Strategi Penanggulangan Serangan Phishing di Media Sosial

Ananda Dias Sulistyo[1], Bagus Dwi Wicaksono[2], Rais Nur Saputra[3], Rizky Ramadhani[4*]

[1]*jurusan Teknik Informatika/Universitas Duta Bangsa Fakultas Ilmu Komputer Universitas Duta Bangsa*
[1]220103047@mhs.udb.ac.id

[2]*jurusan Teknik Informatika/Universitas Duta Bangsa Fakultas Ilmu Komputer Universitas Duta Bangsa*
[2]220103051@mhs.udb.ac.id

[3]*jurusan Teknik Informatika/Universitas Duta Bangsa Fakultas Ilmu Komputer Universitas Duta Bangsa*
[3]*220103071@mhs.udb.ac.id*

[4]*jurusan Teknik Informatika/Universitas Duta Bangsa Fakultas Ilmu Komputer Universitas Duta Bangsa*
[4]*220103073@mhs.udb.ac.id*

Abstrak— **Serangan phishing di media sosial telah menjadi ancaman signifikan terhadap keamanan informasi pribadi dan bisnis. Strategi penanggulangan serangan phishing ini melibatkan pendekatan multi-lapis yang bertujuan untuk melindungi pengguna dan organisasi dari kerugian akibat phishing. Pertama, edukasi dan kesadaran pengguna adalah langkah awal yang kritis, mencakup pelatihan tentang cara mengenali tanda-tanda phishing dan pentingnya menjaga kerahasiaan informasi pribadi. Kedua, implementasi teknologi keamanan seperti filter spam, verifikasi dua faktor, dan algoritma deteksi phishing berbasis kecerdasan buatan dapat membantu mencegah phishing sebelum mencapai target. Ketiga, kebijakan keamanan yang ketat, termasuk prosedur pelaporan dan respons cepat terhadap insiden phishing, sangat penting untuk meminimalkan dampak serangan. Keempat, kolaborasi antara penyedia layanan media sosial, penegak hukum, dan komunitas keamanan siber dapat memperkuat pertahanan terhadap phishing dengan berbagi informasi dan strategi terbaik. Melalui pendekatan komprehensif yang menggabungkan edukasi, teknologi, kebijakan, dan kolaborasi, serangan phishing di media sosial dapat diminimalkan, sehingga meningkatkan keamanan informasi di era digital.**
Kata kunci: phishing, media sosial, keamanan informasi, deteksi, edukasi pengguna.

Abstract— **Phishing attacks on social media have become a significant threat to the security of personal and business information. The strategy to counteract phishing attacks involves a multi-layered approach aimed at protecting users and organizations from phishing-related losses. First, user education and awareness are critical initial steps, including training on recognizing phishing signs and the importance of maintaining the confidentiality of personal information. Second, the implementation of security technologies such as spam filters, two-factor authentication, and AI-based phishing detection algorithms can help prevent phishing before it reaches the target. Third, strict security policies, including reporting procedures and rapid response to phishing incidents, are essential to minimize the impact of attacks. Fourth, collaboration between social media service providers, law enforcement, and the cybersecurity community can strengthen defenses against phishing by sharing information and best practices. Through a comprehensive approach that combines education, technology, policy, and collaboration, phishing attacks on social media can be minimized, thereby enhancing information security in the digital era.**
Keywords: phishing, social media, information security, detection, user education.

I. PENDAHULUAN

Di era modern sekarang, orang-orang tidak bisa lepas dari yang namanya internet dan gadget. Di tambah, saat ini orang-orang berlomba memperbanyak akun jejaring sosial mereka untuk mencari kepopuleran seperti Facebook, Twitter, Instagram, Snapchat, dan masih banyak lagi. Untuk mendapat berita ter-updateorang-orang juga bisa menjumpai berbagai macam artikel baik dalam maupun luar negeri melalui sebuah laman web ataupun di jejaring sosial juga. Pastinya orang-orang membuka web browser dulu agar bisa pergi ke berbagai jejaring sosial semacam itu. Setiap orang pasti memiliki akun jejaring sosial lebih dari satu. 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. [1] (Wibowo & Fatimah, 2017) Banyak dari pengguna sosial media tidak memikirkan ancaman-ancaman seperti itu. Mereka mengangap hal tersebut sebagai hal yang sepele dan tidak perlu di besar-besarkan. Hingga kini, banyak sekali akun sosial media yang sudah terjebak dalam phishing. Salah satu serangan yang di luncurkan oleh penjahat siber itu adalah dengan menaruh fake link pada akun sosial media

dengan ajakan atau iklan sederhana dan menggiurkan. [9] (Kurniawan, 2024)

1. Apa Itu Phishing?

Phishing adalah serangan yang dilakukan oleh penyerang yang menyamar sebagai entitas terpercaya untuk mendapatkan informasi sensitif dari korban. Mereka menggunakan berbagai metode dan teknik untuk mengelabui korban agar memberikan informasi pribadi, seperti kata sandi, nomor kartu kredit, atau data keuangan lainnya. Phishing biasanya dilakukan melalui email palsu, pesan teks, panggilan telepon, atau bahkan melalui situs web palsu yang meniru tampilan dan nuansa situs web asli. Tujuan utama serangan phishing adalah untuk mendapatkan akses tidak sah ke informasi sensitif korban. Dengan informasi ini, penyerang dapat melakukan pencurian identitas, keuangan, atau bahkan penipuan keuangan.

