersebut, data akan langsung dikirim kepada pelaku dan digunakan untuk mengambil alih akun korban (Arisanty et al., 2025).

Keberhasilan serangan *phishing* sangat erat kaitannya dengan teknik *social engineering* atau rekayasa sosial. Teknik ini memanfaatkan aspek psikologis manusia, seperti rasa percaya, rasa penasaran, ketakutan, maupun rasa urgensi, untuk memengaruhi korban agar melakukan tindakan tertentu. Pelaku sering kali mengirimkan pesan yang mengatasnamakan pihak resmi, menawarkan hadiah, memberikan peringatan keamanan akun, atau menginformasikan adanya pelanggaran kebijakan sehingga korban terdorong untuk segera mengakses tautan yang diberikan. Karena serangan *phishing* lebih banyak mengeksploitasi perilaku manusia dibandingkan kelemahan teknologi, maka tingkat kesadaran dan literasi keamanan digital menjadi faktor yang sangat menentukan keberhasilan maupun kegagalan serangan tersebut(Muammar et al., 2026).

Mahasiswa merupakan salah satu kelompok yang memiliki tingkat aktivitas digital yang sangat tinggi. Sebagian besar kegiatan akademik maupun non-akademik dilakukan melalui perangkat digital dan internet, mulai dari komunikasi, pembelajaran daring, penggunaan sistem informasi akademik, hingga interaksi melalui media sosial. Tingginya intensitas penggunaan teknologi menyebabkan mahasiswa memiliki peluang yang lebih besar untuk terpapar berbagai ancaman siber. Meskipun termasuk generasi yang dekat dengan teknologi (*digital native*), berbagai penelitian menunjukkan bahwa masih banyak mahasiswa yang belum menerapkan praktik keamanan digital secara optimal. Perilaku seperti penggunaan kata sandi yang lemah, penggunaan kata sandi yang sama pada beberapa akun, penyimpanan informasi login secara tidak aman, serta tidak mengaktifkan autentikasi dua faktor (*Two-Factor Authentication* atau 2FA) masih sering ditemukan di kalangan mahasiswa. Kondisi ini dapat meningkatkan risiko pencurian akun dan penyalahgunaan data pribadi(Dias Sulistyo et al., 2024).

Selain itu, beberapa penelitian menunjukkan bahwa terdapat kesenjangan antara tingkat kesadaran keamanan digital dan perilaku keamanan yang diterapkan oleh mahasiswa. Sebagian besar mahasiswa telah mengetahui adanya ancaman *phishing* dan memahami pentingnya menjaga keamanan akun digital. Namun, dalam praktiknya masih banyak pengguna yang tetap mengklik tautan mencurigakan, mengabaikan peringatan keamanan, atau tidak memanfaatkan fitur keamanan tambahan yang tersedia. Penelitian mengenai ancaman *phishing* pada generasi muda menunjukkan bahwa mayoritas responden pernah menerima pesan atau tautan yang mencurigakan melalui media sosial. Meskipun tingkat kesadaran terhadap ancaman *phishing* tergolong tinggi, penerapan tindakan pencegahan seperti penggantian kata sandi secara berkala dan penggunaan autentikasi dua faktor masih belum dilakukan secara konsisten. Temuan ini menunjukkan bahwa pengetahuan yang dimiliki pengguna belum sepenuhnya diterapkan dalam bentuk perilaku keamanan yang nyata(Putri Nugroho et al., 2024).

Literasi digital menjadi salah satu faktor penting dalam membentuk perilaku keamanan pengguna. Mahasiswa yang memiliki tingkat literasi digital yang baik cenderung lebih mampu mengenali karakteristik *phishing*, memverifikasi keaslian informasi, memahami risiko berbagi data pribadi, serta menerapkan langkah-langkah perlindungan akun secara lebih efektif. Sebaliknya, rendahnya literasi digital dapat menyebabkan pengguna lebih rentan terhadap berbagai bentuk manipulasi yang dilakukan oleh pelaku kejahatan siber. Oleh karena itu, peningkatan literasi digital tidak hanya berperan dalam meningkatkan kemampuan penggunaan teknologi, tetapi juga menjadi bagian penting dalam upaya perlindungan terhadap data dan akun digital pengguna(Saputra & Marpaung, 2023).

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk menganalisis keamanan akun Instagram mahasiswa terhadap ancaman *phishing* dengan meninjau aspek kesadaran keamanan digital, penggunaan fitur keamanan akun, perilaku perlindungan data pribadi, serta pengalaman mahasiswa dalam menghadapi serangan *phishing*. Hasil penelitian diharapkan dapat memberikan gambaran mengenai kondisi keamanan akun Instagram mahasiswa sekaligus menjadi dasar dalam penyusunan strategi edukasi dan peningkatan literasi keamanan digital di lingkungan perguruan tinggi guna meminimalkan risiko serangan *phishing* yang semakin berkembang di era digital(Vera & Nurohman, 2024).

