JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Studi Keamanan Akun Media Sosial Mahasiswa Terhadap Serangan Phising Berbasis Social Engineering

Yasir Muammar[1], Juliana[2*], Maila Azizah[3], Maita Berliana Sari[4], Hafifatul Hafizah[5], Khairunnisa[6]
[1,2,3,4,5,6]Universitas Malikussaleh, Indonesia
[1]yasir.240170072@mhs.unimal.ac.id

ABSTRACT

The massive use of social media among university students provides convenience in communication, information exchange, and academic activities. However, this condition also increases the risk of cybercrime, particularly phishing attacks based on social engineering. Phishing exploits psychological manipulation to deceive victims into revealing sensitive information such as passwords, OTP codes, and personal data. This study aims to analyze students' awareness of social media account security, identify common forms of phishing attacks experienced, and determine factors contributing to students' vulnerability. This research employs a quantitative descriptive method by distributing online questionnaires to active university students. The collected data were analyzed using descriptive statistics to identify behavioral patterns and security awareness levels. The results indicate that most students have moderate to low digital security awareness, reflected in password reuse across platforms and low adoption of two-factor authentication. Furthermore, most respondents have encountered phishing messages in the form of fake links, prize scams, and account verification requests. The main vulnerability factors include limited cybersecurity literacy, high levels of trust, and lack of information verification. This study highlights the importance of digital security education and improved cybersecurity literacy among students to reduce the risk of social engineering-based phishing attacks.

***Keywords**: account security, social media, students, phishing, social engineering*

PENDAHULUAN

Media sosial telah menjadi bagian tak terpisahkan dari kehidupan mahasiswa. Platform seperti Instagram, WhatsApp, X (Twitter), Facebook, dan TikTok digunakan tidak hanya sebagai sarana bersosialisasi, tetapi juga untuk mendukung kegiatan akademik dan organisasi kemahasiswaan. Intensitas penggunaan media sosial yang tinggi menjadikan mahasiswa sebagai salah satu kelompok pengguna digital yang paling aktif.

Namun, tingginya aktivitas tersebut juga meningkatkan risiko terjadinya kejahatan siber, khususnya serangan phishing berbasis social engineering. Phishing merupakan teknik penipuan yang bertujuan memperoleh informasi sensitif, seperti kata sandi, kode One-Time Password (OTP), dan data pribadi, dengan menyamar sebagai pihak yang tepercaya. Sementara itu, social engineering memanfaatkan aspek psikologis korban, seperti rasa percaya, ketakutan, atau kondisi mendesak, untuk memengaruhi korban agar secara sukarela memberikan informasi rahasia.

Rendahnya tingkat kesadaran keamanan digital di kalangan mahasiswa dapat menyebabkan berbagai kerugian, baik materiil maupun non-materiil, seperti pencurian identitas, pengambilalihan akun media sosial, serta penyalahgunaan data pribadi. Oleh karena itu, diperlukan kajian yang mendalam mengenai tingkat kesadaran keamanan akun media sosial mahasiswa serta pengalaman mereka terhadap serangan phishing berbasis social engineering sebagai upaya pencegahan dan peningkatan literasi keamanan siber.

TINJAUAN PUSTAKA

Keamanan Akun Media Sosial

Keamanan akun media sosial merupakan upaya perlindungan terhadap akun pengguna dari akses tidak sah, penyalahgunaan data, pencurian identitas, serta berbagai bentuk kejahatan siber lainnya. Keamanan ini mencakup penerapan kata sandi yang kuat, pengelolaan pengaturan privasi, serta kewaspadaan pengguna terhadap aktivitas mencurigakan. Krombholz et al. (2015) menyatakan bahwa tingkat keamanan akun sangat bergantung pada perilaku pengguna sebagai faktor utama dalam sistem keamanan informasi.

