JURNAL SISTEM INFORMASI GALUH **ISSN 2964-7746**
Volume 3, Nomor 1, Januari 2025 https://ojs.unigal.ac.id/index.php/jsig/index
(Bagas Adiansyah Souhoka)

Analisis Strategi Pencegahan Phising Studi Kasus Pada Media Sosial *Facebook*

Bagas Adiansyah Souhoka[*1], Rama Afan Fadillah[2], Muhammad Fathan[3], Reza Meldiansah[4], Manarul Iza Mutakin[5], Fauziyah[6]
[*1,2,3,4,5,6]Universitas Bung Karno
E-mail: *[1]souhokabagas@gmail.com, [2]rfadill790@gmail.com, [3]widutbkz123@gmail.com, [4]lmnopatan@gmail.com, [5]manarulizamutakin@gmail.com, [6]fauziyah@ubk.ac.id

Abstract

Social media is a digital platform that allows users to connect and interact with each other. However, social media is also vulnerable to misuse by irresponsible parties, such as phishing. The impact of losing this personal data can be very detrimental, ranging from identity theft to financial fraud resulting in serious economic losses. This research uses a qualitative descriptive research method. This method describes and analyzes data obtained from Facebook social media. Indonesia was the most targeted country for phishing attacks in the last three months of 2023, with an average success rate of 84.3%. Phishing is a serious threat to social media users such as Facebook, causing losses such as identity theft, financial fraud, and the spread of malware. Users should be wary of suspicious links or requests for information, and social media platforms should improve security and user education. Facebook phishing modes include creating fake accounts, spreading phishing links, and using Facebook ads. Effective precautions include verifying website addresses, using an antivirus program, protecting your personal information, and enabling two-factor authentication. Research shows that phishing attacks are rising, with Indonesia being the main target. A joint effort between users and social media platforms is essential to create a safer digital environment.

Keywords : *Phishing, Facebook, Social, Media, Cybercrime.*

Abstrak

Media sosial merupakan platform digital yang memungkinkan penggunanya terhubung dan berinteraksi satu sama lain. Namun media sosial juga rentan disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab, seperti phising. Dampak dari kehilangan data pribadi ini bisa sangat merugikan, mulai dari pencurian identitas hingga penipuan keuangan yang mengakibatkan kerugian finansial yang serius. Penelitian ini menggunakan metode penelitian deskriptif kualitatif. Metode ini digunakan untuk menggambarkan dan menganalisis data yang diperoleh dari media sosial Facebook. Indonesia adalah negara yang paling banyak ditargetkan untuk serangan phishing di tiga bulan terakhir pada tahun 2023, dengan tingkat keberhasilan rata-rata 84,3%. Phishing merupakan ancaman serius bagi pengguna media sosial seperti Facebook yang menimbulkan kerugian seperti pencurian identitas, penipuan finansial, dan penyebaran malware. Pengguna harus waspada terhadap tautan mencurigakan atau permintaan informasi, dan platform media sosial harus meningkatkan keamanan dan pendidikan pengguna. Modus phishing Facebook termasuk membuat akun palsu, menyebarkan tautan phishing, dan menggunakan iklan Facebook. Tindakan pencegahan yang efektif mencakup memverifikasi alamat situs web, menggunakan program antivirus, melindungi informasi pribadi Pengguna, dan mengaktifkan otentikasi dua faktor. Penelitian menunjukkan bahwa serangan phishing sedang meningkat, dan Indonesia menjadi target utamanya. Upaya bersama antara pengguna dan platform media sosial sangat penting untuk menciptakan lingkungan digital yang lebih aman.

Kata Kunci : *Phishing, Facebook, Sosial, Media*, *Cybercrime.*

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

I. PENDAHULUAN

Media sosial merupakan *platform* digital yang memungkinkan penggunanya terhubung dan berinteraksi satu sama lain. Namun media sosial juga rentan disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab, seperti phising.

Phishing adalah teknik yang digunakan untuk mengelabui korban agar menyerahkan data berharga. Manipulasi, rekayasa sosial, dan sering kali peniruan identitas otoritas resmi atau layanan tepercaya digunakan untuk menipu korban. Media sosial seperti *Facebook*, merupakan *platform* digital yang memungkinkan pengguna untuk berinteraksi dan terhubung satu sama lain. Namun, *platform* ini juga rentan terhadap kejahatan digital, salah satunya adalah *phishing*. *Phishing* adalah teknik penipuan yang memanfaatkan manipulasi sosial dan peniruan entitas resmi untuk mencuri data berharga dari korban [1].

