Journal of Information and Information Security (JIFORTY)
Vol. 5, No. 2, Desember 2024, 85-96
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Analisis Ancaman Phishing terhadap Penggunaan E-Commerce di Indonesia

M. Azmi Al Fadillah[1], Mochammad Guntur Ramadhan [1], Mohammad Erza Ariefiandi [1,*]

[1] Informatika;Universitas Bhayangkara Jakarta Raya;Jl. Raya Perjuangan No. 81 Marga Mulya, Bekasi Utara Jawa Barat, 17143,(021) 88955882,
202210715223@mhs.ubharajaya.ac.id, 202210715181@mhs.ubharajaya.ac.id, 202210715211@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: 202210715211@mhs.ubharajaya.ac.id

Diterima: 16 Des 24; Review: 26 Des 24; Disetujui: 26 Des 24; Diterbitkan: 27 Des 24

Abstract

This research investigates the threat of phishing in the context of e-commerce in Indonesia. Phishing is a fraud technique aimed at stealing sensitive information from users through various methods such as fake emails, counterfeit websites, and link manipulation. In Indonesia, the e-commerce sector accounts for 32% of phishing cases. The method used in this research is qualitative narrative analysis, employing data collection through literature review and distribution of questionnaires. The primary objective of this study is to raise user awareness of phishing threats, identify users' ability to recognize phishing indicators, and disseminate preventive approaches. The results of the study indicate that many users are still unaware of phishing indicators, making them vulnerable to attacks. However, the study also found that 53% of trained users were able to identify phishing sites. This research highlights the importance of user education and the implementation of security measures. Recommendations include ongoing training for users, the use of email filters, the implementation of digital fingerprint indicators, and the application of One Time Password (OTP) systems. In conclusion, to address the phishing threat in Indonesia's e-commerce sector, a combination of enhanced user awareness, the adoption of more advanced security technologies, and collaboration among various stakeholders is needed.
***Keywords**: phishing, e-commerce, cybersecurity, user awareness, online fraud prevention.*

Abstrak

Penelitian ini menyelidiki ancaman phishing pada konteks e-commerce pada Indonesia. Phishing adalah teknik penipuan yg bertujuan buat mencuri kabar sensitif pengguna melalui banyak sekali metode misalnya email palsu, situs web tiruan, dan manipulasi tautan. Di Indonesia, sektor e-commerce bertanggung jawab atas 32% perkara phishing. Metode yg dipakai pada penelitian ini merupakan analisis naratif kualitatif, menggunakan pengumpulan data melalui kajian literatur dan penyebaran kuesioner. Tujuan primer penelitian ini merupakan buat menaikkan pencerahan pengguna e-commerce terhadap ancaman phishing, mengidentifikasi kemampuan pengguna pada mengenali perindikasi-perindikasi phishing, dan menyebarkan pendekatan pencegahan. Hasil penelitian menerangkan bahwa pengguna masih kurang tahu perindikasi-perindikasi phishing, mengakibatkan mereka rentan terhadap serangan. Namun, studi juga menemukan bahwa 53% pengguna yang sudah dilatih bisa mengidentifikasi situs phishing. Penelitian ini menyoroti pentingnya edukasi pengguna, dan implementasi langkah-langkah keamanan. Rekomendasi yang diberikan mencakup pembinaan berkelanjutan buat pengguna, penggunaan filter email, implementasi perindikasi tangan digital, dan

penerapan sistem One Time Password (OTP). Kesimpulannya, buat mengatasi ancaman phishing pada sektor e-commerce Indonesia, dibutuhkan kombinasi antara peningkatan pencerahan pengguna, penerapan teknologi keamanan yang lebih canggih, dan kerjasama antara banyak sekali pemangku kepentingan

Kata kunci: Phishing, e-commerce, keamanan siber, kesadaran pengguna, pencegahan penipuan online.

1. Pendahuluan

Saat ini keamanan siber menjadi salah satu pilar untuk menjaga keamanan dan stabilitas pada bidang ekonomi, ketergantungan terhadap teknologi yang selalu berkembang menjadi salah satu faktor utama dalam keamanan ekonomi dari serangan siber, perkembangan teknologi yang pesat juga memberikan dampak positif untuk mencegah dari serangan siber yang semakin marak dan variatif, sehingga perkembangan teknologi dapat meminimalisir terjadinya phising.