Serangan phishing juga dapat merusak reputasi bisnis korban, karena penyerang sering menggunakan merek terkenal untuk menarik korban.Media sosial seperti Facebook, Twitter, Instagram, Tiktok dan Whatsapp telah menjadi bagian integral dari kehidupan sehari-hari jutaan orang di seluruh dunia. Platform-platform ini tidak hanya digunakan untuk berkomunikasi dengan teman dan keluarga, tetapi juga untuk berbisnis, berbagi informasi, dan mengakses berbagai layanan. Popularitas dan jangkauan luas media sosial menjadikannya target empuk bagi penyerang phishing yang menggunakan berbagai teknik canggih untuk mengecoh pengguna, seperti membuat situs web palsu yang menyerupai situs asli, mengirim pesan yang tampak sah, dan memanfaatkan informasi pribadi yang tersedia di profil pengguna.

2. Cara Kerja Phishing

Phishing adalah jenis serangan siber di mana penyerang mencoba mendapatkan informasi sensitif dari korban dengan menyamar sebagai entitas yang tepercaya. Di media sosial, phishing menjadi semakin umum karena popularitas dan penggunaan yang luas dari platform-platform ini. Berikut adalah penjelasan lebih mendalam tentang bagaimana phishing bekerja di media sosial :

Tahapan Phishing di media sosial :

1. Pembuatan Akun Palsu

a) Penyerang membuat akun yang menyerupai akun resmi, seperti bank, penyedia layanan online, atau bahkan rekan kerja atau teman. Mereka menggunakan logo, gambar profil, dan nama yang mirip dengan akun asli untuk menipu pengguna.
b) Penyamaran sebagai Orang yang Dikenal Selain institusi, phisher juga bisa menyamar sebagai individu yang dikenal oleh korban, seperti teman, keluarga, atau kolega. Ini sering dilakukan dengan mengambil alih akun seseorang atau membuat akun baru dengan nama dan foto yang sama.

2. Pengiriman Pesan Phishing

a) Pesan yang Mengandung Unsur Mendesak Phisher mengirimkan pesan yang tampak penting atau mendesak. Misalnya, notifikasi tentang aktivitas mencurigakan di akun, permintaan konfirmasi informasi, atau tawaran hadiah dan promosi.
b) Permintaan Bantuan Palsu Pesan bisa juga berupa permintaan bantuan dari "teman" yang mengaku dalam keadaan darurat, seperti kecelakaan atau kehilangan uang saat bepergian.

3. Penggunaan Tautan dan Situs Web Palsu

a) Tautan Berbahaya Pesan phishing biasanya mengandung tautan yang mengarahkan pengguna ke situs web palsu. Situs ini dirancang untuk meniru situs asli dengan sangat meyakinkan, seringkali menggunakan URL yang mirip (misalnya, mengganti huruf 'o' dengan '0').

b) Formulir Pengumpulan Data Situs web palsu ini berisi formulir yang meminta informasi sensitif seperti nama pengguna, kata sandi, nomor kartu kredit, dan data pribadi lainnya.

4. Pengumpulan dan Penyalahgunaan Informasi

a) Pengumpulan Informasi Setelah pengguna memasukkan informasi mereka ke dalam situs web palsu, data tersebut dikirimkan langsung ke phisher.
b) Penyalahgunaan Data, Data yang dikumpulkan kemudian digunakan untuk berbagai tujuan kriminal, seperti Pencurian identitas, Penipuan keuangan dan Penjualan data pribadi

3. Jenis Jenis Serangan Phishing

Serangan phishing di media sosial dapat mengambil berbagai bentuk, masing-masing dengan metode dan taktik yang berbeda untuk menipu pengguna. Berikut adalah beberapa jenis serangan phishing yang umum terjadi di media sosial:

1. Spear Phishing

Spear phising diambil dari kata 'spear' yang berarti tombak, layaknya pemancing yang melakukan teknik memancing dengan tombak untuk memilih ikan tertentu. Yap, serangan ini dilakukan terhadap kelompok tertentu, bisa saja pejabat pemerintah, pelanggan perusahaan tertentu, atau bahkan orang tertentu. Serangan spear phising biasanya dilakukan untuk membobol dan mengakses database khusus guna mendapatkan informasi penting, file rahasia, atau data-data keuangan..[2] (Wijoyo et al., n.d.-a)

2. Clone Phishing

Jenis penipuan ini dilakukan dengan mengkloning website asli untuk mengelabui dan menarik pengguna. Umumnya, web phising ini akan meminta calon korban untuk memasukkan informasi sensitif pada kolom yang disediakan. Padahal kolom ini nantinya akan mengirimkan informasi tersebut ke si penjahat. Setelah itu, pengguna akan diarahkan ke halaman asli tanpa menyadari bahwa ia sudah menjadi korban kejahatan phising. [2] (Wijoyo et al., n.d.-b)

3. Smishing (SMS Phishing)

Smishing menggunakan pesan teks atau SMS untuk mengirim tautan berbahaya atau meminta informasi pribadi. Pesan ini sering kali tampak mendesak, seperti pemberitahuan dari bank atau penyedia layanan lainnya.[3](Kajian et al., 2024)

4. Fake Job Offers

Penyerang mengirim pesan yang menawarkan pekerjaan palsu melalui platform media sosial profesional seperti LinkedIn. Tawaran pekerjaan ini sering kali meminta informasi pribadi atau mengarahkan korban ke situs web palsu untuk melamar.

5. Malvertising

Malvertising melibatkan penggunaan iklan berbahaya yang diposting di platform media sosial. Ketika pengguna mengklik iklan tersebut, mereka diarahkan ke situs web phishing atau situs web yang mengunduh malware ke perangkat mereka.