Pengguna yang menjadi korban *phishing* dapat kehilangan data pribadi mereka, seperti data *login* akun, nomor kartu kredit, dan informasi sensitif lainnya. Hal ini dapat mengakibatkan pencurian identitas, penipuan keuangan, dan kerugian finansial dan lainnya [3]. Selain itu, *phishing* juga dapat menimbulkan kerugian lain, seperti penyebaran *malware* yang dapat merusak perangkat pengguna atau mencuri informasi tambahan tanpa sepengetahuan pengguna [2]. Upaya *phishing* ini juga dapat berdampak signifikan terhadap kepercayaan dan keamanan pengguna di *platform* sosial.

Untuk melindungi diri dari ancaman *phishing*, penting bagi pengguna media sosial untuk selalu waspada terhadap tautan atau untuk melindungi diri dari ancaman *phishing*, penting bagi pengguna media sosial untuk selalu waspada terhadap tautan atau permintaan informasi yang mencurigakan. Serta, penting juga bagi *platform* untuk terus meningkatkan sistem keamanan dan membesrikan edukasi kepada pengguna tentang praktik *phishing* dan cara mengenali serta menghindarinya [3]. Demikian, dapat diharapkan pengalaman berinteraksi yang lebih aman dan terlindungi di dunia digital yang terus berkembang ini.

Sosial Media merupakan *platform* digital yang memungkinkan penggunanya untuk saling terhubung dan berintrakasi satu sama lain[1]. Pada gambar 1 merupakan perbandingan serangan phising dan protokol HTTPS. Bar birung merupakan jumlah serangan *phising* yang dihosting pada HTTPS dan garis kuning adalah jumlah serangan *phising* melalui situs web.

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

Gambar 1. Data Serangan Phising Dengan Protokol HTTPS

Sumber: Laporan Aktivitas Phising Q3 pada tahun 2023 (IDADX) [4].

Berdasarkan data yang dikumpulkan oleh IDADX, dilakukan analisis situs *phishing* menggunakan protokol HTTPS. Pada gambar 1 diatas dapat dilihat kuartal kesatu tahun 2021, protokol HTTPS yang digunakan lebih tinggi hingga kuartal kedua tahun 2023. Berdasarkan grafik ini, jumlah serangan *phishing* terhadap situs *web* yang menggunakan protokol HTTPS meningkat dari kuartal ketiga tahun 2019 hingga kuartal keempat tahun 2023. Hal ini menunjukkan bahwa situs terenkripsi sering digunakan untuk *phishing* dan memiliki lubang peretasan[4].

Permasalahan yang diangkat pada penelitian ini ialah bagaimana modus operasi *phishing* di *Facebook*, apa dampak *phishing* terhadap pengguna *Facebook*, dan bagaimana strategi pencegahan *phishing* di *Facebook*.

Adapun tujuan dari penelitian ini adalah untuk menganalisis modus operasi *phishing* di *Facebook*, mengidentifikasi faktor-faktor yang menyebabkan pengguna *Facebook* rentan terhadap *phishing*, serta mengidentifikasi strategi pencegahan *phishing* yang efektif untuk pengguna *Facebook*.

Penelitian ini diharapkan dapat memberikan manfaat berupa rekomendasi kepada *Facebook* dan pengguna *Facebook* tentang cara mencegah *phishing*, serta membantu pengguna *Facebook* untuk memahami bahaya *phishing* dan meningkatkan kewaspadaan terhadap penipuan *online*.

1.1 Penelitian Relevan

Penelitian yang dilakukan Irawan pada tahun 2020, dengan judul penelitian Mencuri Informasi Penting Dengan Mengambil Alih Akun *Facebook* dengan metode Phising. Penelitian ini

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

menggunakan pendekatan deskriptif kualitatif, yang menyimpulkan bahwa kegiatan penipuan ini menipu pengguna untuk memasukkan data akun seperti nama pengguna dan kata sandi ke situs *web* palsu (situs *web spoof*). *Website* scam tersebut akan didesain mirip dengan halaman aslinya (*web*site palsu). Misalnya: logo, alamat domain. Jadi, jika tidak dicermati, mereka yang menjadi sasaran penjahat dunia maya akan dengan mudah memberikan detailnya seperti nama pengguna, kata sandi, dan informasi penting lainnya. Hasil dari penelitian ini merupakan langkah-langkah mencegah *phising* yang efektif Perhatikan tautan yang akan kunjungi. Apakah situs *web* yang akan dikunjungi itu asli atau tidak, kenali tanda *giveaway* yang ada dalam email *phising* [2].