METODE PENELITIAN

Penelitian ini merupakan penelitian kuantitatif dengan pendekatan deskriptif yang berfokus pada analisis tingkat keamanan akun Instagram mahasiswa terhadap ancaman *phishing*. Penelitian dilakukan untuk memperoleh gambaran mengenai tingkat kesadaran keamanan digital mahasiswa, penerapan praktik keamanan akun Instagram, serta kerentanan pengguna terhadap berbagai bentuk serangan *phishing* yang semakin berkembang di lingkungan media sosial. Pendekatan kuantitatif dipilih karena memungkinkan pengukuran tingkat keamanan akun dan perilaku pengguna secara objektif berdasarkan data yang diperoleh dari responden melalui instrumen penelitian berupa kuesioner.

Proses penelitian diawali dengan identifikasi permasalahan terkait meningkatnya ancaman *phishing* pada platform media sosial, khususnya Instagram, yang banyak digunakan oleh mahasiswa sebagai sarana komunikasi dan aktivitas digital sehari-hari. Tahap selanjutnya dilakukan studi literatur terhadap berbagai penelitian terdahulu yang membahas keamanan siber, keamanan media sosial, *phishing*, literasi digital, dan perilaku keamanan pengguna internet. Hasil kajian literatur digunakan sebagai dasar dalam penyusunan indikator penelitian yang mencakup pengetahuan tentang *phishing*, kemampuan mengenali tautan dan akun mencurigakan, kesadaran terhadap keamanan digital, perlindungan data pribadi, penggunaan kata sandi yang kuat, penggunaan autentikasi dua faktor (*Two-Factor Authentication*), serta pengaturan privasi akun Instagram.

Pengumpulan data dilakukan melalui penyebaran kuesioner secara daring menggunakan *Google Form* kepada mahasiswa yang aktif menggunakan Instagram. Instrumen penelitian disusun menggunakan skala Likert lima tingkat yang terdiri atas kategori Sangat Setuju, Setuju, Netral, Tidak Setuju, dan Sangat Tidak Setuju. Kuesioner dirancang untuk mengukur tingkat pemahaman responden terhadap ancaman *phishing* serta perilaku keamanan yang diterapkan dalam penggunaan akun Instagram. Selain itu, responden juga diminta memberikan informasi mengenai pengalaman mereka dalam menerima pesan mencurigakan, tautan *phishing*, maupun upaya pengambilalihan akun yang pernah dialami.

Data yang diperoleh kemudian melalui tahap editing, coding, dan tabulasi untuk memastikan kelengkapan serta konsistensi jawaban responden. Tahap editing dilakukan dengan memeriksa kesesuaian data yang masuk, sedangkan coding dilakukan dengan memberikan skor numerik pada setiap jawaban berdasarkan skala Likert yang digunakan. Selanjutnya, data ditabulasi dan diolah menggunakan teknik statistik deskriptif untuk memperoleh gambaran mengenai tingkat keamanan akun Instagram mahasiswa terhadap ancaman *phishing*.

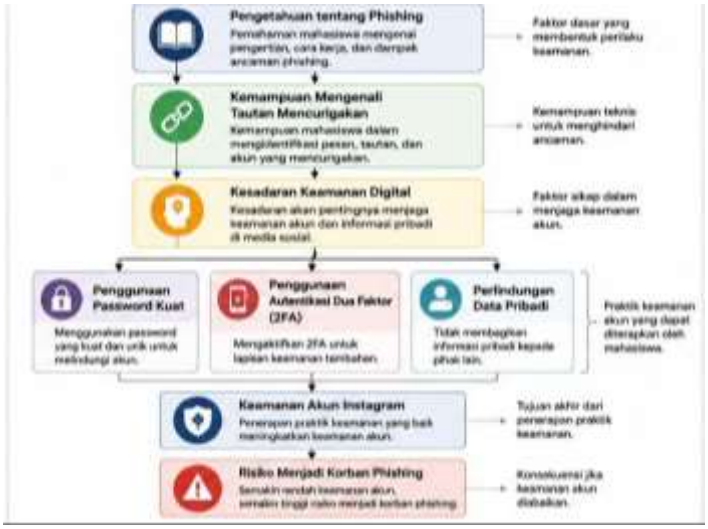
Analisis data dilakukan dengan menghitung skor setiap indikator penelitian dan mengubahnya ke dalam bentuk persentase untuk memudahkan interpretasi hasil. Hasil perhitungan kemudian diklasifikasikan ke dalam kategori tertentu guna menunjukkan tingkat keamanan akun Instagram mahasiswa, mulai dari kategori sangat rendah hingga sangat tinggi. Analisis juga difokuskan pada identifikasi faktor-faktor yang berpotensi meningkatkan kerentanan mahasiswa terhadap serangan *phishing*, seperti penggunaan kata sandi yang lemah, tidak mengaktifkan autentikasi dua faktor, kurangnya kewaspadaan terhadap tautan mencurigakan, serta rendahnya kesadaran dalam melindungi data pribadi.