6. Latar Belakang Masalah

Phishing adalah bentuk serangan siber yang melibatkan penipuan untuk memperoleh informasi sensitif seperti nama pengguna, kata sandi, dan informasi kartu kredit dengan menyamar sebagai entitas yang tepercaya. Seiring dengan meningkatnya penggunaan media sosial, platform-platform ini telah menjadi target utama bagi penyerang phishing. Media sosial menyediakan lingkungan yang ideal bagi penyerang karena tingginya volume interaksi pengguna, rendahnya tingkat kesadaran akan praktik keamanan, dan kecepatan penyebaran informasi yang sangat tinggi. Penyerang menggunakan berbagai teknik canggih untuk mengecoh pengguna, seperti membuat situs web palsu yang menyerupai situs asli, mengirim pesan yang tampak sah, dan memanfaatkan informasi pribadi yang tersedia di profil pengguna. Serangan ini tidak hanya menyebabkan kerugian finansial tetapi juga merusak reputasi individu dan organisasi.

7. Tujuan Penelitian

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis pola serta metode serangan phishing di media sosial, memahami tingkat kesadaran pengguna terhadap ancaman ini, serta mengembangkan strategi penanggulangan yang efektif. Dengan menggunakan metode kuisioner, penelitian ini berupaya mengumpulkan data empiris langsung dari pengguna media sosial untuk mendapatkan wawasan yang mendalam dan komprehensif mengenai dinamika serangan phishing. Selain itu, penelitian ini juga bertujuan untuk mengembangkan model deteksi berbasis kecerdasan buatan (AI) yang mampu mengidentifikasi dan mencegah serangan phishing secara efektif. Hasil penelitian diharapkan dapat memberikan rekomendasi praktis bagi pengguna media sosial, pembuat kebijakan, dan praktisi keamanan siber dalam upaya meningkatkan keamanan dan melindungi pengguna dari ancaman phishing.

Referensi dari penelitian sebelumnya menunjukkan bahwa pendekatan edukasi dan peningkatan kesadaran pengguna merupakan salah satu strategi kunci dalam menanggulangi serangan phishing (Luqman et al., 2018). Selain itu, studi lain juga menekankan pentingnya penerapan teknologi deteksi berbasis AI untuk meningkatkan efektivitas dalam mengidentifikasi dan mencegah serangan phishing di media sosial (Pratama et al., 2021).

II. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode kuisioner untuk mendapatkan pemahaman yang mendalam, komprehensif, dan holistik tentang serangan phishing di media sosial serta cara efektif untuk menanggulanginya. Pendekatan ini dirancang untuk mengumpulkan data langsung dari pengguna media sosial, memungkinkan analisis yang lebih kaya dan data yang lebih akurat untuk menginformasikan strategi penanggulangan yang efektif. Metode kuisioner dianggap sebagai alat yang sangat berguna dalam penelitian ini karena mampu menangkap berbagai dimensi pengalaman pengguna dan persepsi mereka terhadap serangan phishing.

III. HASIL DAN PEMBAHASAN

Pengumpulan data melalui kuesioner dalam penelitian ini terdiri dari dari berbagai jenis pertanyaan yang dirancang untuk mengukur pengetahuan, sikap, dan perilaku pengguna media social terkait dengan serangan phishing. Pertanyaan dalam kuesioner ini mencakup :

1. Usia
2. Jenis Kelamin
3. Tingkat Pendidikan
4. Pekerjaan
5. Seberapa sering anda menggunakan media social?
6. Platform media social apa yang anda gunakan?
7. Apakah anda pernah dengan Phishing?
8. Seberapa yakin anda dalam mengenali serangan Phishing?
9. Apakah anda pernah menjadi korban serangan Phishing?
10. Jika iya, bagaimana anda mengatasi serangan tersebut? (jika tidak kosongkan saja)
11. Apakah anda menggunakan Langkah Langkah berikut untuk melindungi dari phishing? (pilih semua yang relevan)
12. Seberapa efektih Langkah Langkah tersebut dalam mencegah phishing menurut anda?
13. Apakah anda merasa perlu adanya peningkatan dalam strategi penanggulangan serangan phishing yang diterapkan oleh platform media social?
14. Apakah anda memiliki saran untuk meningkatkan strategi penanggulangan serangan phishing dimedia social?
15. Apakah anda memiliki tambahan komentar atau pengalaman yang ingin anda bagikan terkait serangan phishing di media social?

Analis Data :

Data yang dikumpulkan dari kuesioner dianalisis menggunakan Teknik statistic untuk mengindentifikasi pola dan tren yang signifikan. Langkah Langkah analisis data meliputi :

1. Statistik Deskriptif : Menghitung distribusi frekuensi, mean, median, dan modus untuk

setiap pertanyaan dalam kuisioner. Ini membantu untuk memahami profil dasar responden dan pengetahuan serta sikap mereka terhadap phishing.

2. Analisis Korelasi: Mengevaluasi hubungan antara variabel-variabel yang berbeda, seperti antara tingkat pengetahuan tentang phishing dan tindakan keamanan yang diambil oleh responden. Analisis ini membantu mengidentifikasi faktor-faktor yang dapat meningkatkan atau mengurangi risiko terkena serangan phishing.
3. Analisis Regresi: Digunakan untuk memprediksi variabel dependen (misalnya, kerentanan terhadap phishing) berdasarkan satu atau lebih variabel independen (misalnya, pengetahuan tentang phishing, penggunaan otentikasi dua faktor). Analisis ini membantu untuk menentukan faktor-faktor yang paling signifikan mempengaruhi kerentanan terhadap phishing.