Perkembangan teknologi yang semakin maju dapat dilihat dari hadirnya E-Commerce, yang memberikan kemudahan bagi masyarakat dalam bertransaksi jual beli secara daring tanpa perlu berinteraksi langsung dengan penjual. E-Commerce adalah aplikasi dan situs web yang diakses melalui internet yang berfungsi untuk mendukung aktivitas distribusi, pembelian, penjualan, serta pemasaran barang dan jasa melalui sebuah system (Puspitasari & Sutabri, 2023). Dua model e-commerce yang paling banyak ditemui yaitu Business-to-Business (B2B) dan Business-to-Consumer (B2C). Pada model B2C, konsumen dapat membeli beragam produk dengan berbagai variasi melalui platform e-commerce sesuai dengan apa yang mereka perlukan. Terdapat beberapa aspek yang dapat mempengaruhi ketertarikan konsumen serta menjadi penentu kualitas dari suatu platform e-commerce. (Rafki Nazar et al., 2023).

Menurut (Vaithianathan 2010 dalam Noverdiansyah et al., 2022), E-commerce memiliki cakupan yang lebih luas dari sekedar aktivitas jual dan beli. Konsep ini mencakup berbagai aspek dalam rantai nilai perusahaan, termasuk kegiatan pemasaran, penerbitan faktur, mekanisme pembayaran, pengelolaan transaksi, serta penjaminan keamanan bagi pelanggan. Sehingga sistem E-Commerce ini sangat berpengaruh pada sektor ekonomi karena kegiatan jual beli di era sekarang sudah banyak yang bergantung pada E-Commerce. Tidak menutup kemungkinan bahwa E-Commerce dapat menjadi ancaman bagi penggunanya yang dapat merugikan data pengguna itu sendiri karena adanya oknum yang melakukan ancaman dari E-Commerce berupa Phishing.

Phishing merupakan upaya untuk mendapatkan informasi sensitif pengguna dengan cara membuat email atau situs web palsu yang menyerupai desain dan tampilan situs resmi atau asli (Ramadhan & Nurnawati, 2022). Teknik Phishing banyak cara yang dipakai, beberapa contohnya menurut (Puspitasari & Sutabri, 2023) adalah email spoofing, manipulasi tautan (link), dan Malware. Menurut (Rahmanto, 2019), phising biasanya disebarkan oleh pelaku melalui e-mail korban dan digunakan untuk menyebarkan situs web palsu untuk menjebak korban dengan

tujuan tertentu. Istilah "memancing" berasal dari kata "fishing" dalam bahasa Inggris, yang berarti "memancing".

Menurut (James 2005 dalam Bachtiar, 2023) Langkah awal yang diambil oleh pelaku phishing adalah memanfaatkan algoritma untuk menghasilkan nomor-nomor kartu kredit secara random. Nomor kartu kredit yang dibuat secara acak ini kemudian digunakan untuk membuat akun AOL. Setelah berhasil membuat akun, pelaku memanfaatkannya untuk mengirim spam kepada pengguna lain dan melakukan berbagai aktivitas tidak sah lainnya.

Email spoofing adalah teknik yang menggunakan email dengan cara pelaku menyamar menjadi pelaku yang sah dengan mengirim email ke pengguna, yang biasanya meminta pengguna untuk mengisikan nomor kredit, password, atau mengunduh formulir tertentu menurut (Joshi dalam Puspitasari & Sutabri, 2023).

Manipulasi tautan adalah sebuah teknik yang digunakan pisher dengan mengirim link kepada pengguna dan diarahkan ke web. Ketika pengguna mengakses link tersebut maka situs yang terbuka bukan situs web resmi, melainkan situs yang dimanipulasi oleh pisher. Oleh karena itu, pentingnya untuk melakukan analisis secara mendalam tentang kesadaran masyarakat terhadap ancaman Phishing di E-Commerce agar pengguna terhindar dari Phishing. Banyaknya masyarakat yang kurang memahami tanda-tanda dari adanya Phishing, sehingga para pengguna rentan terkena Phishing.