Validasi hasil penelitian dilakukan melalui pemeriksaan konsistensi data responden dan kesesuaian antara indikator penelitian dengan tujuan penelitian yang telah ditetapkan. Evaluasi penelitian difokuskan pada kemampuan instrumen dalam menggambarkan kondisi keamanan akun Instagram mahasiswa secara objektif serta mengidentifikasi perilaku pengguna yang berpotensi meningkatkan risiko terjadinya *phishing*. Pendekatan ini memberikan dasar empiris untuk memahami tingkat keamanan akun Instagram mahasiswa sekaligus menghasilkan rekomendasi yang dapat digunakan sebagai upaya peningkatan literasi keamanan digital dan pencegahan serangan *phishing* di lingkungan perguruan tinggi.

JURNAL KOMPREHENSIF
E ISSN: 3031-0970 | Vol. 4 No. 1 2026 | pp. 741-755
Available online at: https://ejournal.edutechjaya.com/index.php/komprehensif

HASIL DAN PEMBAHASAN

Faktor-Faktor yang Mempengaruhi Keamanan Akun Instagram Mahasiswa



Gambar.1. Faktor-Faktor yang Mempengaruhi Keamanan Akun Instagram Mahasiswa

Berdasarkan Gambar 1, keamanan akun Instagram mahasiswa dipengaruhi oleh beberapa faktor yang saling berkaitan, yaitu pengetahuan tentang *phishing*, kemampuan mengenali tautan mencurigakan, kesadaran keamanan digital, penggunaan password yang kuat, penggunaan autentikasi dua faktor (*Two-Factor Authentication* atau 2FA), serta perlindungan data pribadi. Faktor-faktor tersebut membentuk perilaku keamanan digital yang berperan dalam menentukan tingkat keamanan akun Instagram mahasiswa terhadap ancaman *phishing*(Nurkhusnaedi, 2025).

Pengetahuan tentang *phishing* menjadi faktor dasar yang memengaruhi kemampuan mahasiswa dalam memahami berbagai bentuk serangan siber yang terjadi pada media sosial. Mahasiswa yang memiliki pemahaman mengenai pengertian, cara kerja, serta dampak *phishing* cenderung lebih waspada terhadap berbagai upaya penipuan yang dilakukan melalui pesan pribadi, tautan palsu, maupun akun tiruan. Pengetahuan yang baik memungkinkan pengguna untuk mengenali karakteristik serangan *phishing* sehingga dapat mengurangi kemungkinan menjadi korban pencurian data akun(Rifka Alkhilyatul Ma'rifat, I Made Suraharta, 2024).

Selain itu, kemampuan mengenali tautan mencurigakan juga menjadi faktor penting dalam menjaga keamanan akun Instagram. Mahasiswa yang mampu memeriksa alamat URL, memverifikasi sumber informasi, dan mengidentifikasi indikasi penipuan akan lebih mampu menghindari akses ke situs palsu yang dirancang untuk mencuri informasi login pengguna. Kemampuan ini sangat diperlukan mengingat sebagian besar serangan *phishing* dilakukan melalui penyebaran tautan yang menyerupai halaman resmi Instagram(Rifai et al., 2023).

Faktor berikutnya adalah kesadaran keamanan digital. Kesadaran ini mencerminkan pemahaman mahasiswa mengenai pentingnya menjaga keamanan akun dan melindungi informasi pribadi yang dimiliki. Mahasiswa yang memiliki tingkat kesadaran keamanan digital yang tinggi umumnya lebih berhati-hati dalam membagikan informasi pribadi, menerima permintaan pertemanan dari akun yang tidak dikenal, maupun mengakses tautan yang diterima melalui media sosial(Farida et al., 2023).

Dalam praktiknya, kesadaran keamanan digital diwujudkan melalui beberapa tindakan nyata, seperti penggunaan password yang kuat, aktivasi fitur autentikasi dua faktor (2FA), dan perlindungan data pribadi. Penggunaan password yang kuat dapat mengurangi risiko akun diretas melalui teknik penebakan kata sandi (*password guessing*) maupun serangan *brute force*. Sementara itu, penggunaan 2FA memberikan lapisan keamanan tambahan karena proses login tidak hanya memerlukan kata sandi, tetapi juga kode verifikasi yang dikirimkan kepada pemilik akun. Selain itu, perlindungan data pribadi dilakukan dengan membatasi informasi yang dibagikan kepada publik sehingga dapat meminimalkan peluang penyalahgunaan data oleh pelaku kejahatan siber(Akmal et al., 2026).

Berdasarkan hubungan antar faktor pada Gambar 1, dapat diketahui bahwa keamanan akun Instagram tidak hanya dipengaruhi oleh satu aspek tertentu, melainkan merupakan hasil dari kombinasi pengetahuan, kesadaran, dan perilaku keamanan pengguna. Semakin baik tingkat pemahaman mahasiswa mengenai *phishing* serta semakin konsisten penerapan praktik keamanan digital yang dilakukan, maka semakin tinggi tingkat keamanan akun Instagram yang dimiliki. Sebaliknya, rendahnya pemahaman mengenai *phishing*, penggunaan kata sandi yang lemah, tidak mengaktifkan fitur 2FA, serta kurangnya perlindungan terhadap data pribadi dapat meningkatkan risiko mahasiswa menjadi korban *phishing* dan berbagai bentuk kejahatan siber lainnya(Haya Nur Fadhilah, 2024).

