Analisis Keamanan dan Privasi Data Instagram Terhadap Ancaman Phishing di Era Digital

Abel Amanda Ardelia[1], Qibti Amiroh Rihadatul 'Aisy[2], Santikasari[3]

[1]*Jurusan Teknik Informatika/Fakultas Ilmu Komputer*
Universitas Duta Bangsa Surakarta
[1]220103042@mhs.udb.ac.id

[2] *Jurusan Teknik Informatika/Fakultas Ilmu Komputer*
Universitas Duta Bangsa Surakarta
[2]220103069@mhs.udb.ac.id

[3]*Jurusan Teknik Informatika/Fakultas Ilmu Komputer*
Universitas Duta Bangsa Surakarta
[3]220103075@mhs.udb.ac.id

***Abstrak*— Pertumbuhan signifikan pengguna Instagram, yang kini mencapai lebih dari 1 miliar pengguna aktif bulanan, platform ini menjadi target utama serangan cybercrime, termasuk phishing. Phishing adalah metode penipuan yang menyamar sebagai entitas tepercaya untuk memperoleh informasi sensitif seperti nama pengguna, kata sandi, dan informasi kartu kredit. Penelitian ini menggunakan desain kuantitatif dengan metode eksperimen, melibatkan 100 responden yang dibagi menjadi kelompok kontrol dan eksperimen. Temuan menunjukkan bahwa meskipun 65% responden merasa keamanan data mereka terjaga, 80% pernah menerima pesan mencurigakan dan hanya 30% mengaktifkan autentikasi dua faktor. Dari aspek privasi, hanya 50% pengguna merasa kebijakan privasi Instagram cukup transparan, dan 60% memanfaatkan fitur privasi yang tersedia. Hasil analisis statistik menunjukkan perbedaan signifikan antara kelompok kontrol dan eksperimen dalam pemahaman dan perilaku terkait keamanan dan privasi data, serta kesadaran terhadap phishing. Rekomendasi yang diberikan meliputi peningkatan transparansi kebijakan privasi, kampanye berkelanjutan tentang ancaman phishing, promosi proaktif autentikasi dua faktor, serta penambahan fitur keamanan dan privasi baru. Implementasi langkah-langkah ini diharapkan dapat meningkatkan kesadaran pengguna dan melindungi informasi pribadi mereka dari ancaman phishing di era digital yang semakin kompleks.**
Kata kunci— phishing, cybercrime, keamanan, privasi, Instagram.

***Abstract*— The significant growth of Instagram users, now exceeding 1 billion active monthly users, has made the platform a primary target for cybercrime attacks, including phishing. Phishing is a deceptive method that impersonates a trusted entity to obtain sensitive information such as usernames, passwords, and credit card details. This study employs a quantitative design with an experimental method, involving 100 respondents divided into control and experimental groups. Findings reveal that although 65% of respondents feel their data security is well-maintained, 80% have received suspicious messages, and only 30% have activated two-factor authentication. In terms of privacy, only 50% of users find Instagram's privacy policy sufficiently transparent, and 60% utilize the available privacy features. Statistical analysis results indicate significant differences between the control and experimental groups in terms of understanding and behavior related to data security and privacy, as well as awareness of phishing. Recommendations include enhancing the transparency of privacy policies, ongoing campaigns about phishing threats, proactive promotion of two-factor authentication, and the addition of new security and privacy features. The implementation of these measures is expected to increase user awareness and protect their personal information from phishing threats in the increasingly complex digital era.**
Keywords—phishing, cybercrime, security, privacy, Instagram.

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi di era digital telah mengubah cara masyarakat berinteraksi dan berbagi informasi. Salah satu platform paling populer untuk berbagi foto dan video adalah Instagram. Instagram adalah aplikasi media sosial yang memungkinkan pengguna mengambil, mengedit, dan berbagi foto dengan jaringan mereka. Sejak diluncurkan pada tahun 2010, Instagram telah menjadi salah satu platform media sosial terbesar dengan lebih dari 1 miliar pengguna aktif bulanan. Popularitas tersebut pun menarik perhatian berbagai pihak termasuk para penjahat cyber[2].