Penelitian yang dilakukan N. Elsa Leona pada tahun 2021 dengan judul penelitian Kesadaran Ancaman Privasi Serta Perilaku Perlindungan Privasi Dalam Menggunakan Sosial Media menggunakan pendekatan studi literatur sebagai metode penelitiannya. Banyak pengguna internet, terutama yang aktif di media sosial, seringkali tidak menyadari berbagai bahaya dan ancaman yang dapat mengancam privasi dan identitasnya. Hal ini karena pengguna cenderung mengungkapkan informasi pribadinya. Jika data ini jatuh ke tangan yang salah, baik di dunia maya maupun nyata, maka bisa digunakan untuk tujuan jahat. *Malware*, serangan *phishing*, *spam*, penipuan internet, *clickjacking*, dan sebagainya merupakan bahaya yang dapat membahayakan keamanan informasi pribadi pengguna. Oleh karena itu, sangat penting bagi pengguna untuk menjaga privasi saat menggunakan media sosial. Salah satu langkah yang dapat pengguna ambil adalah memahami kebijakan privasi *platform* media sosial sebelum menggunakannya dan berhati-hati dalam membatasi informasi pribadi yang diposting [5].

Penelitian lainnya yang dilakukan Betty Mesra pada tahun 2021 dengan judul penelitian Keamanan Informasi Data Pribadi Pada Media Sosial. Saat ini, cara masyarakat berkomunikasi telah berubah seiring dengan kemajuan teknologi informasi dan internet. Salah satunya adalah kemajuan media sosial, dimana perolehan, berbagi, dan penyebaran informasi kini sudah menjadi bagian dari kehidupan manusia. Dengan berkembangnya media sosial, keamanan data dan privasi menjadi perhatian utama saat ini. Saat ini sudah sangat umum menggunakan media sosial untuk mengungkapkan informasi sensitif. Informasi pribadi banyak orang tersebar melalui Internet tanpa mereka sadari. Baik penyedia layanan maupun kelalaiannya dapat menyebabkan

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

kebocoran data privasi. Keamanan sistem informasi harus dilindungi. Keselamatan dapat diartikan sebagai kualitas atau keadaan aman dan bebas dari bahaya. Penelitian dilakukan dengan menggunakan metode kombinasi [6].

II. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian deskriptif kualitatif. Metode ini digunakan untuk menggambarkan dan menganalisis data yang diperoleh terkait *phising* di media sosial *Facebook*. Data yang diperoleh berupa data primer dan data sekunder. Berikut adalah metode yang digunakan oleh peneliti dalam Analisis Strategi Pencegahan Phising di media sosial *Facebook* [7].

2.1 Tahapan Penelitian

Penelitian perlu memperhatikan tahapan atau langkah-langkah agar kegiatan penelitian berjalan sesuai dengan ruang lingkup dan hasil penelitian selaras dengan tujuan dari permasalahan yang ditemukan. Pada gambar 2 berikut ini merupakan tahapan penelitian pada kegiatan ini.

Gambar 1. Tahapan Penelitian

1. Identifikasi Masalah

   Proses penelitian diawali dengan mengidentifikasi masalah penelitian. Tema penelitian dan pertanyaan penelitian mempunyai pengaruh yang signifikan terhadap kualitas penelitian. Oleh karena itu, kesalahan dalam mendefinisikan masalah penelitian akan mempengaruhi kualitas hasil penelitian, dengan kata lain, mengidentifikasi pertanyaan penelitian di awal penelitian sangatlah penting karena mempengaruhi hasil penelitian. Selain itu, identifikasi masalah penelitian juga menentukan apakah penelitian dapat dilanjutkan. Apabila pertanyaan penelitian yang diajukan tidak memenuhi kriteria, maka peneliti perlu mencari topik penelitian lain yang lebih penting dan menarik. Peneliti dapat menyimpulkan bahwa

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

masalah penelitian adalah suatu pernyataan atau pertanyaan yang membahas satu atau lebih variabel yang terlibat dalam suatu fenomena [8].