Hasil ini sejalan dengan berbagai penelitian terdahulu yang menunjukkan bahwa literasi keamanan digital dan penerapan praktik keamanan akun memiliki peran penting dalam mengurangi kerentanan pengguna media sosial terhadap serangan *phishing*. Oleh karena itu, peningkatan edukasi mengenai *phishing* dan keamanan digital perlu dilakukan secara berkelanjutan agar mahasiswa mampu melindungi akun Instagram mereka dari berbagai ancaman yang terus berkembang di era digital(Naomira et al., 2024).

JURNAL KOMPREHENSIF
E ISSN: 3031-0970 | Vol. 4 No. 1 2026 | pp. 741-755
Available online at: https://ejournal.edutechjaya.com/index.php/komprehensif

Bentuk Ancaman *Phishing* Pada Instagram

Berdasarkan Gambar 2, ancaman *phishing* pada Instagram dapat muncul dalam berbagai bentuk dengan tujuan utama memperoleh informasi login dan data pribadi pengguna. Serangan *phishing* memanfaatkan teknik rekayasa sosial (*social engineering*) untuk memanipulasi korban agar memberikan informasi sensitif secara sukarela. Dalam penelitian ini, bentuk ancaman *phishing* yang paling umum ditemukan meliputi pesan palsu (*direct message*), tautan *phishing* (*phishing link*), akun tiruan (*fake account*), dan penawaran hadiah palsu (*fake giveaway*)(Ratnadewati & Oktarina, 2024).

Pesan palsu (*direct message*) merupakan salah satu metode yang sering digunakan oleh pelaku *phishing*. Modus ini dilakukan dengan mengirimkan pesan yang mengatasnamakan pihak resmi Instagram atau akun tertentu yang dianggap terpercaya. Pesan tersebut biasanya berisi pemberitahuan mengenai pelanggaran akun, verifikasi identitas, atau informasi bahwa akun pengguna akan dinonaktifkan apabila tidak segera melakukan tindakan tertentu. Kondisi ini sering dimanfaatkan pelaku untuk menciptakan rasa panik sehingga korban terburu-buru mengikuti instruksi yang diberikan tanpa melakukan verifikasi terlebih dahulu(Mellania, 2025).

Selain pesan palsu, pelaku juga sering menggunakan tautan *phishing* yang mengarahkan korban menuju halaman login palsu yang menyerupai tampilan resmi Instagram. Secara visual, halaman tersebut dibuat sangat mirip dengan halaman asli sehingga sulit dibedakan oleh pengguna yang kurang teliti. Ketika korban memasukkan *username* dan *password*, informasi tersebut secara otomatis tersimpan dan dikirimkan kepada pelaku. Metode ini menjadi salah satu teknik *phishing* yang paling efektif karena memanfaatkan kelengahan pengguna dalam memeriksa keaslian alamat situs yang diakses.

Ancaman lainnya adalah penggunaan akun tiruan (*fake account*). Pelaku membuat akun yang menyerupai akun resmi Instagram, akun publik figur, maupun akun milik teman korban. Melalui akun tersebut, pelaku dapat menghubungi korban dan membangun kepercayaan sebelum mengirimkan tautan berbahaya atau meminta

informasi tertentu. Tingginya tingkat kepercayaan terhadap akun yang terlihat familiar sering kali menyebabkan pengguna tidak menyadari bahwa mereka sedang berinteraksi dengan akun palsu.

Bentuk *phishing* yang juga banyak ditemukan adalah penawaran hadiah palsu (*fake giveaway*). Pelaku menawarkan hadiah, voucher, atau sejumlah uang dengan syarat tertentu, seperti mengklik tautan, mengisi formulir, atau memasukkan informasi akun Instagram. Modus ini memanfaatkan rasa penasaran dan ketertarikan korban terhadap hadiah yang ditawarkan. Meskipun terlihat sederhana, metode ini masih sering berhasil karena banyak pengguna yang kurang melakukan pengecekan terhadap keaslian penyelenggara giveaway tersebut(Hastuti et al., 2024).

Seluruh bentuk ancaman *phishing* tersebut pada akhirnya bermuara pada pencurian informasi login pengguna. Data yang berhasil diperoleh pelaku, seperti *username*, *password*, dan kode verifikasi, dapat digunakan untuk mengambil alih akun Instagram korban. Setelah akun berhasil dikuasai, pelaku dapat melakukan berbagai tindakan yang merugikan, seperti menyebarkan spam, melakukan penipuan atas nama korban, mencuri informasi pribadi, hingga memanfaatkan akun untuk melancarkan serangan *phishing* kepada pengguna lain.