Kejahatan dunia maya adalah tindakan kriminal yang dilakukan melalui komputer dan jaringan internet. Bentuk umum kejahatan dunia maya adalah phishing. Phishing adalah metode penipuan yang digunakan untuk menyamar sebagai organisasi tepercaya dalam komunikasi elektronik untuk mendapatkan informasi sensitif seperti nama pengguna, kata sandi, dan informasi kartu kredit. Dengan tumbuhnya pengguna media sosial seperti Instagram, ancaman phishing pun semakin meningkat[2].

Keamanan data dan perlindungan data di Instagram merupakan isu yang sangat penting mengingat meningkatnya serangan siber. Keamanan data adalah upaya untuk melindungi data dari akses, modifikasi, serta penghapusan yang tidak sah. Perlindungan data adalah tentang hak individu untuk mengontrol bagaimana data pribadi mereka dikumpulkan dan digunakan. Sebagai salah satu platform media sosial terbesar, Instagram adalah target utama serangan siber, termasuk phishing, yang dapat membahayakan informasi pribadi pengguna[5].

Ancaman phishing di era digital menunjukkan tren peningkatan yang signifikan. Phisher menggunakan berbagai teknik untuk mengelabui pengguna Instagram agar mengungkapkan informasi pribadi. Teknik yang umum digunakan antara lain membuat website palsu yang menyerupai halaman login Instagram, mengirimkan direct message yang seolah-olah berasal dari pihak resmi Instagram, dan menawarkan hadiah atau verifikasi akun yang sebenarnya termasuk jebakan[7].

Serangan cyber di Instagram tidak hanya berdampak pada pengguna individual, namun juga dapat membahayakan integritas platform secara keseluruhan. Selain kerugian finansial, serangan ini juga dapat merusak reputasi Instagram dan melemahkan kepercayaan pengguna. Oleh karena itu, penting untuk memahami dan menganalisis keamanan dan privasi data Instagram Anda ketika menghadapi ancaman phishing[6].

Jurnal ini merinci konsep dasar Instagram, kejahatan dunia maya, phishing, keamanan dan privasi data Instagram, serta ancaman phishing di era digital. Selain itu, serangan siber yang sering terjadi di Instagram dan cara platform menanganinya juga dianalisis. Tujuan dari penelitian ini adalah untuk memberikan pemahaman komprehensif tentang ancaman phishing dan kemungkinan tindakan untuk meningkatkan keamanan dan privasi data pengguna Instagram.

II. METODOLOGI PENELITIAN

Untuk mencapai tujuan penelitian ini, kami menggunakan desain penelitian kuantitatif dengan menggunakan metode eksperimen. Metode ini dipilih karena dapat mengidentifikasi hubungan antara variabel yang diamati yaitu privasi dan keamanan data di Instagram dan serangan phishing. Berikut penjelasan mengenai metode penelitian yang digunakan pada penelitian ini :

1. Desain Penelitian

Penelitian ini melibatkan dua kelompok sampel, yaitu kelompok kontrol dan kelompok eksperimen. Kelompok kontrol tidak menerima intervensi khusus, sementara kelompok eksperimen diberikan pelatihan dan informasi mengenai langkah-langkah keamanan dan privasi data di Instagram serta cara mengidentifikasi dan menghindari phishing. Dengan membandingkan kedua kelompok ini, kami berharap dapat menilai efektivitas intervensi yang diberikan.

2. Sample

Sampel penelitian terdiri dari 100 pengguna Instagram yang dipilih secara acak. Teknik random sampling digunakan untuk memastikan representativitas sampel dan mengurangi bias. Pengguna yang terpilih kemudian dibagi secara acak menjadi dua kelompok, masing-masing terdiri dari 50 orang.