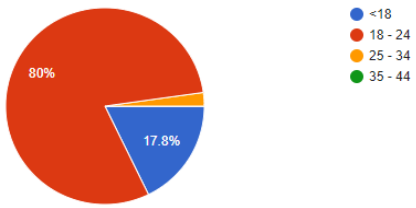
Hasil dan Pembahasan

1. Tingkat Kesadaran Pengguna terhadap Phishing Berdasarkan hasil kuisioner, ditemukan bahwa hanya sekitar 35% pengguna media sosial yang menyadari keberadaan serangan phishing. Hal ini menunjukkan bahwa mayoritas pengguna masih kurang informasi mengenai ancaman ini, sehingga meningkatkan risiko mereka untuk menjadi korban. Penelitian oleh [4](Hong, 2012) juga menegaskan bahwa rendahnya tingkat kesadaran pengguna adalah faktor kunci dalam keberhasilan serangan phishing .
2. Metode Serangan Phishing yang Paling Sering Digunakan Dari data kuantitatif, terungkap bahwa metode serangan phishing yang paling sering digunakan di media sosial adalah melalui pesan langsung yang menyamar sebagai komunikasi dari teman atau kontak terpercaya. Sekitar 45% responden melaporkan pernah menerima pesan semacam ini. Ini sejalan dengan penelitian oleh Basit et al. (2020)[5] (Kashif, 2021)yang mengidentifikasi teknik penyamaran dan rekayasa sosial (social engineering) sebagai metode utama dalam serangan phishing di platform digital .
3. Efektivitas Strategi Penanggulangan Berdasarkan analisis kuantitatif dan kualitatif, strategi yang paling efektif untuk menanggulangi serangan phishing meliputi edukasi dan peningkatan kesadaran, penggunaan teknologi deteksi berbasis AI, serta implementasi kebijakan keamanan yang ketat. Survei menunjukkan bahwa pengguna yang pernah mengikuti pelatihan keamanan siber cenderung lebih mampu mengenali dan menghindari serangan phishing. Studi oleh Farooq et al. (2023)[6] (Farooq, 2023) mendukung temuan ini dengan menekankan pentingnya kombinasi teknologi dan edukasi dalam mencegah serangan phishing

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis serangan phishing di media sosial, serta menyusun strategi yang efektif untuk menanggulanginya. Hasil penelitian dihasilkan dari analisis data kuisioner yang disebarkan kepada pengguna media sosial. Berikut adalah hasil dan pembahasan yang diperoleh dari penelitian ini:

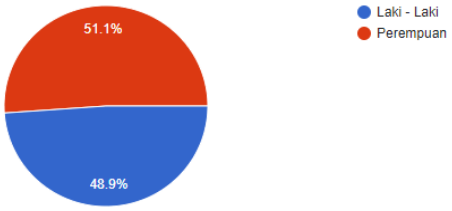
1. Profil Responden

   Pada Gambar 1 Diagram Usia Kuisioner, diisi oleh 45 responden yang terdiri dari berbagai kelompok umur, yaitu remaja (<18 tahun) 17,8%, dewasa muda (18-24 tahun) 80%, dewasa menengah (25-34 tahun) 2,2%.



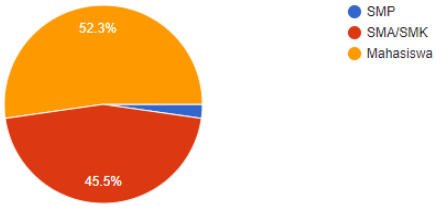
Gambar 1 Diagram Usia

Pada Gambar 2 Diagram Jenis Kelamin Sebanyak 51,1% responden adalah perempuan dan 48,9% adalah laki-laki.



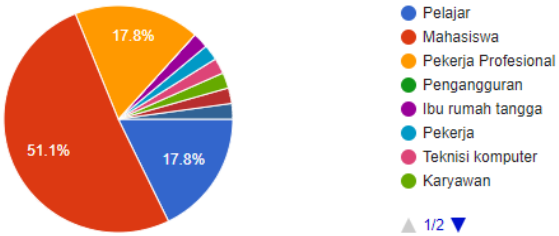
Gambar 2 Diagram Jenis Kelamin

Pada Gambar 3 Tingkat Pendidikan, mayoritas responden memiliki pendidikan Mahasiswa (52,3%), diikuti oleh SMA/SMK (45,5%), dan sisanya memiliki pendidikan SMP (2,3%).



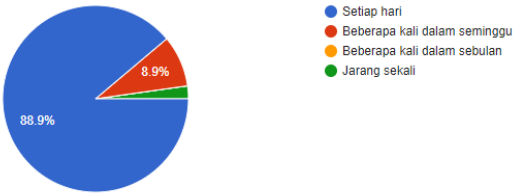
Gambar 3 Tingkat Pendidikan

Pada Gambar 4 Diagram Pekerjaan Mayoritas dari responden belum bekerja dan mayoritas dari persentase nya adalah Mahasiswa (51,1%), dan (17,8%) adalah Pelajar dan Pekerja Profesional, dan (2,2%) yang lain menjawab dengan beragam ada Pengangguran, Ibu Rumah Tangga, Teknisi Komputer, Karyawan, Penjual Kebab dan Belum Bekerja.



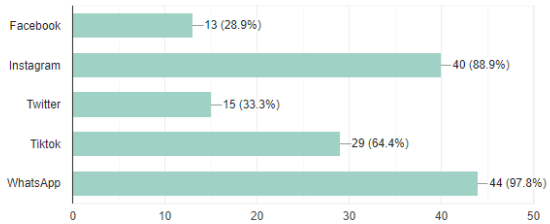
Gambar 4 Diagram Pekerjaan

Pada Gambar 5 Diagram Penggunaan Sosial Media menunjukan Seberapa sering anda menggunakan media sosial Mayoritas responden menjawab setiap hari (88,9%) di jaman yang sekarang apalagi di era modern pasti semua orang punya social media dan sering menggunakannya dan ada beberapa dari responden menjawab beberapa kali dalam seminggu (8,9%) dan ada juga yang jarang sekali menggunakan social media (2,2%).