Berdasarkan hasil analisis pada Gambar 2, dapat disimpulkan bahwa ancaman *phishing* pada Instagram tidak hanya bergantung pada kecanggihan teknologi yang digunakan pelaku, tetapi juga dipengaruhi oleh tingkat kewaspadaan pengguna dalam mengenali berbagai modus penipuan yang ada. Oleh karena itu, mahasiswa perlu meningkatkan pemahaman mengenai karakteristik *phishing*, membiasakan diri memverifikasi sumber informasi, serta menghindari memberikan informasi pribadi kepada pihak yang tidak dapat dipastikan keasliannya. Upaya tersebut penting dilakukan untuk meminimalkan risiko pencurian akun dan penyalahgunaan data pribadi di lingkungan media sosial.

Tingkat Keamamnan Akun Instagram Mahasiswa

Berdasarkan Gambar 3, tingkat keamanan akun Instagram mahasiswa dikelompokkan ke dalam tiga kategori, yaitu tinggi, sedang, dan rendah. Hasil analisis

menunjukkan bahwa sebagian besar mahasiswa berada pada kategori keamanan tinggi sebesar 42%, diikuti kategori sedang sebesar 38%, dan kategori rendah sebesar 20%. Temuan ini menunjukkan bahwa mayoritas mahasiswa telah menerapkan beberapa praktik keamanan digital dalam penggunaan akun Instagram, meskipun masih terdapat sebagian pengguna yang belum menerapkan langkah-langkah keamanan secara optimal(Rapina & Albuchori, 2025).

Mahasiswa yang berada pada kategori keamanan tinggi umumnya telah menerapkan berbagai praktik keamanan digital yang baik, seperti menggunakan kata sandi yang kuat dan unik, mengaktifkan fitur autentikasi dua faktor (2FA), membatasi akses informasi pribadi melalui pengaturan privasi akun, serta memiliki kewaspadaan yang tinggi terhadap pesan atau tautan yang mencurigakan. Penerapan langkah-langkah tersebut mampu meningkatkan perlindungan akun dari berbagai bentuk serangan siber, khususnya *phishing* yang bertujuan mencuri informasi login pengguna (Al Gazali, 2025).

Pada kategori sedang yang mencapai 38%, mahasiswa telah menerapkan beberapa aspek keamanan akun, namun belum secara konsisten menjalankan seluruh praktik keamanan yang direkomendasikan. Sebagai contoh, sebagian pengguna telah menggunakan kata sandi yang cukup kuat tetapi belum mengaktifkan autentikasi dua faktor, atau telah mengaktifkan fitur keamanan tertentu tetapi masih kurang waspada terhadap pesan yang mengandung tautan mencurigakan. Kondisi ini menunjukkan bahwa meskipun tingkat kesadaran keamanan digital sudah cukup baik, masih diperlukan peningkatan pemahaman dan penerapan praktik keamanan secara menyeluruh(Sosial et al., 2026).

Sementara itu, sebanyak 20% mahasiswa berada pada kategori keamanan rendah. Kelompok ini cenderung memiliki kerentanan yang lebih tinggi terhadap ancaman *phishing* karena belum menerapkan langkah-langkah keamanan dasar secara optimal. Beberapa perilaku yang dapat meningkatkan risiko keamanan akun antara lain penggunaan kata sandi yang mudah ditebak, penggunaan kata sandi yang sama pada beberapa akun, tidak mengaktifkan autentikasi dua faktor, serta kurangnya perhatian terhadap keamanan informasi pribadi yang dibagikan melalui media sosial. Kondisi tersebut dapat memberikan peluang yang lebih besar bagi pelaku *phishing* untuk memperoleh akses tidak sah terhadap akun pengguna(Studi et al., 2025).

Hasil pada Gambar 3 menunjukkan bahwa meskipun sebagian besar mahasiswa telah memiliki tingkat keamanan akun yang cukup baik, masih terdapat kelompok pengguna yang memerlukan perhatian khusus dalam meningkatkan praktik keamanan digital mereka. Keberadaan kategori sedang dan rendah menunjukkan bahwa ancaman *phishing* tetap menjadi risiko yang perlu diwaspadai, terutama bagi pengguna yang belum menerapkan fitur keamanan secara maksimal.

Secara keseluruhan, hasil penelitian ini mengindikasikan bahwa tingkat keamanan akun Instagram mahasiswa tergolong cukup baik, namun masih diperlukan upaya peningkatan literasi keamanan digital melalui edukasi mengenai penggunaan kata sandi yang kuat, pentingnya autentikasi dua faktor, perlindungan

data pribadi, serta kemampuan mengenali berbagai bentuk serangan *phishing*. Dengan meningkatnya kesadaran dan penerapan praktik keamanan digital, risiko penyalahgunaan akun dan pencurian data pribadi dapat diminimalkan sehingga keamanan akun Instagram mahasiswa dapat terjaga dengan lebih baik(Dewanto et al., 2024).