3. Instrumen Penelitian

Instrumen utama yang digunakan dalam penelitian ini adalah kuesioner yang dirancang untuk mengukur aspek-aspek keamanan dan privasi data di Instagram, serta pengalaman dan kesadaran pengguna terhadap ancaman phishing. Kuesioner ini mencakup beberapa bagian, yaitu demografi, pemahaman tentang keamanan dan privasi, pengalaman dengan phishing, dan kesadaran phishing.

4. Teknik Pengumpulan Data

Metode pengumpulan data pada penelitian ini menggunakan metode kuantitatif melalui pengisian kuesioner. Jadi kuesioner akan disebarkan secara online kepada orang-orang untuk mengumpulkan data kuantitatif.

5. Analisis Data

Data yang terkumpul dianalisis menggunakan analisis statistik. Statistik deskriptif digunakan untuk menggambarkan karakteristik sampel dan distribusi jawaban kuesioner. Uji t dan uji chi-square digunakan untuk menguji hubungan antara variabel-variabel yang diteliti, sementara regresi linier

digunakan untuk menganalisis pengaruh keamanan dan privasi data terhadap kejadian phishing. Data wawancara dianalisis secara kualitatif menggunakan teknik analisis tematik untuk mengidentifikasi tema utama.

6. Penyajian Hasil

Hasil penelitian disajikan dalam bentuk tabel, grafik, dan narasi deskriptif untuk memudahkan interpretasi data. Hasil analisis statistik menunjukkan apakah ada perbedaan signifikan dalam pemahaman dan perilaku antara kelompok kontrol dan eksperimen, serta mengidentifikasi faktor-faktor yang mempengaruhi keamanan dan privasi data di Instagram dan kesadaran terhadap phishing. Berdasarkan temuan ini, rekomendasi diberikan untuk meningkatkan keamanan dan privasi pengguna Instagram serta meningkatkan kesadaran mereka terhadap ancaman phishing.

III. HASIL DAN PEMBAHASAN

Berdasarkan survei yang telah kami lakukan menggunakan kuesioner terhadap 100 narasumber, maka kami dapat menampilkan hasil kuesioner berupa tabel 1 yang berisi pertanyaan yang kami berikan kepada narasumber serta persentase banyaknya responden yang menjawab ya dan tidak. Berikut tabel hasil kuesioner yang telah kami lakukan :

Tabel 1 Hasil dari Kuesioner

No	Pertanyaan	Ya (%)	Tidak (%)	Jumlah Responden
1	Apakah Anda merasa keamanan data Anda di Instagram terjaga dengan baik?	65%	35%	100
2	Pernahkah Anda menerima pesan mencurigakan di Instagram?	80%	20%	100
3	Apakah Anda pernah mengklik tautan yang tidak dikenal di Instagram?	45%	55%	100
4	Apakah Anda mengaktifkan autentikasi dua faktor di akun Instagram Anda?	30%	70%	100
5	Apakah Anda mengetahui tentang ancaman phishing di Instagram?	75%	25%	100
6	Apakah Anda pernah menjadi korban phishing di Instagram?	10%	90%	100
7	Apakah Anda secara rutin memperbarui kata sandi Instagram Anda?	40%	60%	100
8	Apakah Anda merasa Instagram cukup transparan mengenai kebijakan privasi?	50%	50%	100

9	Apakah Anda menggunakan fitur privasi yang tersedia di Instagram?	60%	40%	100
10	Apakah Anda merasa edukasi mengenai keamanan di Instagram perlu ditingkatkan?	85%	15%	100

Penelitian ini mengungkap beberapa temuan yang signifikan terkait dengan keamanan dan privasi data pengguna Instagram serta kesadaran mereka terhadap ancaman phishing. Dari hasil survei terhadap 100 pengguna Instagram, sebagian besar responden (65%) menyatakan bahwa mereka merasa keamanan data mereka di Instagram terjaga dengan baik. Namun, sebanyak 80% responden mengaku pernah menerima pesan mencurigakan di Instagram, sementara 45% pernah mengklik tautan yang tidak dikenal. Fakta bahwa hanya 30% dari mereka yang mengaktifkan autentikasi dua faktor menunjukkan bahwa masih ada kekurangan dalam penerapan langkah-langkah keamanan yang lebih lanjut. Sebagian besar responden (75%) menyatakan bahwa mereka mengetahui tentang ancaman phishing di Instagram, namun hanya sebagian kecil dari mereka yang (10%) pernah menjadi korban phishing.