Pada penelitian ini, diperoleh data yang didapat adalah 46 responden, pertanyaan yang diajukan untuk kuisioner adalah 15 pertanyaan sistem pengambilan datanya menggunakan survey dengan Google Form.

2. Metode Penelitian

Penelitian dilakukan dengan pendekatan deskriptif kualitatif, dimana pengumpulan datanya dilaksanakan melalui studi pustaka dan penyebaran kuesioner. Tujuannya adalah untuk mengukur sejauh mana kesadaran para pengguna e-commerce di Indonesia mengenai bahaya serangan phishing. Jurnal ilmiah yang ditinjau dipilih berdasarkan kriteria yang relevan dan diterbitkan dalam kurun waktu sepuluh tahun terakhir. Proses identifikasi, seleksi, dan analisis jurnal yang terkait dengan phishing di e-commerce merupakan bagian dari proses pengumpulan data.

Salah satu ciri penelitian kuantitatif adalah bahwa datanya ditampilkan tanpa diubah dalam bentuk simbol atau bilangan dan dalam keadaan kewajaran atau keadaan natural.

(1) Meningkatkan kesadaran pengguna e-commerce terhadap ancaman phishing.
(2) Mengidentifikasi kemampuan pengguna untuk mengidentifikasi tanda-tanda phishing.
(3) pendekatan pencegahan untuk menangani ancaman phishing.

3. Hasil dan Pembahasan

Phishing dalam konteks E-Commerce merupakan metode manipulasi dimana pelaku kejahatan menyamar sebagai pihak penjual atau platform E-Commerce yang sah. Para pelaku

biasanya menggunakan berbagai strategi penipuan dengan membuat penawaran-penawaran yang tidak valid untuk menjebak pengguna (Ramadhan & Nurnawati, 2022) . Pelaku phising biasanya melakukan serangan tersebut untuk mendapatkan identitas pribadi pengguna seperti pin, password yang tercantum di akun E-Commerce, dan lainnya, lalu digunakan untuk kepentingan pelaku.

Table 1. Faktor Penyebab terjadinya Phishing

No	Penulis dan Tahun	Faktor penyebab Phisisng
1	(Ramadhan & Nurnawati, 2022)	Pengetahuan pengguna yang minim
2	(Puspitasari & Sutabri, 2023)	Pengetahuan Pengguna yang minim
3	(Nur et al., 2022)	Kesalahan Sistem, pengetahuan pengguna yang minim
4	(Radiansyah & Priyadi, 2016)	Pengetahuan pengguna yang minim, Psikologis
5	(Muftadi et al.,2022)	Pengetahuan pengguna yang minim, Psikologis

Sumber : Artikel Ilmiah (2024)

Menurut (Puspitasari & Sutabri, 2023) , ada beberapa faktor penyebab terjadinya phishing di E-Commerce, yaitu:

1) Kurangnya pengetahuan pengguna yang minim sehingga butuh edukasi agar Masyarakat dapat mengetahui ancaman phishing yang terdapat pada E-Commerce.
2) Kebocoran data karena pengguna yang tidak memiliki pengetahuan tentang phishing, dapat dimanfaatkan pelaku untuk mengambil data pribadi pengguna dari sebuah link yang diberikan untuk menjebak pengguna untuk mengakses link yang tidak jelas.
3) Pengguna yang terkejut dengan penawaran yang dikirim melalui email palsu oleh pelaku phishing.
4) Sistem keamanan dan kebijakan pemerintah yang kurang tegas. Insiden kebocoran data di sektor e-commerce mengindikasikan bahwa platform e-commerce di Indonesia belum sepenuhnya aman, dan lemahnya kebijakan pemerintah memungkinkan terjadinya

kejahatan siber. Walaupun terdapat undang-undang yang mengatur dan memantau keamanan transaksi e-commerce di Indonesia, penerapan kebijakan tersebut masih belum optimal, sebagaimana dibuktikan oleh banyaknya kasus penipuan di e-commerce.