Dalam konteks mahasiswa, keamanan akun media sosial menjadi hal yang sangat penting karena akun tersebut sering terhubung dengan data pribadi, jaringan pertemanan, serta aktivitas akademik dan organisasi kemahasiswaan. Kerentanan akun media sosial dapat berdampak pada penyalahgunaan identitas digital dan gangguan terhadap aktivitas akademik.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Phishing

Phishing merupakan teknik penipuan yang dilakukan dengan menyamar sebagai pihak tepercaya dengan tujuan memperoleh informasi sensitif korban, seperti kata sandi, kode One-Time Password (OTP), dan data pribadi. Serangan phishing umumnya dilakukan melalui email, pesan singkat, media sosial, maupun situs web palsu yang dirancang menyerupai platform resmi.

Menurut Al-Qurishi et al. (2020), phishing termasuk salah satu bentuk kejahatan siber yang paling sering terjadi karena relatif mudah dilakukan dan memiliki tingkat keberhasilan yang tinggi, terutama jika dikombinasikan dengan teknik manipulasi psikologis terhadap korban.

Social Engineering

Social engineering merupakan teknik manipulasi psikologis yang bertujuan memengaruhi korban agar secara sukarela memberikan informasi rahasia. Teknik ini memanfaatkan kelemahan manusia, seperti rasa percaya, ketakutan, rasa ingin tahu, atau kondisi mendesak. Dalam praktiknya, social engineering sering dikombinasikan dengan serangan phishing untuk meningkatkan efektivitas dan tingkat keberhasilan serangan.

Penelitian Terdahulu

Beberapa penelitian terdahulu menunjukkan bahwa tingkat kesadaran keamanan siber di kalangan mahasiswa masih relatif rendah. Krombholz et al. (2015) menemukan bahwa faktor manusia merupakan titik terlemah dalam sistem keamanan informasi, sehingga menjadi sasaran utama dalam serangan social engineering. Penelitian lain oleh Al-Qurishi et al. (2020) menyimpulkan bahwa edukasi dan pelatihan keamanan siber dapat secara signifikan menurunkan tingkat keberhasilan serangan phishing serta meningkatkan kewaspadaan pengguna terhadap ancaman siber.

METODE PENELITIAN

Desain Penelitian

Penelitian ini menggunakan metode kuantitatif dengan pendekatan deskriptif. Pendekatan ini dipilih untuk memperoleh gambaran yang sistematis, objektif, dan faktual mengenai tingkat keamanan akun media sosial mahasiswa terhadap serangan phishing berbasis social engineering. Metode kuantitatif memungkinkan pengukuran tingkat kesadaran keamanan dan pengalaman mahasiswa secara objektif melalui data numerik yang dianalisis secara statistik.

Populasi dan Sampel Penelitian

Populasi dalam penelitian ini adalah seluruh mahasiswa aktif di perguruan tinggi. Teknik pengambilan sampel yang digunakan adalah *random sampling*, di mana setiap anggota populasi memiliki peluang yang sama untuk menjadi responden. Jumlah sampel dalam penelitian ini sebanyak 100 mahasiswa, yang dinilai telah mewakili populasi serta mencukupi untuk analisis statistik deskriptif.

Variabel Penelitian

Variabel yang digunakan dalam penelitian ini terdiri dari dua jenis, yaitu:

1. Variabel independen, yaitu tingkat kesadaran keamanan digital mahasiswa.
2. Variabel dependen, yaitu tingkat kerentanan akun media sosial terhadap serangan phishing berbasis social engineering.

Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui penyebaran kuesioner secara daring menggunakan platform digital. Kuesioner disusun dalam bentuk pertanyaan tertutup dengan skala Likert untuk mengukur tingkat kesadaran keamanan akun media sosial, kebiasaan penggunaan media sosial, serta pengalaman responden terkait serangan phishing. Selain itu, beberapa pertanyaan digunakan untuk mengidentifikasi jenis dan bentuk serangan phishing yang pernah dialami responden.

