Pengukuran Kesadaran Keamanan Informasi Terhadap Phising Pada Aplikasi Facebook di Indonesia

Syaelan Raka Pramuja Ananda[1], Muhammad Saifullah[2], Ridlo Fauzi Rakhmadianto[3*]

[1] *Teknik Informatika, Universitas Duta Bangsa, Jalan Bhayangkara No.55, Surakarta*
[1]220103190@udb.ac.id

[2] *Teknik Informatika, Universitas Duta Bangsa, Jalan Bhayangkara No.55, Surakarta*
[2]220103199@udb.ac.id

[3] *Teknik Informatika, Universitas Duta Bangsa, Jalan Bhayangkara No.55, Surakarta*
[3]220103186@udb.ac.id

Abstrak

Facebook menduduki peringkat ketiga dengan persentase pengguna aktif sebanyak 83.8% dari jumlah pengguna aktif media sosial di Indonesia mencapai 167.0 juta orang pada Januari tahun 2023 (Christanto, 2023). Namun, semakin banyak pengguna juga mengundang banyak kasus keamanan informasi yang disebabkan oleh kurangnya kesadaran antara pengguna, seperti spam, spoofing/phishing, insiden jaringan, malware, mengunggah sesuatu yang bersifat pribadi seperti foto, nomor telepon, alamat, dan tidak memiliki antivirus. Penelitian ini bertujuan untuk mengetahui tentang keamanan informasi pada pengguna aplikasi Facebook dengan melakukan pengukuran masalah dari dimensi kesadaran (*sikap, pengetahuan, dan perilaku*) dengan fokus area keamanan informasi terhadap spoofing/phishing. Penelitian ini menggunakan metode survei kuantitatif dengan pengembangan kuesioner yang mencakup berbagai aspek kesadaran keamanan bagi para pengguna Facebook. Pertanyaan mencakup pengetahuan tentang fitur keamanan, perilaku penggunaan, dan persepsi tentang ancaman. Sampel menggunakan teknik sampling acak untuk mengumpulkan data dari berbagai demografi, termasuk usia dan jenis kelamin. Survei didistribusikan secara online melalui platform yang sering digunakan oleh target responden. Hasil penelitian menunjukkan bahwa 81% responden pernah mendengar tentang phishing, 65% mengetahui caramengenali tanda-tanda phishing, dan 50% memahami langkah-langkah yang harus diambil jika menjadi korban phishing. Kesadaran akan pentingnya otentikasi dua faktor cukup tinggi dengan 65% responden mengetahui cara mengaktifkannya, namun hanya 18% yang rutin mengganti kata sandi mereka. Disarankan agar pengguna Facebook secara berkala mengganti kata sandi dan melaporkan aktivitas mencurigakan untuk meningkatkan keamanan informasi mereka.

Kata kunci: keamanan informasi; phising; survei kuantitatif; facebook

Abstrak

Facebook ranks third with an active user percentage of 83.8% out of 167.0 million active social media users in Indonesia as of January 2023 (Christanto, 2023). However, an increase in users also invites numerous information security issues caused by a lack of user awareness, such as spam, spoofing/phishing, network incidents, malware, uploading personal information like photos, phone numbers, addresses, and not having antivirus software. This study aims to assess information security among Facebook users by measuring awareness dimensions (attitudes, knowledge, and behavior) with a focus on information security against spoofing/phishing, including the characteristics of phishing, phishingmedia, phishing perpetrators, signs of phishing, and countermeasures against phishing. This study employsa quantitative survey method with a questionnaire covering various aspects of security awareness among Facebook users. Questions include knowledge about security features, usage behavior, and threat perception. The sample uses random sampling techniques to collect data from various demographics, including age and gender. The survey is distributed online through platforms frequently used by the target respondents. The study results indicate that 81% of respondents have heard about phishing, 65% know how to recognize phishing signs, and 50% understand the steps to take if they become victims of phishing.

Awareness of the importance of two-factor authentication is relatively high, with 65% knowing how to activate it, but only 18% routinely change their passwords. It is recommended that Facebook users regularly change their passwords and report suspicious activities to enhance their information security.
Keywords: information security; phishing; quantitative survey; Facebook.