5) Mencegah serangan kejahatan phising dengan cara:
   a) Memeriksa URL atau alamat yang dituju untuk memastikan bahwa alamat di address bar sesuai dengan alamat web e-commerce resmi.
   b) Pastikan untuk memeriksa alamat web yang Anda kunjungi dan hindari tautan yang terlihat mencurigakan.
   c) Ganti password secara berkala,bertujuan agar pelaku phishing sulit untuk melacak password pengguna.
   d) Jangan tertarik pada email yang mencurigakan, terutama yang meminta kata sandi dan data pribadi. Pelaku phishing biasanya mengirimkan email ke pengguna e-commerce.
   e) Jika Anda menerima permintaan untuk informasi rahasia, sebaiknya buka browser baru dan akses situs web resmi organisasi tersebut serta situs web yang dicurigai sebagai phisher. Jika Anda tidak yakin dengan alamat webnya, langkah terbaik adalah mengunjungi situs web resmi organisasi untuk memverifikasinya.
   f) Hindari mengunjungi situs web yang mencurigakan atau tidak terpercaya. Pastikan bahwa URL yang disebutkan di atas adalah alamat resmi milik organisasi tersebut, bukan halaman web palsu yang berada di domain lain.
   g) Waspada terhadap penawaran yang dikirim melalui email pengguna yang terlihat mudah untuk mendapatkannya, kemungkinan itu adalah phishing.
   h) Menggunakan browser filter phishing untuk mengetahui kemungkinan serangan dari phishing. alamat situs website aman biasanya dimulai dengan “https://&#8221”.

Meningkatkan Kesadaran Masyarakat

Langkah penting untuk menghentikan kejahatan siber di sektor e-commerce adalah meningkatkan kesadaran masyarakat terhadap ancaman phishing. Phishing merupakan aksi penipuan yang menipu pengguna dengan memanfaatkan email palsu atau situs web untuk memungkinkan pelaku memperoleh informasi pribadi sensitif dari pengguna (Puspitasari & Sutabri, 2023) . Rekayasa sosial sering digunakan dalam teknik ini untuk menyamar sebagai pihak yang dapat dipercaya untuk mendapatkan data pribadi seperti username, password, dan informasi kartu kredit (Radiansyah & Priyadi, 2016).

Pelaku melakukan manipulasi pada sebuah tampilan website yang sangat mirip dengan website resminya dan memanipulasi tautan seolah-olah tautan dari web resmi, sehingga pengguna yang tidak mengetahui atau menyadari bahwa yang mereka akses adalah bukan web resmi, maka pelaku dengan mudah mendapatkan hak akses yang diberikan oleh korban.

Di Indonesia, sektor e-commerce bertanggung jawab atas 32% kasus phishing (Efendy et al., 2019) . Dianggap penting untuk melindungi pengguna terhadap ancaman ini dengan memberikan instruksi kepada mereka (Ramadhan & Nurnawati, 2022) . Pengguna harus tahu

bahwa phishing dapat terjadi melalui berbagai cara, seperti email, pesan singkat, dan bahkan telepon (Puspitasari & Sutabri, 2023).

Mengidentifikasi Kemampuan Pengguna

Beberapa penelitian telah dilakukan untuk menentukan seberapa baik pengguna dapat membedakan tanda-tanda phishing. Salah satu penelitian menemukan bahwa 53% pengguna yang telah dilatih mampu menemukan situs phishing (Radiansyah & Priyadi, 2016) . Namun, penelitian tersebut mengantisipasi bahwa 86% pengguna mampu menemukan situs phishing (Radiansyah & Priyadi, 2016).

Studi lain menunjukkan bahwa pelatihan terus-menerus dan pelatihan praktis sangat diperlukan untuk meningkatkan kemampuan pengguna untuk mengidentifikasi fitur phishing karena pengguna hanya melihat indikator keamanan pada browser 6% dari waktunya dan lebih fokus pada melihat konten website (Radiansyah & Priyadi, 2016).