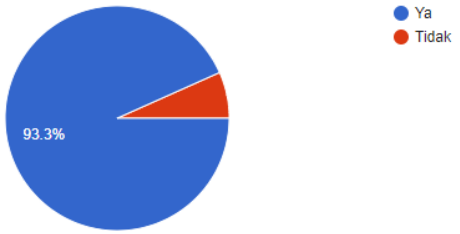
Gambar 5 Diagram Penggunaan Sosial Media

Pada Gambar 6 Presentasi Media Sosial menunjukan platform media sosial apa yang anda gunakan. Pasti di era modern seperti ini banyak yang menggunakan platfrom media social seperti WhatsApp (97,8%) pasti hamper semua orang menggunakan WhatsApp untuk berkomunikasi dengan keluarga, teman, pacar dan saudara. Dan banyak juga yang memakai Instagram (88,9%) untuk kebutuhan sehari hari mereka upload foto/video keseharian mereka atau untuk meng upload foto/video mereka yang ganteng dan cantik. Dan ada juga TikTok (64,4%) banyak dari orang menghabiskan waktu mereka dengan scroll tiktok atau membuat video di TikTok seperti yang kita tahu saat ini. Ada juga Platfrom media social Facebook (28,9%) kebanyakan orang disini menggunakan Facebook untuk memposting jual beli di grup Facebook. Dan yang terakhir ada Twitter (33,3%) Biasanya banyak berita terpanas atau terbaru yang berada di platfrom Twitter.



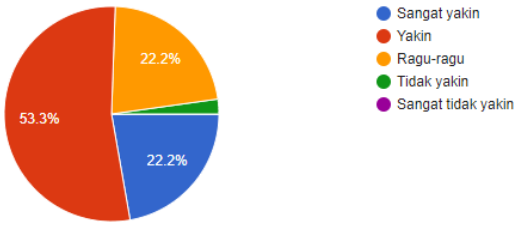
Gambar 6 Persentase Media Sosial

Pada Gambar 7 Mengetahui Tentang Phising menunjukan bahwa mayoritas semua tahu tentang dengan phishing (93,3%) dan ada juga yang tidak tahu mengenai Phishing (6,7%).



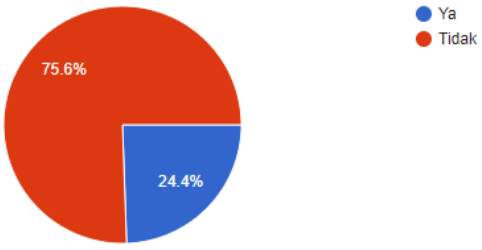
Gambar 7 Mengetahui Tentang Phishing

Pada Gambar 8 Mengenali Serangan Phising Mayoritas menjawab yakin (53,3%) tentang mengenali serangan phishing, beberapa orang menjawab sangat yakin dan ragu ragu (22,2%) dan ada juga yang menjawab tidak yakin (2,2%).



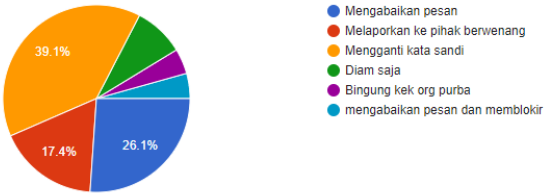
Gambar 8 Mengenali Serangan Phishing

Pada Gambar 9 Korban Serangan Phising Mayoritas belum pernah menjadi korban serangan Phishing (75,6%) dan (24,4) pernah menjadi korban serangan Phishing



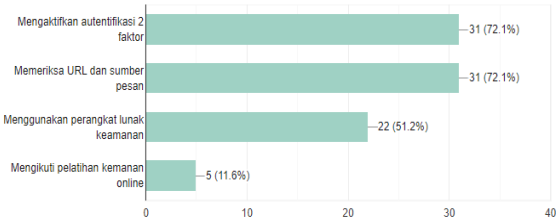
Gambar 9 Korban Serangan Phishing

Pada Gambar 10 Cara Mengatasi Serangan Phising banyak responden yang menjawab mengganti kata sandi (39,1%), ada juga yang mengabaikan pesan (26,1%), ada juga yang melaporkan nya ke pihak yang berwenang (17,4%), bahkan ada yang menjawab diam saja (8,7%) dan sisa nya bingung dan mengabaikan pesan dan memblokir (4,3%).



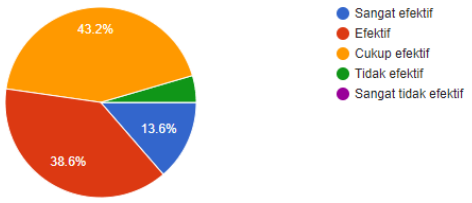
Gambar 10 Cara Mengatasi Serangan Phishing

Pada Gambar 11 Langkah Melindungi Dari Phising, sebanyak (72,1%) responden menjawab mengaktifkan autentifikasi 2 faktor dan memeriksa URL dan sumber pesan, (51,2%) menggunakan perangkat lunak keamanan dan sisanya (11,6%) mengikuti pelatihan keamanan.



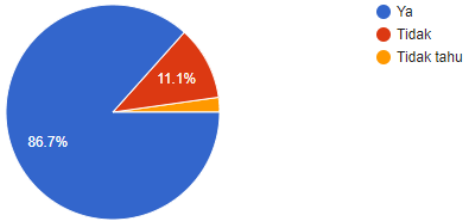
Gambar 11 Langkah Melindungi Dari Phishing

Pada Gambar 12 Seberapa Efektif Langkah Tersebut Mencegah Phishing, Mayoritas responden sudah cukup efektif (43,2%) tentang Langkah Langkah mencegah serangan phishing tersebut, ada yang menjawab efektif (38,6%) dan ada juga yang menjawab sangat efektif (13,6%) dan sisanya menjawab tidak yakin (4,5%).