Dari segi privasi, hanya separuh dari responden (50%) yang merasa Instagram cukup transparan mengenai kebijakan privasi, dan 60% menggunakan fitur privasi yang tersedia di platform tersebut. Temuan ini menunjukkan bahwa masih ada ruang untuk peningkatan dalam hal transparansi dan penerapan fitur privasi di Instagram. Selain itu, mayoritas responden (85%) menyatakan bahwa edukasi mengenai keamanan di Instagram perlu ditingkatkan, menyoroti pentingnya pendekatan proaktif dalam meningkatkan kesadaran pengguna terhadap ancaman phishing.

Hasil analisis statistik juga mengungkap adanya perbedaan yang signifikan antara kelompok kontrol dan eksperimen dalam pemahaman dan perilaku terkait keamanan dan privasi data di Instagram. Ini menunjukkan bahwa pelatihan dan informasi mengenai langkah-langkah keamanan dan privasi data serta cara mengidentifikasi dan menghindari phishing dapat secara efektif meningkatkan kesadaran dan tindakan pengguna dalam melindungi informasi pribadi mereka.

Berdasarkan temuan ini, rekomendasi dapat diberikan untuk meningkatkan keamanan dan privasi pengguna Instagram serta meningkatkan kesadaran mereka terhadap ancaman phishing. Rekomendasi tersebut termasuk peningkatan transparansi kebijakan privasi, penyuluhan secara teratur tentang ancaman phishing dan langkah-langkah pencegahannya, serta peningkatan penerapan fitur keamanan seperti autentikasi dua faktor. Dengan mengambil langkah-langkah ini, diharapkan dapat mengurangi risiko penyalahgunaan data dan meningkatkan keamanan serta privasi pengguna Instagram di era digital yang semakin kompleks ini.

Solusi untuk meningkatkan keamanan dan privasi pengguna Instagram serta kesadaran akan ancaman phishing memerlukan beberapa langkah. Pertama, buat kebijakan privasi Anda lebih transparan dengan menggunakan bahasa yang lebih sederhana dan menyebarkan informasi melalui berbagai saluran, termasuk email, notifikasi dalam aplikasi, dan video instruksi. Kedua, kami meningkatkan kesadaran akan ancaman phishing melalui kampanye berkelanjutan, tutorial video, infografis, artikel, dan kolaborasi dengan pakar keamanan di webinar dan sesi tanya jawab langsung.

Ketiga, secara proaktif mempromosikan otentikasi dua faktor (2FA) dengan pemberitahuan rutin dan petunjuk langkah demi langkah, dan fitur keamanan tambahan seperti memverifikasi identitas Anda saat masuk dari perangkat baru dan memperingatkan Anda tentang login yang mencurigakan. Keempat, kami akan meningkatkan penggunaan fitur privasi dengan memberikan informasi yang jelas tentang pengaturan privasi dan menambahkan fitur privasi

baru yang memungkinkan kontrol lebih besar dan penghapusan data otomatis.

Terakhir, perkenalkan program pelatihan pengguna yang berfokus pada keamanan data dan privasi melalui kursus online bersertifikat dan berikan tips keamanan dan privasi dalam aplikasi, terutama saat pengguna terlibat dalam perilaku berisiko seperti: Penawaran, klik tautan dari sumber yang tidak dikenal.