2. Pengumpulan Data

   Teknik pengumpulan data adalah cara atau cara yang digunakan peneliti untuk mengumpulkan berbagai data, informasi, dan fakta pendukung lainnya untuk tujuan penelitian. Metode penelitian ini tidak lepas dari metode penelitian yang digunakan oleh peneliti. Ketika peneliti memilih teknik pengumpulan data kualitatif, digunakan metode seperti observasi, wawancara mendalam, *Focus Group Discussion (FGD)*, atau studi kasus. Sedangkan jika menggunakan teknik pengumpulan data kuantitatif, metode yang digunakan dapat berupa angket, studi dokumen, dan wawancara. Bagian ini memberikan konteks untuk banyak teknik pengumpulan data yang digunakan pada partisipan manusia [9].

3. Analisis Data

   Proses penelitian baru dilaksanakan setelah semua informasi yang diperlukan untuk memecahkan masalah yang diteliti tersedia secara lengkap. Ketajaman dan ketepatan penggunaan alat analisis sangat menentukan keakuratan kesimpulan. Oleh karena itu, kegiatan analis data ini merupakan kegiatan yang tidak dapat diabaikan dalam proses penelitian. Spesifikasi peralatan analisis yang tidak akurat dapat berdampak buruk pada kesimpulan dan, lebih buruk lagi, pada penggunaan dan penerapan hasil penelitian. Oleh karena itu, pengetahuan dan pemahaman berbagai metode analisis sangat penting bagi peneliti untuk memberikan kontribusi yang signifikan dalam memecahkan masalah atau menjelaskan hasil secara ilmiah. Secara umum teknik analisis data dibagi menjadi dua bagian, yaitu analisis kuantitatif dan analisis kualitatif. Satu-satunya perbedaan antara kedua teknik ini adalah jenis datanya. Analisis kualitatif digunakan untuk menganalisis data Data kuantitatif bersifat kualitatif (tidak terhitung), namun dapat juga dianalisis secara kuantitatif atau kualitatif [10].

4. Penyajian Data

   Penyajian data atau informasi merupakan fungsi pelaporan penelitian yang dilakukan sedemikian rupa sehingga memungkinkan untuk dilakukan analisis. dan dipahami sesuai dengan tujuan yang diinginkan. Tugas penyajian informasi ini adalah mengorganisasikan

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

kumpulan data secara sistematis dan mudah dipahami sehingga dapat ditarik kesimpulan. Informasi yang disajikan harus sederhana, jelas, dan mudah dibaca. Selain itu, tujuan penyajian data adalah untuk membantu pengamat dengan mudah memahami apa yang disajikan peneliti untuk dianalisis dan dibandingkan lebih lanjut [11].

5. Kesimpulan

   Peneliti menarik kesimpulan berdasarkan penyajian hasil yang diperoleh setelah proses pengumpulan data dan analisis data. Selain itu saran juga diberikan sebagai masukan bagi penelitian selanjutnya yang berkaitan dengan penelitian ini [12]. Berdasarkan hasil penelitian dan kajian yang telah dijelaskan pada dokumen sebelumnya.

2.2 Metode Pengumpulan Data

Penelitian tentang phising di *Facebook* bagaikan penelusuran untuk menguak modus operasi modus penipuan digital ini, berbagai metode untuk pengumpulan data sebagai berikut:

1. Wawancara

   Pada penelitian ini, tim peneliti mewawancarai langsung korban yang terkena tindak kejahatan phising selaku informan untuk mendapatkan data primer mengenai permasalahan yang dihadapi dalam tindak kejahatan phising. Berdasarkan hasil tanya jawab (Wawancara) tersebut maka diperoleh data-data yang terkait dengan permasalahan yang ada yaitu Wawancara dapat digunakan untuk mengumpulkan data yang lebih mendalam tentang pengalaman pengguna dengan *phishing* di *Facebook*. Wawancara ini dapat memberikan wawasan tentang pengalaman mereka dengan *phishing* dan ide-ide mereka untuk mencegahnya.

2. Studi Kasus

   Menganalisis studi kasus *phishing* di *Facebook* untuk mengidentifikasi faktor-faktor yang berkontribusi terhadap serangan *phishing* dan pelajaran yang dapat dipelajari dari serangan tersebut.

3. Observasi

   Observas idilakukan untuk mengumpulkan data tentang bagaimana pengguna berinteraksi dengan *Facebook* dan bagaimana mereka bereaksi terhadap upaya *phishing.*

III. HASIL DAN PEMBAHASAN

Phishing merupakan masalah serius yang dapat berdampak serius pada pengguna media sosial. Berdasarkan Analisis tahunan Kaspersky terhadap

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

lanskap ancaman spam dan *phishing* mengungkapkan tren yang terus berlanjut sejak 2022, yakni peningkatan tajam dalam serangan *phishing*. Jumlah ini terus meningkat pada 2023, melonjak lebih dari 40 persen dan mencapai 709.590.011 upaya serangan *phishing*.