Hubungan Tingkat Keamanan Akun dan Resiko *Phishing*

Berdasarkan Gambar 4, terdapat hubungan yang berbanding terbalik antara tingkat keamanan akun Instagram mahasiswa dengan risiko menjadi korban *phishing*. Semakin tinggi tingkat keamanan akun yang diterapkan oleh pengguna, maka semakin rendah risiko akun tersebut menjadi sasaran serangan *phishing*. Sebaliknya, semakin rendah penerapan praktik keamanan digital, maka semakin besar kemungkinan pengguna mengalami pencurian informasi login, pengambilalihan akun, maupun penyalahgunaan data pribadi oleh pihak yang tidak bertanggung jawab.

Mahasiswa yang berada pada kategori tingkat keamanan tinggi umumnya memiliki risiko *phishing* yang relatif rendah. Hal ini disebabkan oleh penerapan berbagai langkah keamanan, seperti penggunaan kata sandi yang kuat dan unik, aktivasi autentikasi dua faktor (2FA), pengaturan privasi akun yang baik, serta kemampuan mengenali pesan dan tautan yang mencurigakan. Pengguna dengan karakteristik tersebut cenderung lebih berhati-hati dalam menerima informasi yang masuk dan tidak mudah terpengaruh oleh berbagai bentuk manipulasi yang dilakukan pelaku *phishing*. Akibatnya, peluang keberhasilan serangan *phishing* menjadi lebih kecil(Miles, 2006).

Pada kategori keamanan sedang, risiko *phishing* masih berada pada tingkat menengah. Meskipun pengguna telah menerapkan beberapa langkah keamanan, masih terdapat celah yang dapat dimanfaatkan oleh pelaku. Sebagai contoh, pengguna mungkin telah menggunakan kata sandi yang cukup kuat tetapi belum mengaktifkan autentikasi dua faktor, atau memiliki pemahaman mengenai *phishing* namun masih kurang teliti dalam memverifikasi keaslian tautan yang diterima.

Kondisi ini menunjukkan bahwa penerapan keamanan yang tidak konsisten dapat menyebabkan akun tetap rentan terhadap ancaman *phishing*.

Sementara itu, pengguna yang berada pada kategori keamanan rendah memiliki risiko *phishing* yang paling tinggi. Rendahnya tingkat keamanan biasanya ditandai dengan penggunaan kata sandi yang sederhana, penggunaan kata sandi yang sama pada beberapa akun, tidak mengaktifkan fitur keamanan tambahan, serta kurangnya kewaspadaan terhadap pesan atau tautan mencurigakan. Perilaku tersebut memberikan peluang yang lebih besar bagi pelaku untuk memperoleh akses terhadap akun Instagram pengguna melalui berbagai teknik *phishing* yang digunakan.

Hasil analisis ini menunjukkan bahwa keamanan akun Instagram tidak hanya bergantung pada fitur keamanan yang disediakan oleh platform, tetapi juga sangat dipengaruhi oleh perilaku dan kesadaran pengguna dalam menerapkan praktik keamanan digital. Pengetahuan mengenai *phishing*, kemampuan mengenali ancaman, serta kebiasaan menjaga kerahasiaan informasi pribadi menjadi faktor penting yang dapat mengurangi risiko serangan siber. Dengan kata lain, peningkatan literasi keamanan digital memiliki peran yang sangat besar dalam memperkuat perlindungan akun media sosial(Data et al., 2025).

Secara keseluruhan, Gambar 4 menegaskan bahwa penerapan langkah-langkah keamanan digital yang baik mampu menurunkan risiko menjadi korban *phishing* secara signifikan. Oleh karena itu, mahasiswa perlu meningkatkan kesadaran terhadap ancaman keamanan siber, memanfaatkan fitur keamanan yang tersedia, serta menerapkan perilaku digital yang lebih aman agar akun Instagram yang dimiliki dapat terlindungi dari berbagai bentuk serangan *phishing* yang terus berkembang di era digital saat ini.

KESIMPULAN

Berdasarkan hasil penelitian mengenai Analisis Keamanan Akun Instagram Mahasiswa terhadap Ancaman *Phishing*, dapat disimpulkan bahwa keamanan akun Instagram mahasiswa dipengaruhi oleh beberapa faktor utama, yaitu pengetahuan mengenai *phishing*, kemampuan mengenali tautan mencurigakan, kesadaran keamanan digital, penggunaan kata sandi yang kuat, penggunaan autentikasi dua faktor (2FA), serta kemampuan dalam melindungi data pribadi. Faktor-faktor tersebut memiliki peran yang saling berkaitan dalam membentuk tingkat keamanan akun pengguna terhadap berbagai ancaman siber, khususnya *phishing*.

Hasil penelitian menunjukkan bahwa *phishing* masih menjadi salah satu ancaman yang sering ditemukan pada platform Instagram. Bentuk serangan yang umum terjadi meliputi pesan palsu yang mengatasnamakan pihak tertentu, tautan *phishing*, akun tiruan, serta penawaran hadiah palsu yang bertujuan memperoleh informasi login dan data pribadi pengguna. Keberhasilan serangan *phishing* tidak hanya dipengaruhi oleh teknik yang digunakan pelaku, tetapi juga oleh tingkat kewaspadaan dan kesadaran pengguna dalam mengenali berbagai bentuk ancaman yang ada.