I. PENDAHULUAN

Facebook merupakan salah satu mediajejaring sosial yang terlaris di Indonesia bahkan di dunia. Di Indonesia, Facebook sudah menjadi gaya hidup yang tidak terpisahkan. Jejaring sosial ini digunakan untuk berinteraksi dengan relasi, teman, berbagi foto, dan bahkan untuk mengembangkan bisnis. Facebook merupakan salah satu fenomena yang telah berkembang pesat dalam sejarah internet belakangan ini (Brad Dinerman , 2011)

Oleh karena itu, diperlukan pemahaman terhadap isu keamanan data dan ancaman yang terdapat pada Facebook. Pemahaman ini diperlukan untuk kewaspadaan dan pencegahan terhadap serangan ini, (Harvey Jones, Jos_e Hiram Soltren,2005).

Menurut Whitman dan Mattord (2011), keamanan informasi merupakan upaya untuk melindungi informasi dan elemen-elemen penting yang ada di dalamnya, baik berupa sistem atau perangkat keras yang digunakan untuk menyimpan dan mengirimkan informasi. Menurut McLeod dan Schell (2008) keamanan informasi ditujukan untuk mencapai tiga tujuan utama, yaitu kerahasiaan ketersediaan, dan integritas.

Perkembangan teknologi sekarang ini tidak dapat dipungkiri sangat berkembang dengan pesat dan semakin maju seiring dengan perkembangan zaman dan ilmu pengetahuan. Selain banyak manfaatnya yang diberikan, smartphone juga merupakan alat mobile atau mudah dibawa kemana saja. Menurut survei dari Databoks pengguna smartphone diperkirakan mencapai 89% populasi pada tahun 2025, Pusparisa, Y. (2020). Penggunaan smartphone diprediksi akan terus meningkat karena seiring berjalannya waktu, ponsel pintar semakin terjangkau, sehingga meningkatkan penggunaannya pula. Lebih dari setengah populasi di Indonesia atau 56,2% telah menggunakan ponsel pintar pada 2018. Setahun setelahnya, sebanyak 63,3% masyarakat menggunakan ponsel pintar. Hingga 2025, setidaknya 89,2% populasi di Indonesia telah memanfaatkan ponsel pintar. Dalam kurun enam tahun sejak 2019.(Retalia, Tritjahjo Danny Soesilo, Sapto Irawan. 2022), dijalankan tanpa kehadiran fisik melalui media sosial. Meningkatnya penggunaan jejaring sosial dan ketergantungan pada internet juga membawa dampak negatif, terutama dalam bentuk kejahatan siber (Sabrina Tabrani1, Vivi Safitri,Putu Audy Nayla P,Asmak Ul Hosnah, 2024).

Di saat maraknya pengguna sosial media di seluruh dunia, saat itu juga penjahat-penjahat dunia siber mulai melancarkan aksinya untuk mencari keuntungan dari pengguna sosial media. Salah satunya yaitu dengan phishing. Phishing merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara tidak langsung memberikan semua informasi yang di butuhkan oleh sang penjebak. Phishing termasuk dalam kejahatan siber, dimana sekarang ini marak terjadi tindak kriminal melalui jaringan komputer (Fadly Ariadi1, Suhanda Saputra, Anggreita Tiara Putri, 2023).

Berdasarkan laporan IDADX, total pengaduan serangan phishing di Indonesia mengalami peningkatan signifikan. Tercatat,IDADX menerima sebanyak 26.675 laporan serangan phishing pada periode kuartal I 2023. Sedangkan, pada periode kuartal 4 2022 hanya terdapat sekitar 6.106 laporan phishing. Hal tersebut mengalami kenaikan sebanyak 20.569 laporan phishing (IDADX).