Penelitian menunjukkan bahwa jumlah serangan *phishing* terhadap situs *web* HTTPS telah meningkat dalam beberapa tahun terakhir. Hal ini menunjukkan bahwa penjahat dunia maya semakin menyadari pentingnya keamanan HTTPS dan mulai menggunakannya untuk menyembunyikan serangan *phishing* mereka. Namun, meskipun jumlah serangan *phishing* terhadap situs *web* HTTPS meningkat, namun jumlah tersebut masih kecil dibandingkan dengan jumlah serangan *phishing* terhadap situs *web* non-HTTPS[4].

3.1 Tabel Transkrip Wawancara

Pada penelitian ini, tim peneliti menggunakan wawancara sebagai metode utama dalam pengkajian data secara mendalam. Wawancara ini dilakukan pada tanggal 9 Juli 2024. Hasil wawancara dengan korban dapat dilihat pada tabel 1 berikut ini.

Tabel 1. Transkrip Wawancara Penelitian

Pertanyaan (A)	Jawaban (B)
A: Bisakah Pengguna ceritakan tentang pengalaman Pengguna dengan *phishing* di *Facebook*?”	B: Ya, tentu. Beberapa bulan lalu, saya sedang menonton *Reels* di *Facebook*. *Reels* itu berisi tautan ke situs web yang konon menawarkan hadiah menarik. Saya tergoda dan mengklik tautan tanpa berpikir panjang. Setelah itu, saya diminta untuk memasukkan informasi pribadi saya, termasuk password akun *Facebook* saya. Saya tidak curiga pada saat itu, karena situs webnya terlihat seperti situs web *Facebook* resmi. Namun, setelah saya memasukkan informasi saya, akun *Facebook* saya diretas dan semua data pribadi saya dicuri.
A: Apa yang Pengguna lakukan setelah akun *Facebook* Pengguna diretas?	B: Ketika mengetahui *Facebook* says telah di retas, saya mencoba untuk memulihkan akun tersebut. Namun, akun saya tidak bisa pulih kembali karena si peretas sudah mengubah data *login* akun saya bahkan saya sudah pergi ke pusat bantuan *Facebook* namun tidak ada hasil.
A: Bagaimana cara pengguna melindungi data pengguna setelah akun pengguna terkena phising?	B: Saya memutuskan semua akun yang terhubung dengan akun *Facebook* tersebut seperti akun sosmed lainnya dan akun game.
A: Berdasarkan kejadian tersebut, pelajaran apa yang pengguna dapatkan?	B: Lebih berhati-hati lagi terhadap link yang belum jelas dan tidak mudah tergiur dengan hadiah-hadiah yang

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

	menarik. Selanjutnya lebih waspada lagi terhadap keamanan data saya agar tidak sembarang menyebarkan nya lagi.

3.2 Modus Operasi *Phising* di Sosial Media *Facebook*

Pelaku *phishing* di *Facebook* menggunakan berbagai macam cara untuk menipu dan mencuri informasi dari pengguna. Berikut adalah beberapa modus operasi yang umum digunakan [13]:

1. Membuat akun palsu

   Membuat akun palsu yang menyerupai akun resmi *Facebook*, organisasi, atau individu terkenal. Akun palsu ini biasanya digunakan untuk mengirim pesan pribadi kepada pengguna, meminta informasi pribadi, atau mengarahkan pengguna ke situs *web phishing*. Setelah mendapatkan kepercayaan pengguna, penjahat cyber akan meminta pengguna untuk melakukan sesuatu yang berbahaya, seperti mengklik tautan, membuka lampiran, atau memberikan informasi pribadi [1].
2. Menyebarkan tautan *phishing*

   Menyebarkan tautan *phishing* melalui pesan pribadi, komentar, atau postingan di *Facebook*. Tautan *phishing* ini biasanya mengarah ke situs *web* palsu yang dibuat menyerupai situs *web* resmi *Facebook*, game, atau layanan *online* lainnya [2].
3. Memanfaatkan *Facebook Ads*