Instrumen Penelitian

Instrumen penelitian berupa kuesioner yang terdiri dari beberapa indikator, antara lain penggunaan kata sandi, penerapan autentikasi dua faktor, kewaspadaan terhadap tautan dan pesan mencurigakan, serta perilaku verifikasi informasi sebelum memberikan data pribadi. Instrumen penelitian disusun berdasarkan kajian pustaka yang relevan dan disesuaikan dengan konteks penggunaan media sosial di kalangan mahasiswa.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Teknik Analisis Data

Data yang diperoleh dianalisis menggunakan teknik statistik deskriptif, seperti persentase dan distribusi frekuensi. Teknik analisis ini bertujuan untuk menggambarkan tingkat kesadaran keamanan digital mahasiswa serta pola kerentanan akun media sosial terhadap serangan phishing berbasis social engineering. Hasil analisis disajikan dalam bentuk tabel, grafik, dan uraian deskriptif untuk memudahkan proses interpretasi.

HASIL DAN PEMBAHASAN

Karakteristik Responden

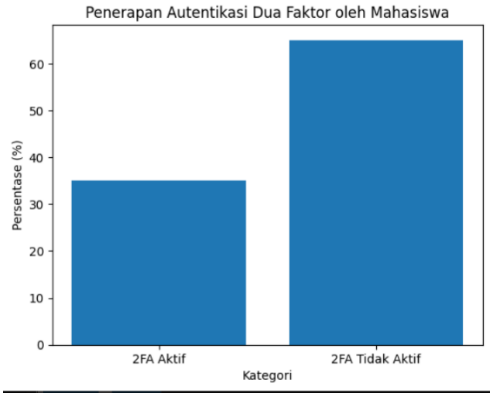
Penelitian ini melibatkan 100 mahasiswa aktif yang berasal dari berbagai program studi. Berdasarkan data demografis, responden terdiri dari 58% mahasiswa perempuan dan 42% mahasiswa laki-laki dengan rentang usia antara 18–23 tahun. Seluruh responden merupakan pengguna aktif media sosial dengan intensitas penggunaan lebih dari 3 jam per hari.

Tingginya intensitas penggunaan media sosial menunjukkan bahwa mahasiswa memiliki tingkat keterpaparan yang tinggi terhadap berbagai aktivitas digital, termasuk potensi ancaman keamanan siber. Kondisi ini menjadikan mahasiswa sebagai kelompok yang rentan terhadap serangan phishing berbasis social engineering.

Tingkat Kesadaran Keamanan Akun Media Sosial

Tingkat kesadaran keamanan akun media sosial mahasiswa dianalisis untuk mengetahui sejauh mana mahasiswa memahami dan menerapkan praktik keamanan digital dalam aktivitas daring sehari-hari. Kesadaran keamanan ini diukur melalui beberapa indikator utama, yaitu penggunaan kata sandi, penerapan autentikasi dua faktor, kewaspadaan terhadap tautan dan pesan mencurigakan, serta kebiasaan dalam menjaga kerahasiaan data pribadi.

Selain itu, hanya 35% responden yang telah mengaktifkan fitur autentikasi dua faktor (*two-factor authentication*), sedangkan 65% responden lainnya belum menerapkan fitur keamanan tambahan tersebut. Rendahnya penerapan autentikasi dua faktor mengindikasikan bahwa sebagian besar mahasiswa belum memanfaatkan mekanisme perlindungan akun yang lebih kuat.



Gambar 1. Tingkat Kesadaran Keamanan Akun Media Sosial

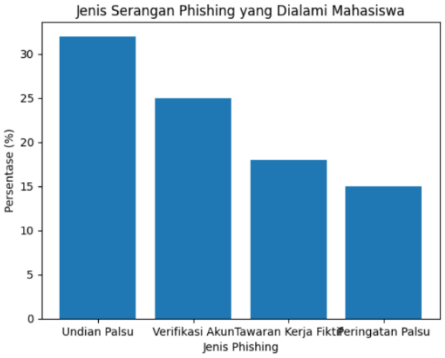
Pengalaman Mahasiswa terhadap Serangan Phishing

Pengalaman mahasiswa terhadap serangan phishing dianalisis untuk mengetahui tingkat paparan serta bentuk serangan yang paling sering dialami dalam penggunaan media sosial. Analisis ini penting untuk menggambarkan pola serangan phishing berbasis social engineering yang menyasar mahasiswa sebagai kelompok pengguna aktif media digital.