Ada banyak jenis phishing yang sering dilakukan pisher pada E-Commerce. Beberapa contohnya menurut (Puspitasari & Sutabri, 2023) yaitu:

1) Email spoofing adalah teknik yang menggunakan email dengan cara pelaku menyamar menjadi pelaku yang sah dengan mengirim email ke pengguna, yang biasanya meminta pengguna untuk mengisikan nomor kredit, password, atau mengunduh formulir tertentu.
2) Manipulasi tautan, sebuah teknik yang digunakan pisher dengan mengirim link kepada pengguna dan diarahkan ke website. Saat pengguna akan mengakses link website tersebut maka situs yang terbuka bukan situs web resmi, melainkan situs yang dimanipulasi oleh pisher.
3) Malware, teknik phishing yang memanfaatkan malware untuk mencuri data, biasanya dilakukan dengan menyisipkan malware pada email yang dikirimkan kepada pengguna. Ketika pengguna mengklik tautan tersebut, malware akan aktif dan mulai bekerja.

Rencana dan Tindakan Pencegahan

Pengguna harus memiliki rencana dan tindakan pencegahan yang jelas untuk menghadapi ancaman phishing. Mereka dapat menggunakan browser dengan filter phishing, menghindari mengklik link yang mencurigakan, mengganti password secara teratur, tidak mencari tau tentang email yang mencurigakan atau memasukkan data diri pada situs yang tidak terpercaya, dan memeriksa dengan cermat URL atau alamat yang ditujuf (Puspitasari & Sutabri, 2023) . Selain itu, penting untuk berhati-hati terhadap penawaran yang terlalu menggiurkan karena ini seringkali merupakan strategi phishing. Selain itu, pengguna harus memastikan bahwa alamat web aman dimulai dengan "https://" dan bahwa browser mereka menampilkan gembok tertutup (Puspitasari & Sutabri, 2023).

Selain itu, tindakan di tingkat sistem juga diperlukan untuk mencegah phishing. Serangan dapat dicegah dengan menggunakan filter email yang dapat membedakan pesan menjadi asli dan palsu (Radiansyah & Priyadi, 2016) . Selain itu, tanda tangan digital dapat

meningkatkan keamanan email. Penggunaan sistem One Time Password (OTP) dapat meningkatkan keamanan transaksi online di bidang perbankan dan e-commerce (Radiansyah & Priyadi, 2016).

Penting untuk diingat bahwa, meskipun ada berbagai opsi teknis, pendidikan pengguna masih sangat penting untuk mencegah phishing. Pengguna harus dididik untuk memahami tanda-tanda phishing di email dan web, memahami bahaya membagikan informasi pribadi di media sosial, dan selalu waspada terhadap strategi rekayasa sosial yang digunakan oleh phisher (Ramadhan & Nurnawati, 2022) . Dengan menggunakan kesadaran, pengetahuan, dan kewaspadaan, pengguna dapat lebih baik melindungi diri mereka dari ancaman phishing yang terus meningkat di dunia e-commerce.

Ada beberapa komponen utama yang harus diperhatikan untuk meningkatkan kesadaran pengguna pada ancaman phishing, yaitu adanya kesadaran (Awarness), adanya kesadaran akan adanya ancaman phishing dapat membuat pengguna lebih berhati-hati saat menggunakan E-Commerce, melakukan pelatihan (Training) untuk melatih keterampilan dalam kinerja keamanan pada E-Commerce, sehingga Tingkat keamanan dapat lebih ketat lagi, melakukan edukasi (Education) agar pengguna memiliki pengetahuan tentang ancaman phishing baik dari cara kerja maupun upaya pencegahannya, dan professional Development untuk membangun professional dalam karir security menurut (NIST dalam Nur et al., 2022).

Pishing dapat dicegah melalui pemasangan filter yang dibagi dua kategori asli (*legitimate*) dan palsu (*fraudulent*) (Castilo, et al dalam Radiansyah & Priyadi, 2016). Fungsi dari filter email ini untuk melindungi dan menjaga pengguna dan pegawainya dari email yang berasal dari pisher yang mengancam untuk mencuri data pengguna. Pendidikan dipandang sebagai salah satu elemen krusial dalam upaya pencegahan kejahatan siber (Drew, et al dalam Syah, 2023).

Solusi lain untuk mencegah ancaman phishing adalah mengganti password secara berkala untuk mempersulit pisher melacak password pengguna, jangan merasa penasaran terhadap email yang mencurigakan, jangan pernah membuka tautan yang mencurigakan dan lakukan identifikasi pada URL apakah tautan tersebut resmi di domain lain seperti www.shopee.net (Puspitasari & Sutabri, 2023).