   Facebook Ads merupakan salah satu fitur dari aplikasi *facebook* itu sendiri. Umumnya di gunakan untuk strategi bisnis untuk menarik pelanggan agar membeli produk yang di promosikan. Namun dimanfaatkan oleh Sebagian pengguna untuk mengambil informasi pengguna *facebook* lainnya dengan membuat iklan palsu yang menawarkan hadiah, diskon, atau produk menarik. Ketika pengguna mengklik iklan, mereka akan diarahkan ke situs *web* palsu yang dirancang untuk meniru situs *web* resmi. Di situs *web* palsu ini, pengguna akan diminta untuk memasukkan data pribadi mereka, seperti nama pengguna, kata sandi, atau informasi kartu kredit. Iklan palsu ini biasanya berisi tautan *phishing* yang mengarah ke situs *web* palsu untuk mencuri informasi pribadi pengguna.
4. Menggunakan Fitur *Facebook*

   Memanfaatkan fitur-fitur *Facebook*, seperti grup dan halaman, untuk menyebarkan informasi palsu dan tautan *phishing*. Para pelaku *phishing* dapat membuat grup atau halaman palsu untuk meniru komunitas *online* yang sah dan menipu pengguna agar bergabung.

Data dalam tabel 2 menunjukkan persentase serangan phishing di Indonesia yang menargetkan negara-negara berbeda

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

pada bulan Oktober, November, dan Desember 2023. Indonesia adalah negara yang paling banyak ditargetkan untuk serangan phishing di semua tiga bulan, dengan tingkat keberhasilan rata-rata 84,3%. Indonesia memiliki populasi pengguna internet yang besar, dan banyak dari pengguna ini tidak terbiasa dengan penipuan phishing. Hal ini membuat mereka lebih rentan terhadap serangan Phising [4].

Tabel 2. Data Persentase Negara Yang Menghosting Situs Phising

Negara	Oktober	November	Desember
Indonesia	91.3%	85.89%	95.7%
United States	3.89	3.93%	1.19%
Russia	3.11%	9.31%	3.0%
United Kingdom	0.11%	0.06%	0%
Singapore	0.92%	0.17%	0.03%
Germany	0.32%	0.17%	
None	0.36%	0l.46%	0.08%

3.3 Faktor-faktor yang Menyebabkan Pengguna *Facebook* Rentan Terhadap *Phishing*

Ada banyak faktor yang membuat pengguna *Facebook* rentan terhadap *phishing*. Berikut faktor-faktor yang menyebabkan pengguna terkena *phishing* [14]:

1. Kurangnya Kesadaran
   Banyak pengguna *Facebook* yang tidak menyadari bahaya *phishing* dan cara menghindarinya. Hal ini membuat mereka lebih mudah tertipu oleh serangan *phishing*.
2. Ketidakmampuan Membedakan Situs *Web* Asli dan Palsu
   Banyak situs *web phishing* dirancang agar terlihat seperti situs *web* asli, sehingga menyulitkan pengguna untuk membedakannya. Pengguna yang tidak hati-hati saat menggunakan *Facebook* lebih mudah terjebak dalam serangan *phishing*. Contohnya, mereka mungkin mengklik tautan yang tidak dikenal atau memasukkan informasi pribadi mereka ke dalam situs *web* yang tidak terpercaya [14].
3. Tidak Dapat Mengidentifikasi Tautan Berbahaya
   Banyak tautan *phishing* dirancang agar terlihat seperti tautan asli, sehingga menyulitkan pengguna untuk mengidentifikasinya. Pengguna mungkin mengklik tautan yang diterima melalui email, pesan pribadi, atau postingan di *Facebook* tanpa terlebih dahulu memastikan keasliannya.
4. Tidak dapat melindungi informasi pribadi
   Banyak pengguna *Facebook* yang tidak menjaga keamanan informasi pribadi mereka, sehingga informasi ini mudah tersedia bagi penjahat dunia maya. Pengguna mungkin memasukkan informasi pribadi, seperti data *login*, nomor kartu kredit, atau informasi sensitif lainnya, ke situs *web* yang tidak dikenal atau mencurigakan.