Banyaknya laporan phising tersebut dipengaruhi juga oleh rendahnya tingkat kesadaran masyarakat. Selain itu, faktor lainnya karena pelaku phising saat ini bisa memakai lebih dari satu nama domain sehingga lebih banyak laporan yang masuk. Makadari itu orang-orang harus memanfaatkannya sebaik mungkin agar mengurangi resiko terkena serangan phishing. Bila enggan melakukan sesuatu yang menurutnya terlalu merepotkan, mereka juga

bisa menjaga akunnya sebaik mungkin dengan pengamanan yang tepat. Hanya dengan cara itu akun tidak akan di serang dan pengguna bisa nyaman bersosialisasi di dunia maya tanpahambatan (Fadly Ariadi1, Suhanda Saputra, Anggreita Tiara Putri, 2023).

Tujuan penulisan ini adalah untuk menganalisis tingkat kesadaran pengguna Facebook di Indonesia terhadap keamanan informasi, Penelitian ini berusaha mengidentifikasi berbagai faktor seperti demografi, pengetahuan, dan pengalaman yang mempengaruhi kesadaran pengguna terhadap keamanan data mereka. Dan menyediakan rekomendasi yang dapat diimplementasikan oleh pengguna, Facebook, dan pemangku kepentingan terkait untuk meningkatkan kesadaran dan perlindungan terhadap keamanan informasi.

II. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode survei kuantitatif untuk mengukur kesadaran pengguna Facebook di Indonesia terhadap keamanan informasi. survei adalah penelitian kuantitatif dengan menggunakan pertanyaan terstruktur yang sama pada setiap orang, kemudian semua jawaban yang diperoleh peneliti dicatat, diolah, dan dianalisis (Victor Richardo, 2021). Survei ini dirancang untuk mencakup berbagai aspek kesadaran keamanan, yang meliputi sikap, pengetahuan, dan perilaku pengguna terkait keamanan informasi terhadap spoofing/phishing.

A. Desain Penelitian

Penelitian ini mengadopsi desain survei kuantitatif dengan pengembangan kuesioner yang berisi pertanyaan tertutup dan terbuka. Pertanyaan dalam kuesioner mencakup berbagai aspek kesadaran keamanan, seperti:

1. Pengetahuan: Mengukur pemahaman pengguna tentang fitur keamanan Facebook, tanda-tanda phishing, dan cara penanggulangan.
2. Sikap: Menilai persepsi dan kekhawatiran pengguna terhadap ancaman keamanan informasi.
3. Perilaku: Mengidentifikasi kebiasaan dan tindakan yang diambil oleh pengguna untuk melindungi data mereka di Facebook.

B. Populasi dan Sampel

Populasi dalam penelitian ini adalah pengguna Facebook di Indonesia yang berusia 18 tahun ke atas. sampel yang digunakan dalam penelitian ini yaitu pengguna Facebook yang dipilih secara acak.

C. Instrumen Penelitian

Instrumen yang digunakan adalah kuesioneryang terdiri dari beberapa bagian:

1. Bagian Demografi: Meliputi pertanyaan tentang usia, dan jenis kelamin.
2. Bagian Pengetahuan: Mengukur pemahaman pengguna tentang fitur keamanan Facebook dan ancaman phishing.
3. Bagian Sikap: Menilai persepsi pengguna terhadap ancaman keamanan.
4. Bagian Perilaku: Mengidentifikasi tindakan yang diambil oleh pengguna untuk melindungi akun mereka.

D. Pengumpulan Data

Data akan dikumpulkan melalui survei online yang didistribusikan melalui media sosial, email, dan platform lain yang sering digunakan oleh target responden. Survei akan berlangsung selama 4 minggu untuk memastikan jumlah responden yang memadai.

E. Etika Penelitian

Penelitian ini memastikan bahwa seluruh responden memberikan persetujuan setelah memahami tujuan dan prosedur penelitian. Data responden dijaga kerahasiaannya dan hanya digunakan untuk keperluan penelitian ini.

III. HASIL DAN PEMBAHASAN

Berdasarkan data yang telah terkumpul dari penyebaran kuesioner melalui Google Form, jumlah keseluruhan data kuesioner yang didapat adalah sebanyak 155 data responden, di bawah ini merupakan karakteristik responden dari segi jenis kelamin dapat dilihat pada tabel 1.