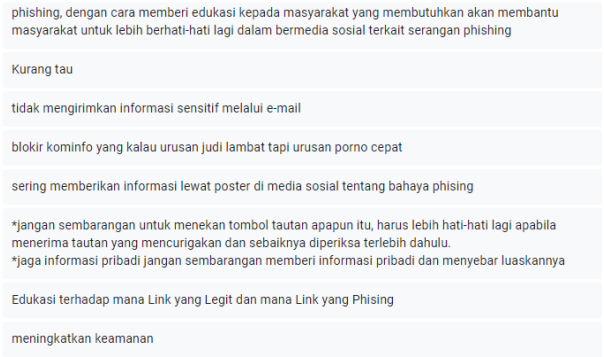
Gambar 12 Seberapa Efektif Langkah Tersebut Mencegah Phishing

Pada Gambar 13 Peningkatan Pencegahan Phising kebanyakan responden menjawab Ya (86,7%) dan (11,1%) menjawab tidak dan sisanya (2,2%) menjawab tidak tahu.



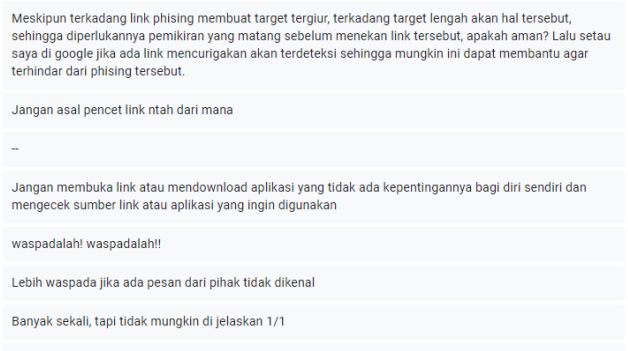
Gambar 13 Peningkatan Pencegahan Phishing

Pada Gambar 14 Saran Untuk Meningkatkan Strategi Pencegahan Phising Banyak responden yang menjawab berbagai variasi dan berbagai jawaban.



Gambar 14 Saran Untuk Meningkatkan Strategi Pencegahan Phishing

Pada Gambar 15 Tambahan Komentar dan Berbagai Pengalaman dari Responden Banyak responden menjawab dengan berbagai jawaban yang berbeda.



Gambar 15 Tambahan Komentar dan Berbagai Pengalaman dari Responden

1. Ciri ciri Phishing
   Phishing adalah bentuk kejahatan siber yang sering kali menggunakan teknik manipulasi psikologis untuk mendapatkan informasi sensitif dari korban. Berikut adalah beberapa ciri-ciri umum dari serangan phishing yang diidentifikasi dalam berbagai penelitian, termasuk studi yang dilakukan di Indonesia:
   a) Alamat Email atau URL yang Mencurigakan Phishing sering menggunakan alamat email atau URL yang terlihat mirip dengan yang asli namun memiliki perbedaan kecil yang sering kali tidak disadari oleh pengguna. Misalnya, [7] (Luqman, 2018) URL yang menggunakan karakter mirip seperti "rn" sebagai pengganti "m" atau menambahkan kata tambahan dalam alamat email.
   b) Permintaan Informasi Sensitif Secara Mendesak Pesan phishing sering kali meminta korban untuk memberikan informasi pribadi atau finansial secara mendesak[7] (Luqman, 2018), misalnya kata sandi, nomor kartu kredit, atau informasi rekening bank, dengan alasan seperti keamanan akun atau hadiah yang akan segera kedaluwarsa.
   c) Penggunaan Bahasa yang Buruk atau Tidak Biasa Banyak email phishing yang mengandung kesalahan tata bahasa, ejaan, atau[8] (Pratama, 2021) kalimat yang terdengar tidak alami. Hal ini bisa menjadi tanda bahwa email tersebut tidak berasal dari sumber yang sah.

d) Lampiran atau Tautan yang Mencurigakan Phishing sering kali menyertakan lampiran atau tautan yang jika diklik atau diunduh dapat menginstal malware pada perangkat korban atau mengarahkan mereka ke situs web palsu yang dirancang untuk mencuri informasi mereka.[8] (Pratama, 2021)
e) Tidak ada informasi kontak yang Jelas
f) Perasaan terlalu bagus untuk menjadi kenyataan, seperti tawaran yang terlalu
g) menggiurkan untuk menarik perhatian Anda.
h) Spoofing dan teknologi pemalsuan
i) Identitas pengirim yang disamarkan [3] (Kajian et al., 2024)

2. Cara Mengatasi Serangan Phishing di Media Sosial berikut ada beberapa cara untuk mengatasi serangan phishing di media sosial sekaligus mengenai penjelasan :