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

3.4 Dampak *Phishing* Terhadap Pengguna Media Sosial

Serangan *phishing* terhadap pengguna mempunyai dampak yang beragam[14]. Berikut beberapa pengaruh *phishing* terhadap pengguna, diantaranya:

1. Hilangnya Privasi Data
   Kehilangan data pribadi, seperti data *login* akun, informasi akun game, dan informasi sensitif lainnya. Data ini dapat digunakan oleh para pelaku *phishing* untuk melakukan pencurian identitas, penipuan keuangan, atau aktivitas ilegal lainnya.
2. Rusaknya Reputasi
   Kerusakan reputasi akibat pencurian identitas. Para pelaku *phishing* dapat menggunakan informasi pribadi korban untuk membuat akun palsu di media sosial atau *platform online* lainnya, dan menyebarkan informasi yang merusak reputasi korban.
3. Menimbulkan Kecemasan
   Kecemasan dan stres akibat menjadi korban penipuan. Pengalaman menjadi korban *phishing* dapat menyebabkan kecemasan, stres, dan trauma bagi pengguna *Facebook*.
4. Mengalami Kerugian
   Kerugian akibat penipuan seperti kehilangan akun *game* dan juga informasi penting lainnya. Para pelaku *phishing* dapat menggunakan informasi yang dicuri untuk mengelabui korban dan berdampak bagi pengguna lainnya seperti friendlist *Facebook* korban tersebut.

3.5 Strategi Pencegahan *Phishing* yang Efektif untuk Pengguna *Facebook*

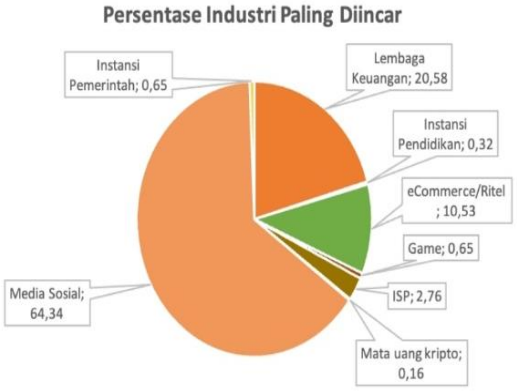
Ada beberapa strategi pencegahan *phishing* yang efektif untuk pengguna *Facebook* [3], antara lain:

1. Ketelitian Dalam Mengolah Informasi
   Berhati-hatilah dengan pesan, iklan, grup, dan profil yang tidak dikenal, jangan klik tautan atau buka lampiran dari pesan, iklan, grup, atau profil yang tidak dikenal.
2. Periksa Alamat Situs *Web* dengan Cermat
   Pastikan alamat situs *web* yang akan di kunjungi sama dengan alamat situs *web* yang dituju.
3. Gunakan Antivirus Dan Anti-*Phishing*
   Gunakan antivirus dan anti-*phishing* untuk membantu melindungi dari situs *web phishing*.
4. Jaga Informasi Pribadi
   Pengguna *Facebook* tidak boleh membagikan informasi pribadi mereka kepada orang lain, termasuk melalui media sosial. Jangan membagikan informasi pribadi dengan orang asing atau di situs *web* yang tidak ragu untuk di percayai.

ISSN 2964-7746
https://ojs.unigal.ac.id/index.php/jsig/index

5. Aktifkan Autentikasi Dua Faktor

   Autentikasi dua faktor menambahkan lapisan keamanan ekstra ke akun *Facebook*. Ini berarti bahwa *user* harus memasukkan kode verifikasi yang dikirim ke ponsel pengguna selain kata sandi untuk masuk ke akun *Facebook* tersebut.



Gambar 3. Industri Sasaran Phising

Berdasarkan Data Indonesia *Anti-Phishing Data Exchange (IDADX),* Data tersebut menunjukkan bahwa media sosial adalah industri yang paling banyak menjadi target serangan *phishing*. Pada kuartal keempat tahun 2023, 64,34% serangan *phishing* menargetkan *platform* media sosial. Hal ini kemungkinan karena *platform* media sosial populer dan memiliki banyak pengguna [4]. Pada gambar 3 merupakan Industri yang menjadi target atau sasaran phising.

IV. KESIMPULAN

Phishing merupakan ancaman serius bagi pengguna media sosial seperti *Facebook* yang menimbulkan kerugian seperti pencurian identitas, penipuan finansial, dan penyebaran *malware*. Pengguna harus waspada terhadap tautan mencurigakan atau permintaan informasi, dan *platform* media sosial harus meningkatkan keamanan dan pendidikan pengguna. Modus *phishing Facebook* termasuk membuat akun palsu, menyebarkan tautan *phishing*, dan menggunakan iklan *Facebook*. Pengguna berisiko karena kurang kesadaran dan kesulitan membedakan situs asli dan palsu. Dampak *phishing* meliputi hilangnya informasi pribadi, kerusakan reputasi, kecemasan, dan kerugian finansial. Tindakan pencegahan yang efektif mencakup memverifikasi alamat situs *web*, menggunakan program antivirus, melindungi informasi pribadi Pengguna, dan mengaktifkan otentikasi dua faktor. Penelitian menunjukkan bahwa serangan *phishing* sedang meningkat, dan Indonesia menjadi target utamanya. Upaya bersama antara pengguna dan *platform* media sosial sangat penting untuk menciptakan lingkungan digital yang lebih aman.