Berdasarkan hasil kuesioner, sebanyak 70% responden menyatakan pernah menerima pesan atau tautan yang terindikasi sebagai phishing. Pesan tersebut umumnya dikirim melalui media sosial dan aplikasi pesan instan dengan tampilan yang menyerupai akun atau layanan resmi. Temuan ini menunjukkan bahwa mahasiswa memiliki tingkat paparan yang cukup tinggi terhadap serangan phishing dalam aktivitas digital sehari-hari.

Jenis serangan phishing yang paling sering dialami mahasiswa adalah pesan undian atau hadiah palsu, yang dialami oleh 32% responden. Selain itu, 25% responden menerima pesan permintaan verifikasi akun dengan alasan keamanan, 18% responden mengalami tawaran kerja atau beasiswa fiktif, serta 15% responden menerima peringatan keamanan palsu yang mengancam penonaktifan akun apabila tidak segera melakukan tindakan tertentu. Bentuk-bentuk serangan ini dirancang untuk memanfaatkan rasa penasaran, kepercayaan, dan urgensi korban.

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026



Gambar 2. Pengalaman Mahasiswa terhadap Serangan Phishing

Peran Social Engineering dalam Keberhasilan Serangan Phishing

Hasil penelitian menunjukkan bahwa teknik social engineering memiliki peran yang sangat signifikan dalam meningkatkan keberhasilan serangan phishing terhadap mahasiswa. Sebagian besar responden menyatakan bahwa pesan phishing yang diterima tampak meyakinkan karena menggunakan bahasa formal, identitas visual yang menyerupai akun resmi, serta narasi yang dirancang untuk memanipulasi emosi korban.

Sebanyak 65% responden mengaku mengalami kesulitan dalam membedakan pesan phishing dengan pesan resmi, terutama ketika pesan tersebut menciptakan rasa urgensi. Teknik social engineering yang paling sering digunakan oleh pelaku adalah penciptaan kondisi darurat, seperti ancaman penonaktifan akun atau pembatasan akses apabila korban tidak segera melakukan verifikasi.

Selain itu, teknik iming-iming hadiah dan peluang tertentu, seperti undian berhadiah dan tawaran kerja, juga terbukti efektif dalam menarik perhatian mahasiswa. Kondisi ini menunjukkan bahwa faktor psikologis, seperti rasa takut kehilangan akses dan keinginan memperoleh keuntungan, dimanfaatkan secara optimal oleh pelaku kejahatan siber.

Mahasiswa yang memiliki tingkat kesadaran keamanan rendah cenderung lebih mudah terpengaruh oleh teknik social engineering. Hal ini diperparah oleh kebiasaan penggunaan media sosial yang tinggi dan kecenderungan untuk merespons pesan secara cepat tanpa melakukan verifikasi terlebih dahulu. Temuan ini sejalan dengan teori keamanan informasi yang menyatakan bahwa manusia merupakan titik terlemah dalam sistem keamanan siber.

Pembahasan

Hasil penelitian menunjukkan bahwa tingkat keamanan akun media sosial mahasiswa masih berada pada kategori sedang hingga rendah. Hal ini tercermin dari kebiasaan penggunaan kata sandi yang sama pada beberapa platform serta rendahnya penerapan autentikasi dua faktor. Kondisi tersebut mengindikasikan bahwa sebagian besar mahasiswa belum sepenuhnya memahami risiko keamanan digital yang dapat timbul dari perilaku penggunaan media sosial yang kurang aman.