Pada penelitian ini dilakukan pengumpulan data pada pengguna e-commerce dengan menyebarkan kuisioner. Sampel data yang digunakan adalah 46 responden, berikut adalah diagram dari beberapa pertanyaan yang mewakili sebagian besar dari keseluruhan pertanyaan:

Sumber : Hasl Penelitiaan (2024)

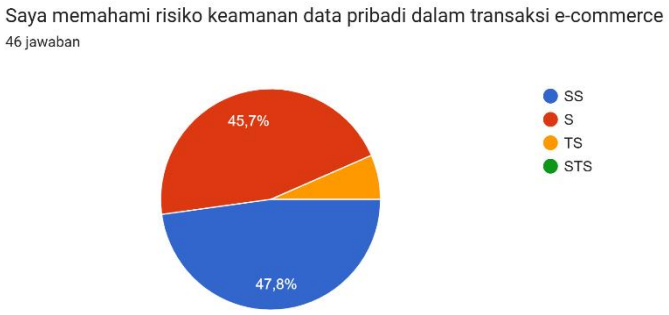
Gambar 1. Pemahaman Mengenai Phising

Pada gambar 1 menunjukan sebanyak 52,2% yang menyatakan “Sangat Setuju” dan 45,7% menyatakan “Setuju”, dengan ini responden memberikan respon positif, dan hanya 2,1% yang menyatakan “Tidak Setuju” dan tidak ada responden yang memilih “Sangat Tidak Setuju”. Hal Ini menunjukkan bahwa mayoritas responden memiliki pemahaman yang baik tentang serangan phising dalam konteks e-commerce, namun terdapat juga yang belum memahami tentang phising, sehingga harus diberikan edukasi kepada orang lain terkait dengan apa itu phising dan bagaimana phising itu bekerja.

Sumber : Hasil Penelitian (2024)

Gambar 2. Ciri-ciri Website E-Commerce Phising

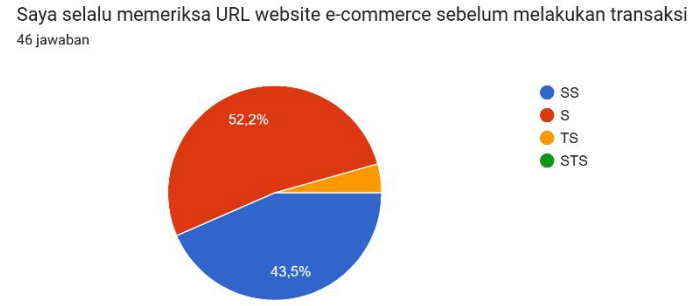
Pada gambar 2 menunjukan bahwa sebanyak 26,1% menyatakan “Sangat Setuju” dan 60,9% menyatakan “Setuju”, ini menunjukkan mayoritas responden mempunyai pemahaman tentang bagaimana ciri-ciri dari website e-commerce yang mengindikasikan phising. Hal ini menunjukkan bahwa responden sangat menyadari potensi ancaman keamanan dalam bertransaksi online. Namun, 13% responden menyatakan tidak setuju, menunjukkan bahwa orang lain mungkin perlu diberikan edukasi lebih lanjut tentang keamanan siber, khususnya bagaimana mengidentifikasi situs e-commerce palsu.



Sumber : Hasil Penelitian (2024)

Gambar 3. Pemahaman Risiko Keamanan Dalam Transaksi Online

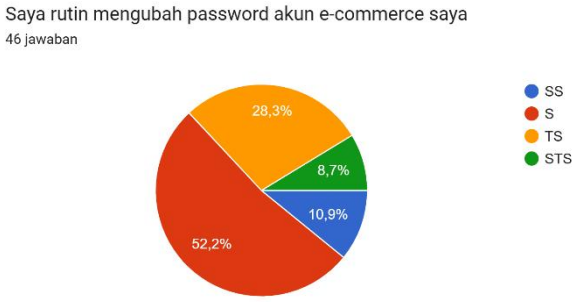
Pada gambar 3 menunjukkan bahwa mayoritas responden mempunyai pemahaman yang baik tentang risiko keamanan dalam bertransaksi online, dengan data 47,8% responden menyatakan “Sangat Setuju” dan 45,7% menyatakan “Setuju”. Ini menunjukkan bahwa sebagian besar pengguna e-commerce sangat menyadari pentingnya menjaga data pribadi mereka saat melakukan transaksi online. Namun, ada beberapa responden yang memilih "Tidak Setuju", menunjukkan bahwa masyarakat masih perlu diedukasi lebih banyak tentang keamanan data pribadi saat melakukan transaksi e-commerce.