Tabel 1. Jenis Kelamin Responden

No.	Jenis Kelamin	Jumlah	Persentase
1	Laki Laki	87	56,1%
2	Perempuan	68	43,8%

Pada tabel 1 di atas menggambarkan di mana jumlah responden laki-laki lebih banyak dari responden perempuan. Hal ini menunjukkan mayoritas responden adalah laki-laki. Kemudian karakteristik responden bila dilihat dari segi usia dapat dilihat pada tabel 2.

Tabel 2. Usia Responden

No.	Jenis Kelamin	Jumlah	Persentase
1	18-25 tahun	54	34,1%
2	26-35 tahun	50	32,2%
3	36-45 tahun	52	33,5%

Pada tabel tersebut menunjukkan bahwa jumlah responden terhadap usia tidak jauh berbeda mulai dari usia 18 tahun hingga 45 tahun.

Terdapat 9 pertanyaan yang terfokus kepada keamanan informasi terhadap phising yang terbagi menjadi beberapa aspek yaitu pengetahuan, sikap, dan perilaku lebih detailnya dapat dilihat pada tabel 3.

Tabel 3. Pertanyaan Tentang Kesadaran Keamanan Informasi terhadap phising

No.	Pertanyaan
1	Apakah Anda pernah mendengar tentang phishing?
2	Apakah Anda tahu cara mengenali tanda-tanda phishing?
3	Apakah Anda tahu langkah-langkah yang harus diambil jika Anda menjadi korban phishing?
4	Apakah Anda tahu cara mengaktifkan otentikasi dua faktor di Facebook?
5	Apakah Anda merasa bahwa ancaman phishing merupakan masalah serius bagi pengguna Facebook?
6	Apakah Anda secara rutin mengganti kata sandi akun Facebook Anda?
7	Apakah Anda mengabaikan pesan atau email yang mencurigakan yang mengaku dari Facebook?
8	Apakah Anda menggunakan otentikasi dua faktor untuk akun Facebook Anda?
9	Apakah Anda pernah melaporkan aktivitas mencurigakan atau phishing kepada Facebook?

Dari kuesioner yang telah diberikan kepada responden, berikut persentase kesadaran keamanan informasi menurut usia responden.

Tabel 3. Kesadaran Keamanan Informasi Menurut Umur

	18-25 tahun		26-35 tahun		36-45 tahun		Total
	Ya	Tidak	Ya	Tidak	Ya	Tidak	Ya
P1	90,5%	9,4%	84,0%	16,0%	69,2%	30,7%	81,2%
P2	86,7%	13,2%	66,0%	34,0%	44,2%	55,7%	65,8%
P3	75,4%	24,5%	48,0%	52,0%	28,8%	71,1%	50,9%
P4	90,5%	9,4%	64,0%	36,0%	42,3%	57,6%	65,8%
P5	86,7%	13,2%	72,0%	28,0%	65,3%	34,6%	74,8%
P6	28,3%	71,6%	18,0%	82,0%	7,6%	92,3%	18,0%
P7	94,3%	80,2%	80,0%	20,0%	63,4%	36,5%	79,3%
P8	84,9%	15,0%	66,0%	34,0%	44,2%	55,7%	65,1%
P9	73,5%	26,4%	48,0%	52,0%	21,1%	78,8%	47,4%

Dalam Tabel 3, hasil survei menunjukkan beberapa temuan penting terkait kesadaran dan tindakan responden terhadap ancaman phishing di aplikasi Facebook. Sebanyak 81% responden pernah mendengar atau tahu apa itu phishing. Dari jumlah tersebut, 65% responden mengetahui cara mengenali ciri-ciri phishing. Selain itu, 50% responden memahami langkah- langkah yang harus diambil jika mereka menjadi korban phishing. Kesadaran akan pentingnya otentikasi dua faktor juga cukup tinggi, dengan 65% responden mengetahui cara mengaktifkannya. Sebanyak 74% responden menganggap bahwa phishing merupakan masalah serius bagi pengguna Facebook. Namun, hanya 18% responden yang rutin mengganti pasword mereka. Menariknya, 79% responden cenderung mengabaikan pesan atau email yang dicurigai sebagai phishing. Penggunaan otentikasi dua faktor tercatat pada 65% responden, dan 47% dari mereka pernah melaporkan aktivitas phishing. Temuan ini memberikan gambaran yang jelas mengenai tingkat kesadaran dan perilaku keamanan informasi pengguna Facebook di Indonesia dalam menghadapi ancaman phishing.