Pengalaman mahasiswa terhadap serangan phishing juga menunjukkan tingginya tingkat paparan ancaman siber di lingkungan perguruan tinggi. Mayoritas responden pernah menerima pesan phishing dengan berbagai modus, seperti undian palsu, permintaan verifikasi akun, dan tawaran kerja fiktif. Modus tersebut dirancang secara persuasif dan memanfaatkan identitas visual yang menyerupai layanan resmi, sehingga sulit dibedakan oleh pengguna awam.

Peran social engineering terbukti sangat dominan dalam keberhasilan serangan phishing terhadap mahasiswa. Teknik manipulasi psikologis seperti penciptaan rasa urgensi, ancaman kehilangan akses akun, serta iming-iming keuntungan menjadi strategi utama pelaku dalam memengaruhi perilaku korban. Temuan ini memperkuat pandangan bahwa peningkatan keamanan digital tidak dapat hanya bergantung pada sistem teknologi, tetapi juga harus melibatkan peningkatan kesadaran, literasi keamanan siber, dan perubahan perilaku pengguna.

KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa tingkat kesadaran keamanan akun media sosial mahasiswa masih tergolong sedang hingga rendah. Hal ini tercermin dari kebiasaan penggunaan kata sandi yang sama pada beberapa akun media sosial, rendahnya penerapan autentikasi dua faktor, serta kurangnya kewaspadaan terhadap pesan dan tautan mencurigakan. Kondisi tersebut menyebabkan mahasiswa menjadi kelompok yang rentan terhadap serangan phishing berbasis social engineering.

Hasil penelitian juga menunjukkan bahwa mahasiswa memiliki tingkat paparan yang tinggi terhadap serangan phishing. Berbagai modus phishing, seperti undian palsu, permintaan verifikasi akun, tawaran kerja atau beasiswa fiktif, serta peringatan keamanan palsu, sering dialami oleh mahasiswa dalam aktivitas penggunaan media sosial. Teknik

social engineering terbukti efektif karena memanfaatkan faktor psikologis korban, seperti rasa percaya, urgensi, dan ketakutan kehilangan akses akun.

Selain itu, penelitian ini menunjukkan adanya hubungan yang jelas antara tingkat kesadaran keamanan digital dengan tingkat kerentanan terhadap serangan phishing. Mahasiswa yang menerapkan praktik keamanan digital yang baik cenderung lebih mampu mengenali dan menghindari serangan phishing, sedangkan mahasiswa dengan literasi keamanan siber yang rendah memiliki risiko lebih tinggi mengalami penyalahgunaan akun media sosial. Oleh karena itu, peningkatan kesadaran dan literasi keamanan siber menjadi faktor penting dalam meminimalkan risiko serangan phishing berbasis social engineering di kalangan mahasiswa.

REFERENSI

Al-Qurishi, M., Alrubaian, M., Alharthi, S., & Alhazmi, S. (2020). Social engineering attacks: Detection and prevention. *Journal of Information Security and Applications, 53*, 102-114. https://doi.org/10.1016/j.jisa.2020.102-114

APJII. (2022). *Laporan survei internet Indonesia 2022*. Jakarta: Asosiasi Penyelenggara Jasa Internet Indonesia.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 581–590). New York, NY: ACM. https://doi.org/10.1145/1124772.1124861

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31*(8), 983–988. https://doi.org/10.1016/j.cose.2012.08.004

Herley, C. (2012). Why do Nigerian scammers say they are from Nigeria? *WEIS Proceedings*, 1–9.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. Indianapolis, IN: Wiley Publishing.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly, 34*(4), 757–778.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373–382.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64–71. https://doi.org/10.1109/MC.2010.35

Sugiyono. (2019). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Bandung: Alfabeta.

Symantec. (2019). *Internet security threat report*. Mountain View, CA: Symantec Corporation.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability. *Decision Support Systems, 51*(3), 576–586. https://doi.org/10.1016/j.dss.2011.02.002

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662–674. https://doi.org/10.1002/asi.20779