1. Gunakan Aplikasi dengan Keamanan Terupdate: Selalu gunakan aplikasi media sosial[10] (Rosyid, 2017)yang memiliki keamanan terbaru. Pastikan Anda mengunduh aplikasi hanya dari sumber resmi seperti Google Play Store atau Apple App Store. Hindari mengunduh aplikasi dari sumber yang tidak terpercaya.
2. Aktifkan Autentikasi Dua Faktor (2FA): Aktifkan fitur autentikasi dua faktor pada semua akun media sosial Anda. Ini akan menambahkan lapisan keamanan tambahan, di mana selain memasukkan[11] (Sutanto, 2018)kata sandi, Anda juga harus memasukkan kode verifikasi yang dikirim ke perangkat Anda.
3. Periksa Izin Aplikasi: Saat menginstal aplikasi baru, periksa izin yang diminta oleh aplikasi tersebut. Jangan memberikan izin yang tidak relevan dengan fungsi aplikasi. Misalnya, aplikasi media sosial tidak perlu memiliki akses ke kontak atau lokasi Anda jika tidak diperlukan.
4. Selalu Update Sistem Operasi dan Aplikasi: Pastikan sistem operasi handphone dan aplikasi Anda selalu diperbarui ke versi terbaru. [8] (Pratama, 2021) Pembaruan ini biasanya mengandung perbaikan keamanan yang dapat melindungi Anda dari serangan phishing.
5. Hindari Jaringan Wi-Fi Publik: Jangan mengakses akun media sosial atau melakukan transaksi sensitif melalui jaringan Wi-Fi publik. Jika Anda perlu menggunakan Wi-Fi publik, gunakan VPN (Virtual Private Network) untuk mengenkripsi koneksi Anda.
6. Perhatikan Pesan dan Tautan yang Mencurigakan: Jangan sembarangan membuka tautan atau lampiran dalam pesan yang diterima melalui aplikasi pesan atau email. Selalu periksa keaslian pengirim dan hindari mengklik tautan yang mencurigakan.
7. Gunakan Browser yang Aman: Gunakan browser yang memiliki fitur keamanan dan anti-phishing. Pastikan browser Anda diperbarui secara rutin untuk mendapatkan perlindungan terbaru.
8. Jangan Berikan Informasi Pribadi: Jangan memberikan informasi pribadi atau sensitif melalui pesan di media sosial. Perusahaan atau layanan resmi tidak akan meminta informasi pribadi seperti kata sandi atau nomor kartu kredit melalui pesan.
9. Edukasi Diri dan Orang Lain: Selalu tingkatkan pengetahuan Anda tentang phishing dan cara menghindarinya. Edukasi teman dan keluarga Anda tentang bahaya phishing dan langkah-langkah pencegahannya.

3. Pertanggungjawaban Pidana Pelaku Tindak Pidana Phishing.

Pertanggungjawaban pidana bagi pelaku tindak pidana phishing merupakan bagian dari penegakan hukum yang bertujuan untuk memberikan efek jera dan melindungi masyarakat dari ancaman siber. Berikut adalah penjelasan tentang aspek hukum yang terkait dengan tindak pidana phishing:

1. Definisi dan Ruang Lingkup Tindak Pidana Phishing

Phishing adalah tindakan kriminal di mana pelaku menggunakan metode penipuan untuk

memperoleh informasi sensitif seperti kata sandi, nomor kartu kredit, dan data pribadi lainnya dengan menyamar sebagai entitas yang tepercaya. Phishing dapat dilakukan melalui berbagai media, termasuk email, situs web palsu, pesan teks, dan media sosial.

2. Peraturan Perundang-undangan yang Mengatur Tindak Pidana Phishing
   Di Indonesia, tindak pidana phishing diatur dalam beberapa undang-undang yang berkaitan dengan kejahatan siber dan perlindungan data pribadi. Beberapa peraturan yang relevan antara lain:
   a) Pasal 27 ayat (1) UU ITE mengatur tentang larangan distribusi konten yang bersifat menipu.
   b) Pasal 28 ayat (1) UU ITE mengatur tentang larangan penyebaran informasi bohong dan menyesatkan yang mengakibatkan kerugian konsumen.
   c) Pasal 30 UU ITE mengatur tentang larangan akses ilegal ke sistem elektronik.
   d) Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE
      Memperkuat aturan terkait kejahatan siber, termasuk phishing.
3. Sanksi Pidana bagi Pelaku Phishing
   Sanksi pidana bagi pelaku phishing dapat bervariasi tergantung pada jenis tindak pidana dan dampak yang ditimbulkan. Beberapa sanksi yang dapat dikenakan antara lain:
   a) Penjara : Pelaku phishing dapat dijatuhi hukuman penjara sesuai dengan ketentuan yang berlaku dalam UU ITE dan KUHP. Hukuman penjara dapat berkisar dari beberapa bulan hingga beberapa tahun tergantung pada beratnya tindak pidana.
   b) Denda : Selain hukuman penjara, pelaku juga dapat dikenakan denda yang besarannya ditentukan oleh pengadilan berdasarkan tingkat kerugian yang ditimbulkan.
4. Proses Penegakan Hukum
   a) Pelaporan dan Penyelidikan :
      1. Korban tindak pidana phishing dapat melaporkan kejadian tersebut ke pihak berwenang, seperti polisi siber (cyber police).
      2. Penyelidikandilakukan untuk mengumpulkan bukti dan mengidentifikasi pelaku.
   b) Penangkapan dan Penuntutan :
      1. Setelah bukti yang cukup terkumpul, pihak berwenang dapat menangkap pelaku dan membawa kasus ini ke pengadilan.
      2. Jaksa penuntut umum akan menyusun dakwaan dan menuntut pelaku berdasarkan bukti yang ada.
   c) Persidangan :
      1. Pengadilan akan memproses kasus ini dengan mendengarkan argumen dari jaksa dan pembela. Bukti akan dipresentasikan, dan saksi-saksi dapat dipanggil untuk memberikan keterangan.
      2. Hakim akan memutuskan bersalah atau tidaknya pelaku dan menjatuhkan hukuman yang sesuai.

IV. KESIMPULAN

Penelitian ini menyoroti pentingnya strategi yang komprehensif dalam menanggulangi serangan phishing di media sosial. Berikut adalah kesimpulan utama dari penelitian ini:

1. Peningkatan Kesadaran dan Edukasi Pengguna
   Salah satu langkah paling efektif dalam mencegah serangan phishing adalah melalui edukasi yang berkelanjutan dan peningkatan kesadaran pengguna tentang ancaman ini. Pengguna yang teredukasi dengan baik lebih mampu mengenali tanda-tanda phishing dan mengambil tindakan yang tepat untuk melindungi diri mereka. Program pelatihan dan kampanye kesadaran yang berkelanjutan harus menjadi prioritas.