Selain itu, tingkat keamanan akun Instagram mahasiswa menunjukkan bahwa masih terdapat perbedaan dalam penerapan praktik keamanan digital. Sebagian mahasiswa telah menerapkan langkah-langkah keamanan yang baik, seperti penggunaan kata sandi yang kuat, aktivasi autentikasi dua faktor, serta pengaturan privasi akun. Namun, masih terdapat pengguna yang belum memanfaatkan fitur keamanan tersebut secara optimal sehingga memiliki tingkat kerentanan yang lebih tinggi terhadap ancaman *phishing*.

Penelitian ini juga menunjukkan adanya hubungan antara tingkat keamanan akun dengan risiko menjadi korban *phishing*. Semakin baik praktik keamanan digital yang diterapkan oleh pengguna, maka semakin rendah risiko akun menjadi sasaran serangan *phishing*. Sebaliknya, rendahnya penerapan keamanan akun dapat meningkatkan peluang terjadinya pencurian informasi login, pengambilalihan akun, maupun penyalahgunaan data pribadi oleh pihak yang tidak bertanggung jawab.

Berdasarkan temuan tersebut, dapat disimpulkan bahwa peningkatan literasi keamanan digital, pemahaman mengenai *phishing*, serta penerapan fitur keamanan akun secara optimal merupakan langkah penting dalam meningkatkan keamanan akun Instagram mahasiswa. Oleh karena itu, diperlukan upaya edukasi dan sosialisasi yang berkelanjutan mengenai keamanan siber agar mahasiswa mampu mengenali, mencegah, dan menghadapi berbagai ancaman *phishing* yang terus berkembang di era digital saat ini.

DAFTAR PUSTAKA

Adinda Nova Octavia, Achmad Fauzi, Gilang Aditya Kurniawan, Nazwa Febriyana Putri, Rama Dwi Alghifari, Rasim Rasim, Sumarno Manrejo, & Yusrina Mutiara Adienda. (2025). Peran Pemahaman Cyber Security untuk Keamanan Akun Media Sosial Instagram Mahasiswa. *Orbit : Jurnal Ilmu Multidisiplin Nusantara*, *1*(2), 89–99. https://doi.org/10.63217/orbit.v1i2.80

Akmal, S., Andari, Z. D., Dahlawi, M. W., Salsabila, M., & Ramadhan, R. (2026). Analisis Penerapan Keamanan Berlapis melalui Autentikasi Dua Faktor dalam Melindungi Privasi Komunikasi Digital pada Platform Media Sosial Instagram. *JIKUM: Jurnal Ilmu Komputer*, *2*(1), 74–79. https://doi.org/10.62671/jikum.v2i1.176

Al Gazali, B. K. A. S. A. (2025). Pengukuran Tingkat Kesadaran Keamanan Data Pribadi Mahasiswa Menggunakan Metode HAIS-Q. *JIPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)*, *10*(4), 3740–3748.

Amanda Ardelia, A., Rihadatul 'Aisy, Q. A., & Santikasari. (2024). Analisis Keamanan dan Privasi Data Instagram Terhadap Ancaman *Phishing* di Era Digital. *Seminar Nasional Teknologi Informasi Dan Bisnis (SENATIB)*, 18–2024.

Arisanty, M., Riady, Y., Anastassia, S., Kharis, A., Permatasari, S. M., Sukatmi, S., Perpustakaan, S. I., Hukum, F., Terbuka, U., Matematika, P. S., Terbuka, U., Statitstika, P. S., Terbuka, U., Studi, P., Anak, P., & Dini, U. (2025). Cerdas Dan Aman Bermedia Digital : Peningkatan. *Jurnal Abdimas Patikala*, *4*(4), 1407–1418.

Data, P., Kampanye, D., & Don, V. (2025). *Analisis resepsi khalayak terhadap pesan edukasi perlindungan data dalam kampanye video*.

Dewanto, M. A. B., Fathurrahman, M., Firdaus, D. R., & Setiawan, A. (2024). Penipuan Penambah Followers Instagram: Analisis Serangan Phising dan Dampaknya pada Keamanan Data. *Journal of Internet and Software Engineering*, *1*(4), 11. https://doi.org/10.47134/pjise.v1i4.2672

Dias Sulistyo, A., Dwi Wicaksono, B., Nur Saputra, R., & Ramadhani, R. (2024). Strategi Penanggulangan Serangan *Phishing* di Media Sosial. *Seminar Nasional Teknologi Informasi Dan Bisnis (SENATIB)*, 18–2024.