IV. KESIMPULAN

Setelah menganalisis dan membahas mengenai Keamanan dan Privasi Data Instagram Terhadap Ancaman Phishing di Era Digital, sebagian besar pengguna Instagram merasa data mereka aman, namun banyak yang menerima pesan mencurigakan dan belum mengaktifkan autentikasi dua faktor. Hanya 30% yang mengaktifkan fitur keamanan ini, sementara 75% menyadari ancaman phishing tetapi hanya 10% yang menjadi korban. Dari sisi privasi, hanya 50% pengguna merasa Instagram transparan dalam kebijakan privasinya, dan 60% memanfaatkan fitur privasi yang ada, menunjukkan perlunya peningkatan dalam transparansi dan penerapan fitur privasi di platform tersebut.

Untuk meningkatkan keamanan dan privasi, solusi yang diberikan meliputi peningkatan transparansi kebijakan privasi dengan bahasa sederhana dan berbagai saluran informasi, kampanye kesadaran phishing, promosi proaktif autentikasi dua faktor, serta penambahan fitur keamanan dan privasi baru. Selain itu juga disarankan untuk mengadakan program pelatihan pengguna yang fokus pada keamanan data dan privasi melalui kursus online bersertifikat dan memberikan tips keamanan dalam aplikasi.

UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan, bantuan, dan bimbingan selama penyusunan jurnal ini. Untuk mengungkapkan rasa terima kasih kami:

1. **Bapak Bondan Wahyu Pamekas, S.Kom, M.Kom**, sebagai pembimbing utama kami yang selalu memberikan arahan, saran, dan dukungan tanpa henti.
2. **Universitas Duta Bangsa Surakarta**, yang telah memberikan fasilitas dan dukungan selama penelitian ini berlangsung.

Kami berharap jurnal ini dapat memberikan kontribusi yang berarti bagi perkembangan ilmu pengetahuan dan bermanfaat bagi semua pihak yang membaca. Semoga segala bantuan dan dukungan yang diberikan dapat dibalas oleh Tuhan Yang Maha Esa.

REFERENSI

[1] Adetya Firnanda, R. P. (2021). Kebocoran Data Pribadi Melalui Fitur Sticker di Dalam Platform Instagram. *Semnastekmu, Volume 1 No. 1*, 154-159.

[2] Arifah Hanum, D. A. (2022). Ancaman Phising Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime. *Academia edu*, 1-5.

[3] Indrawan Ady Saputro, L. S. (2024). Sosialisasi Penggunaan Media Sosial yang Aman dari Bahaya Phising di Masjid Al Huda Pandeyan. *Jurnal Pengabdian Kepada Masyarakat, Volume 4 No. 1*, 28-33.

[4] Khairunnissa Zahran Ansyafa, M. F. (2024). Analisis Keamanan Media Sosial terhadap Serangan Phising Onlinemenggunakan Metode Zphisherdan Social Engineering Toolkit. *Journal of Internet and Software EngineeringVol: 1, No 4*, 1-10.

[5] Malahayati, N. N. (2024). Analisis Tingkat Kesadaran Mahasiswa Terhadap Serangan Rekayasa Sosial (Studi Kasus: Mahasiswa Teknologi Informasi Univesitas Islam Negeri Ar-Raniry). *Journal of Information Technology*, 12-24.

[6] MOHD. Yusuf DM, A. J. (2022). Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia. *Jurnal Pendidikan dan Konseling, Volume 4 Nomor 5* , 8018-8023.

[7] Nunu Vadila, A. R. (2021). Analisis Kesadaran Keamanan Terhadap Ancaman Phising. *Journal UII*, 1-4.

[8] Ratri Ayunita Kinasih, A. W. (2020). AnalisisKeamanan Browser Menggunakan Metode National Institute of Justice(Studi Kasus: Facebookdan Instagram). *Jurnal Teknologi Informasi & Komunikasi, Volume 11, Nomor2*, 174-184.

[9] Rendi Budi Syahputra Siregar, L. R. (2023). Analisis Penggunaan Media Sosial Instagram Terhadap Komunikasi Pembangunan di Kota Medan. *Sibatik Journal, Volume 2 No.3*, 1047-1054.

[10] Rian Dwi Hapsari, K. G. (2023). Ancaman Cyber Crime di Indonesia. *Jurnal Konstituen Vol.5 (1)*, 1-17.