Sumber : Hasil Penelitian (2024)

Gambar 4. Apakah Selalu Memeriksa URL Website E-Commerce Sebelum Transaksi

Pada gambar 4 menunjukan mayoritas responden bahwa mereka selalu mengecek URL website e-commerce sebelum melakukan transaksi, dengan data 43,5% yang menyatakan “Sangat Setuju” dan 52,2% menyatakan “Setuju”, sedangkan sisanya berada pada kategori “Tidak Setuju” dan “Sangat Tidak Setuju” dengan presentase yang lebih kecil. Ini mengindikasikan bahwa sebagian besar responden telah memiliki kesadaran yang baik tentang pentingnya memverifikasi URL website terlebih dahulu sebelum melakukan transaksi, yang merupakan salah satu langkah dalam mencegah penipuan dan menjaga keamanan transaksi.



Sumber : Hasil Penelitian (2024)

Gambar 5. Apakah Rutin Mengubah Password Akun E-Commerce

Pada gambar 5 menunjukan perilaku pengguna e-commerce dalam mengubah password akunnya, data menunjukkan sebesar 52,2% yang menyatakan “Setuju” bahwa mereka rutin mengubah password, diikuti 28,3% menyatakan “Tidak Setuju”, sementara itu 10,9% menyatakan “Sangat Setuju”, dan sisanya 8,7% “Sangat Tidak Setuju”. Dengan ini menunjukkan bahwa sebagian besar pengguna e-commerce mempunyai kesadaran tentang pentingnya mengubah password untuk menjaga keamanan akun mereka, meskipun masih terdapat sejumlah responnden yang belum menerapkan cara ini untuk menjaga keamanan akunnya, sehingga diperlukan edukasi lebih lanjut mengenai pentingnya bagaimana mengubah password dapat menjaga keamanan akun.

Sumber : Hasil Penelitian (2024)

Gambar 6. Apakah Pernah Mengklik Tautan Yang Mencurigakan Dalam Email Terkait E-Commerce

Pada gambar 6 menunjukan bahwa mayoritas responden yaitu 52,2% menyatakan “Sangat Setuju” bahwa mereka tidak pernah mengklik tautan yang mencurigakan, diikuti 43,5% menyatakan “Setuju”, sementara sisanya memberikan respon “Tidak Setuju” dan “Sangat Tidak Setuju” dengan presentase yang relatif kecil. Data ini mengindikasikan sebagian responden memiliki kesadaran dalam keamanan digital dan menerapkannya untuk menghindari potensi ancaman phising atau penipuan melalui tautan yang mencurigakan dalam email.

Sumber : Hasil Peneltian (2024)

Gambar 7. Apakah Menggunakan Password Yang Sama Untuk Semua Akun Online

Pada gambar 7 menunjukan bahwa sebagian besar responden 47,8% menyatakan “Setuju” bahwa mereka tidak menggunakan password yang sama untuk semua akun online mereka, diikuti 23,9% menyatakan “Tidak Setuju”, 17,4% “Sangat Setuju”, dan 10,9% “Sangat Tidak Setuju”. Dengan data ini mengatakan mayoritas responden sebanyak 65,2% (gabungan Sangat Setuju dan Setuju) telah memiliki kesadaran yang baik untuk tidak menggunakan password yang identik untuk semua akun mereka, namum masih terdapat juga 34,8% (gabungan Tidak Setuju dan Sangat Tidak Setuju) yang mungkin perlu diedukasi lebih lanjut mengenai risiko keamanan dalam penggunaan password yang sama untuk beberapa akun.