IV. KESIMPULAN

Penelitian ini telah mengidentifikasi tingkat kesadaran pengguna Facebook di Indonesia terhadap ancaman phishing, yang merupakan salah satu bentuk kejahatan siber yang semakin marak terjadi. Berdasarkan survei yang dilakukan, ditemukan bahwa sebagian besar responden memiliki pemahaman dasar tentang phishing dan cara mengenalinya. Sebanyak 81% responden pernah mendengar atau tahu apa itu phishing, dan 65% mengetahui cara mengenali ciri-ciri phishing. Namun, hanya 50% yang memahami langkah-langkah yang harus diambil jika menjadi korban phishing.

Kesadaran akan pentingnya otentikasi dua faktor cukup tinggi dengan 65% responden mengetahui cara mengaktifkannya, tetapi hanya 18% yang rutin mengganti kata sandi mereka. Selain itu, 79% responden cenderung mengabaikan pesan atau email yang dicurigai sebagai phishing, dan 47% dari mereka pernah melaporkan aktivitas phishing.

Temuan ini menunjukkan bahwa meskipun ada tingkat kesadaran yang cukup baik mengenai ancaman phishing, masih terdapat celah dalam tindakan preventif yang diambil oleh pengguna. Pengguna cenderung tidak mengambil langkah-langkah proaktif yang cukup untuk melindungi akun mereka, seperti rutin mengganti kata sandi atau melaporkan aktivitas mencurigakan.

Sebagai langkah untuk meningkatkan keamanan informasi, pengguna Facebook di Indonesia disarankan untuk lebih proaktif dalam melindungi akun mereka. Disarankan untuk mengganti kata sandi secara berkala dengan kombinasi yang kuat dan unik untuk setiap akun. Selain itu, penting bagi pengguna untuk melaporkan setiap aktivitas mencurigakan atau upaya phishing yang mereka temui kepada pihak Facebook. Dengan melakukan langkah-langkah ini, pengguna dapat membantu mencegah akses tidak sah ke akun mereka dan berkontribusi pada upaya kolektif dalam melawan ancaman keamanan siber. Edukasi terus-menerus dan kesadaran akan pentingnya tindakan preventif juga harus ditingkatkan untuk memastikan setiap pengguna memiliki pengetahuan dan alat yang diperlukan untuk melindungi informasi pribadi mereka.

V. DAFTAR PUSTAKA

Sabrina Tabrani1, Vivi Safitri,Putu Audy Nayla P,Asmak Ul Hosnah, 2024. Kejahatan Phising Ditinjau Dari Perspektif Hukum Dan Kejahatan Siber. Vol3,No1 .1-13.

Retalia, Tritjahjo Danny Soesilo, Sapto Irawan, 2022. Pengaruh Penggunaan Smartphone Terhadap Interaksi Sosial Remaja.

Fadly Ariadi1, Suhanda Saputra, Anggreita Tiara Putri, 2023. Sosialisasi Ancaman Dan Pencegahan Phising Teerhadap Pengguna Sosial Media Kepada Siswa/I SMK Ricardo Auto Macine. ISSN: 2986-5778.

Brad Dinerman (2011). Networking Security and Security Risks.

Harvey Jones, Jos_e Hiram Soltren (2005). Facebook: Threats to Privacy.

Witman, M. E., Mattord, H. J., 2011. Principles ofInformation security. 4thEdition. Atlanta:Cengage Learning.

McLeod, Raymond & Schell, George P. 2008. Sistem Informasi Manajemen, Edisi 10. Jakarta:Salemba Empat.

Christanto, 2023. Penggunaan Media Sosial di Indonesia Tahun 2023.

Victor Richardo, 2021. Survei Pembelajaran Pjok Di Masa Pandemi Covid-19 Siswa Kelas VII Di Tiga SMP Kecamatan Sepuluh Kabupaten Bangkalan.

(2024) website idadx. [Online]. Available: https://idadx.id/