DAFTAR PUSTAKA

[1] L. A. Febrika Ardy, I. Istiqomah, A. E. Ezer, and S. N. Neyman, “Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial,” *Journal of Internet and Software Engineering*, vol. 1, no. 4, p. 11, Jun. 2024, doi: 10.47134/pjise.v1i4.2753.

[2] D. Irawan and S. Kom, "MENCURI INFORMASI PENTING DENGAN MENGAMBIL ALIH AKUN FACEBOOK DENGAN METODE PHISING," 2020.

[3] L. A. Febrika Ardy, I. Istiqomah, A. E. Ezer, and S. N. Neyman, "Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial," *Journal of Internet and Software Engineering*, vol. 1, no. 4, p. 11, Jun. 2024, doi: 10.47134/pjise.v1i4.2753.

[4] "LAPORAN AKTIVITAS PHISHING DOMAIN ~.ID Indonesia Anti-Phishing Data Exchange," 2023. Accessed: Jul. 07, 2024. [Online]. Available: https://api.idadx.id/documents/uploads/1705892888_Laporan%20Q4%202023.pdf.pdf.

[5] L. N. Elsa, A. C. Nur, N. M. Putu Jeanny, and A. I. Ramadhana S, "KESADARAN ANCAMAN PRIVASI SERTA PERILAKU PERLINDUNGAN PRIVASI DALAM MENGGUNAKAN SOSIAL MEDIA INFORMATION SECURITY AWARENESS AND PRIVACY PROTECTION BEHAVIOR IN USING SOCIAL MEDIA," 2021.

[6] M. Betty Yel and M. K. M Nasution, "KEAMANAN INFORMASI DATA PRIBADI PADA MEDIA SOSIAL," *JIK)*, vol. 6, no. 1, 2022.

[7] M. Butarbutar, *Pengantar Metodologi Penelitian*. Bandung: CV. MEDIA SAINS INDONESIA, 2022.

[8] A. G. Santika, R. G. Whendasmoro, and I. Zulkarnain, "Aplikasi Manajemen Komplain Gedung Plaza Setiabudi Menggunakan Framework Ionic," *Eksplorasi Teknologi Enterprise & Sistem Informasi (EKSTENSI)*, vol. 1, no. 1, p. 037045, 2022, [Online]. Available: https://journal.fikom.site/ekstensiCommonsAttribution4.0

[9] B. G. Sudarsono, I. Zulkarnain, E. Buulolo, and D. P. Utomo, "Analisa Penerapan Metode MOOSRA dan MOORA dalam Keputusan Pemilihan Lokasi Usaha," *Building of Informatics, Technology and Science (BITS)*, vol. 4, no. 3, pp. 1456–1463, Dec. 2022, doi: 10.47065/bits.v4i3.2696.

[10] A. Syaeful Millah, D. Arobiah, E. Selvia Febriani, and E. Ramdhani, "Analisis Data dalam Penelitian Tindakan Kelas," *Jurnal Kreativitas Mahasiswa*, vol. 1, no. 2, p. 2023.

[11] B. Widjanarko Otok and Ms. Dewi Juliah Ratnaningsih, "Konsep Dasar dalam Pengumpulan dan Penyajian Data."

[12] Store Deepublish, "Pengertian, Cara Membuat dan Contoh Kesimpulan," https://deepublishstore.com/blog/pengertian-kesimpulan/.

[13] A. Dzulfaroh and I. Wedhaswarry, "Apa Itu Phising?," https://www.kompas.com/tren/read/2021/03/11/123700665/apa-itu-phishing-.

[14] H. J. Parker, S. V Flowerday, and S. Flowerday, "South African Journal of Information Management," 2020, doi: 10.4102/sajim.

[15] Usep Abdul Rosid, Sidiq, M., Mulyana, D., & Yudi Permana, N. (2023). Website Design with Waterfall Method in Ciamis Regency (Case Study in Galuh Ciamis Nature and Environment Care Community) . *Jurnal Sistem Informasi Galuh*, *1*(2), 52–58. https://doi.org/10.25157/jsig.v1i2.3203