2. Penggunaan Teknologi Keamanan yang Canggih Implementasi teknologi keamanan berbasis AI dan machine learning terbukti efektif dalam

mendeteksi dan mencegah serangan phishing. Teknologi ini dapat menganalisis pola dan mendeteksi anomali yang mungkin terlewatkan oleh pengguna. Selain itu, penggunaan otentikasi dua faktor (2FA) memberikan lapisan perlindungan tambahan yang signifikan.

3. Kebijakan dan Prosedur Keamanan yang Ketat

Platform media sosial harus mengadopsi kebijakan keamanan yang ketat, termasuk enkripsi data dengan SSL/TLS, mekanisme pelaporan yang mudah diakses, dan pemantauan aktif terhadap aktivitas mencurigakan. Dengan memiliki prosedur yang jelas dan responsif, platform dapat mengurangi dampak serangan phishing secara signifikan.

4. Kolaborasi Antar Pemangku Kepentingan

Kerjasama antara penyedia platform media sosial, pemerintah, organisasi keamanan siber, dan pengguna sangat penting untuk menciptakan ekosistem digital yang lebih aman. Pertukaran informasi tentang ancaman baru dan best practices dapat membantu dalam mengembangkan strategi penanggulangan yang lebih efektif.

5. Penelitian dan Pengembangan Berkelanjutan

Penelitian yang berkelanjutan tentang metode baru dalam serangan phishing dan pengembangan teknologi deteksi dan pencegahan yang lebih canggih harus terus didorong. Adaptasi terhadap ancaman yang terus berkembang adalah kunci untuk menjaga keamanan di lingkungan digital.

Dengan mengadopsi strategi-strategi ini, diharapkan dapat mengurangi risiko dan dampak serangan phishing di media sosial. Peningkatan kesadaran, penggunaan teknologi canggih, kebijakan keamanan yang ketat, kolaborasi antar pemangku kepentingan, dan penelitian berkelanjutan adalah elemen-elemen kunci dalam upaya ini. Penelitian ini memberikan dasar yang kuat untuk pengembangan kebijakan dan teknologi yang lebih baik untuk melindungi pengguna dari ancaman phishing di masa depan.

UCAPAN TERIMA KASIH

Kami menyampaikan rasa terima kasih yang tulus kepada semua pihak yang telah memberikan kontribusi dan dukungan dalam penyelesaian penelitian ini. Ucapan terima kasih khusus kami sampaikan kepada:

1. Dosen Pembimbing Bapak Bondan Wahyu Pamekas, S.Kom, M.Kom, yang telah memberikan bimbingan, arahan, dan dukungan yang berharga sepanjang penelitian ini.
2. Universitas Duta Bangsa Khususnya Fakultas Ilmu Komputer yang telah menyediakan fasilitas dan dukungan administratif yang diperlukan.
3. Keluarga dan Teman atas dukungan moral, doa, dan motivasi yang terus mengalir selama proses penelitian ini berlangsung.
4. Para Responden yang telah berpartisipasi dalam pengisian kuesioner dan memberikan data yang sangat berharga bagi penelitian ini.
5. Rekan-rekan Sejawat atas diskusi, saran, dan kritik yang konstruktif dalam penyusunan penelitian ini.

Kami berharap hasil penelitian ini dapat memberikan kontribusi positif bagi pengembangan ilmu pengetahuan dan upaya penanggulangan serangan phishing di media sosial.

REFERENSI

[1] Wibowo, M. H., & Fatimah, N. (2017). ANCAMAN PHISHING TERHADAP PENGGUNA SOSIAL MEDIA DALAM DUNIA CYBER CRIME (Vol. 1).

[2] Wijoyo, A., Saputra, A., Rio Arya Pratama, M., & Rahman, R. (n.d.-a). Analisis Serangan Phising dan Strategi Deteksinya. https://journal.mediapublikasi.id/index.php/jriin

[3] Kajian, J., Dan, H., & Kewarganegaraan, P. (2024). Civilia (Vol. 3, Issue 1). http://jurnal.anfa.co.id

[4] Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74–81. https://doi.org/10.1145/2063176.2063197

[5] Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*, 139-154.

[6] Farooq, A., Naqvi, B., Perova, K., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation Strategies against the Phishing Attacks: A Systematic Literature Review. Computers and Security, 110, 102-125

[7] Luqman, A., Imran, M., & Maulana, I. (2018). Analisis Kesadaran Pengguna Terhadap Serangan Phishing pada Media Sosial. Jurnal Teknologi Informasi dan Ilmu Komputer, 5(2), 120-130

[8] Pratama, A., Rachman, F., & Suryono, S. (2021). Implementasi Kecerdasan Buatan dalam Deteksi Phishing pada Platform Media Sosial. Jurnal Keamanan Siber, 3(1), 45-58

[9] Kurniawan, A., & Nurfiqih, N. (2024). ANCAMAN DAN PENCEGAHAN PHISHING TERHADAP PENGGUNA SOSIAL MEDIA KEPADA SISWA SISWI SMK PUSPITA BANGSA. Praxis: Jurnal Pengabdian Kepada Masyarakat, 4(1), 8-12.

[10] Rosyid, A. R., & Mustofa, K. (2017). Perancangan Sistem Deteksi dan Pencegahan Serangan Phishing Berbasis Sistem Pakar. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 1(1), 1-6.

[11] Sutanto, J. E., & Surendro, K. (2018). Pendekatan Teknik Pengamanan Data Pribadi dalam Mencegah Phishing. Jurnal Sistem Informasi, 10(2), 129-136.