Pada hasil yang disajikan dalam bentuk diagram dan persentase, bisa diidentifikasi bahwa mayoritas responden sebagai pengguna e-commerce memiliki pengetahuan tentang ancaman siber (Cyber crime). Tingkat kesadaran yang tinggi dari persentase tersebut bisa diketahui bahwa pengguna memiliki kesadaran (awareness) terhadap ancaman siber seperti phishing, namun dari mayoritas responden yang memiliki pengetahuan yang cukup tentang phishing masih terdapat beberapa responden yang memahami apa itu phishing, tapi tidak mengetahui Langkah-langkah spesifik untuk melindungi diri dari ancaman phishing.

4. Kesimpulan

Hasil penelitian menunjukkan bahwa banyak pengguna tidak memahami indikator keamanan saat berinteraksi di platform e-commerce, sehingga lebih rentan menjadi korban phishing. Solusi yang disarankan mencakup penerapan teknologi seperti filter email dan tanda tangan digital, serta penguatan edukasi dan pelatihan kepada pengguna. Penelitian ini mengkaji ancaman phishing yang kerap terjadi pada sektor e-commerce di Indonesia.

Phishing adalah bentuk penipuan yang bertujuan mencuri informasi pribadi pengguna dengan cara membuat situs web palsu, mengirim email yang dimanipulasi, menggunakan tautan berbahaya, atau menyebarkan malware. Faktor utama yang menyebabkan phishing meliputi minimnya pengetahuan pengguna, kelemahan pada sistem, dan aspek psikologis.

Untuk mengatasi ancaman ini, penting dilakukan peningkatan kesadaran, pelatihan pengguna, serta penerapan langkah-langkah pencegahan yang efektif.

Daftar Pustaka

Bachtiar, A. (2023). *ANALISIS WEB PHISHING MENGGUNAKAN METODE NETWORK FORENSIC DAN BLOCK ACCESS SITUS DENGAN ROUTER MIKROTIK*.

Efendy, Z., Putra, I. E., & Saputra, R. (2019). ASSET RENTAL INFORMATION SYSTEM AND WEB-BASED FACILITIES AT ANDALAS UNIVERSITY. *Jurnal Terapan Teknologi Informasi*, *2*(2), 135–146. https://doi.org/10.21460/jutei.2018.22.103

Noverdiansyah, R., Khoiriah, A., Kananda, V., Sutoro, M., & Supratikta, H. (2022). Pemanfaatan Teknologi Informasi Berbasis E-Commerce Terhadap Peningkatan Kualitas dan Kinerja SDM Untuk Meningkatkan Profit UKM di Masa Pandemi. In *Jurnal Peradaban Masyarakat* (Vol. 2, Issue 2). https://journal-stiehidayatullah.ac.id/index.php/peradaban

Nur, R., Pusdiklat, R., Siber, B., & Negara, S. (2022). *Cendekia Niaga Journal of Trade Development and Studies Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia*.

Puspitasari, D., & Sutabri, T. (2023). Analisis kejahatan phising pada sektor e-commerce di marketplace shopee. *Jurnal Digital Teknologi Informasi*, *6*(2). https://doi.org/10.32502/digital.v6i2.5653

Radiansyah, I., & Priyadi, Y. (2016). ANALISIS ANCAMAN PHISHING DALAM LAYANAN ONLINE BANKING. *Bulan Januari Tahun*, *7*(1), 1–14. http://ejournal.umm.ac.id/index.php/

Rafki Nazar, M., Timotius Oloando, A., Putri, M. A., Berri, C., & Tazkia, M. (2023). *Pengaruh Perkembangan Teknologi terhadap E-Commerce* (Vol. 7).

Rahmanto, T. Y. (2019). Penegakan Hukum terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik. *Jurnal Penelitian Hukum De Jure*, *19*(1), 31. https://doi.org/10.30641/dejure.2019.v19.31-52

Ramadhan, I. H., & Nurnawati, E. K. (2022). *ANALISIS ANCAMAN PHISHING DALAM LAYANAN E-COMMERCE*. www.shopee.co.id

Syah, R. (2023). STRATEGI KEPOLISIAN DALAM PENCEGAHAN KEJAHATAN PHISING MELALUI MEDIA SOSIAL DI RUANG SIBER. *Jurnal Impresi Indonesia*, *2*(9), 864–870. https://doi.org/10.58344/jii.v2i9.3594