Farida, N., Bakhtiar, A., & Rif'at, M. (2023). Analisis kesadaran keamanan informasi dan privasi pengguna Instagram. *Jurnal Informatika Dan Sistem Informasi*, 415–420. https://jurnal.uisu.ac.id/index.php/informasi/article/view/7803

Hastuti, P. T., Fitriandra, B., & Lestari, S. (2024). Kesadaran dan Perlindungan Privasi dalam Penggunaan Media Sosial | Prosiding Seminar Nasional Teknologi Informasi dan Bisnis. *Prosiding Seminar Nasional Teknologi Informasi Dan Bisnis (SENATIB)*, 518–523. https://ojs.udb.ac.id/Senatib/article/view/4641

Haya Nur Fadhilah. (2024). Membangun Komunitas Literat Di Era Digital Analisis Kinerja @oyusep Di Instagram. *Literasi : Jurnal Kajian Keislaman Multi-Perspektif*, *5*(1), 47–69. https://doi.org/10.22515/literasi.v5i1.10961

Mellania, P. (2025). Analisis Kampanye Tentang Doxing Dalam Upaya Menjaga Data Pribadi Di Media Sosial. *Sintesa*, *4*(01), 158–182. https://doi.org/10.30996/sintesa.v4i01.12656

Miles, A. (2006). *Old Media Avatars*. *2020*, 1–49.

Muammar, Y., Azizah, M., Sari, M. B., & Hafizah, H. (2026). *Studi Keamanan Akun Media Sosial Mahasiswa Terhadap Serangan Phising Berbasis Social Engineering*. *2*(2), 144–148.

Naomira, A. D., Soesanto, E., & Vilani, L. (2024). Implementasi Nilai-Nilai Kebangsaan Bersumber UUD 45 dan NKRI Pada Peran Manajemen Sekuriti Guna Meningkatkan Kesadaran , Keamanan Data Pribadi Media Sosial Instagram. *Jurnal Media Hukum Indonesia (MHI)*, *2*(2), 114–121.

Nurkhusnaedi, R. A. (2025). Tugas Akhir. *175.45.187.195*, 162. ftp://175.45.187.195/Titipan-Files/BAHAN WISUDA PERIODE V 18 MEI 2013/FULLTEKS/PD/lovita meika savitri (0710710019).pdf

Putri Nugroho, F. N., Listanto, M. F., Amelia, N., & Annisa, S. (2024). Analisis Kebocoran Data Pribadi Dalam Media Sosial. *Fibonacci : Jurnal Ilmu Ekonomi, Manajemen Dan Keuangan*, *1*(2), 58–65. https://doi.org/10.63217/fibonacci.v1i2.70

Rapina, & Albuchori, I. F. (2025). Analisis Risiko Keamanan Data Pribadi Pada Penggunaan Media Sosial Instagram Dengan Menggunakan Metode DREAD. *Jurnal Sains, Nalar, Dan Aplikasi Teknologi Informasi*, *4*(2), 149–156. https://doi.org/10.20885/snati.v4.i2.40362

Ratnadewati, D. Y., & Oktarina, R. V. (2024). Pengaruh Kesadaran Keamanan Informasi terhadap Pengguna Media Sosial Instagram. *Seminar Nasional*

Teknologi Informasi Dan Bisnis (SENATIB) 2024, 442–448.

Rifai, A., Meliyani, A., Chyntia, P., & Sakti, I. A. (2023). Penerapan Metode Technology Threat Avoidance Theory Terhadap Tingkat Kesadaran Data Privasi Pengguna Media Sosial. *Journal of Information System Research (JOSH)*, *4*(3), 1026–1032. https://doi.org/10.47065/josh.v4i3.3081

Rifka Alkhilyatul Ma'rifat, I Made Suraharta, I. I. J. (2024). *No Title 済無No Title No Title No Title*. *2*, 306–312.

Saputra, D., & Marpaung, Z. A. (2023). Analisis Yuridis Penanggulangan Penyalahgunaan Data Pribadi Dalam Bentuk Phising Yang Dilakukan Oleh Paid Verified Account Di Media Sosial Menurut Undang-Undang Perlindungan Data Pribadi. *Uneslaw Review*, *5*(4), 4764–4775.

Satrio, A. A., & Syafaat, A. (2025). *Perilaku Mahasiswa dalam Menjaga Keamanan Akun Digital di Era Siber : Studi Literatur Pendahuluan Kajian Teori*. *xx*(xx).

Sosial, M., Kasus, S., Smk, S., & Asam, B. (2026). *Analisis evaluasi tingkat literasi keamanan*. *11*(1), 408–415.

Studi, P., Informasi, S., & Labuhanbatu, U. (2025). *1,2,3,4*. *6*(November), 6–10.

Vera, N., & Nurohman, H. A. (2024). Keamanan Informasi pada Media Sosial Instagram. *Seminar Nasional Teknologi Informasi Dan Bisnis (SENATIB) 2024*, 511–517.

Wijiastuti, P., Azahro, H., & Edward, A. (2025). Analisis Kesadaran Ancaman Phising di Social Media Terhadap Gen Z di Indonesia. *Jurnal Informatika Utama*, *3*(1), 82–93.