Journal of Internet and Software Engineering Vol: 1, No 4, 2024, Page: 1-11

Phishing di Era Media Sosial: Identifikasi dan Pencegahan Ancaman di Platform Sosial

Lutfi Aziz Febrika Ardy*, Iklima Istiqomah, Angga Eben Ezer, Shelvie Nidya Neyman
IPB University

Abstrak: Era digital telah membawa perubahan signifikan dalam cara komunikasi dan interaksi sosial. Namun, perkembangan ini juga memunculkan tantangan baru dalam bentuk ancaman keamanan siber, salah satunya adalah *phishing*. *Phishing* adalah metode penipuan di mana pelaku kejahatan mencoba memperoleh informasi sensitif seperti kata sandi dan data kartu kredit dengan menyamar sebagai entitas terpercaya. Artikel ini bertujuan untuk mengidentifikasi dan menganalisis ancaman *phishing* yang berkembang di platform media sosial serta memberikan strategi pencegahan yang efektif. Dengan menggunakan alat seperti Kali Linux dan Zphisher, penelitian ini mengeksplorasi teknik-teknik *phishing* yang paling umum digunakan di media sosial. Studi ini juga mengevaluasi efektivitas metode deteksi dan pencegahan yang ada. Hasil penelitian menunjukkan bahwa peningkatan kesadaran pengguna dan implementasi teknologi keamanan yang canggih sangat penting untuk meminimalkan risiko *phishing*. Rekomendasi praktis diberikan untuk pengguna media sosial dan penyedia platform dalam upaya bersama untuk meningkatkan keamanan siber.

Kata kunci: *Phishing*, Kali Linux, Zphisher, Media Sosial.

DOI: https://doi.org/10.47134/pjise.v1i4.2753
*Correspondence: Lutfi Aziz Febrika Ardy
Email: lutfiaziz@apps.ipb.ac.id

Received: 01-08-2024
Accepted: 15-09-2024
Published: 31-10-2024

Abstract: *The digital age has brought significant changes in the way we communicate and interact socially. However, this development has also brought about new challenges in the form of cybersecurity threats, one of which is phishing. Phishing is a method of fraud where criminals try to obtain sensitive information such as passwords and credit card data by posing as trusted entities. This article aims to identify and analyze the growing phishing threats on social media platforms and provide effective prevention strategies. Using tools such as Kali Linux and Zphisher, this study explores the most common phishing techniques used on social media. The study also evaluated the effectiveness of existing detection and prevention methods. The results show that increased user awareness and implementation of advanced security technologies are essential to minimize the risk of phishing. Practical recommendations are provided for social media users and platform providers in a joint effort to improve cybersecurity.*

Keywords: *Phishing, Kali Linux, Zphisher, Social Media.*

Pendahuluan

Internet telah menjadi bagian integral dari kehidupan sehari-hari di era modern ini. Sejak pertama kali dikembangkan pada akhir abad ke-20, internet telah berkembang pesat dan mengubah cara manusia berkomunikasi, bekerja, belajar, dan mengakses informasi. Dengan internet, informasi dari seluruh penjuru dunia dapat diakses dengan mudah dan cepat, memungkinkan terjadinya globalisasi dalam berbagai bidang seperti bisnis, pendidikan, dan hiburan (Scharfman, 2023; Tampati, 2023).

Kemudahan akses internet untuk mendapatkan informasi tentunya menjadi salah satu titik lemah yang bisa dimanfaatkan oleh para peretas, sehingga menjadi ancaman bagi pengguna internet (Atanassov, 2021; Yahva, 2021). Kelemahan ini dieksploitasi oleh peretas untuk melancarkan serangan siber, salah satunya adalah serangan *phishing* (Prakoso & Khamas Heikmakhtiar, 2024). *Phishing* merupakan salah satu jenis aktivitas yang bertujuan untuk memancing seseorang dengan cara mengancam atau menjebaknya (Rubio-Laborda, 2021; Swarnalatha, 2021). Artinya, dengan mengelabui seseorang agar memberikan semua informasi yang dibutuhkan si penjebak secara tidak langsung (Moorthy, 2020; Nielsen, 2021). *Phishing* adalah kejahatan dunia maya (Kim, 2022; Pérez, 2023).

Platform media sosial memiliki kelebihan dan kekurangan dibandingkan platform lainnya. Di Indonesia, beberapa platform media sosial yang paling banyak digunakan adalah Facebook dengan 15% pengguna, Twitter dengan 11% pengguna, dan Instagram dengan 10% pengguna. Meskipun persentase pengguna Instagram tidak terlalu besar, platform ini menjadi sangat populer karena menawarkan fitur audio, video, dan grafis yang menarik. Fitur-fitur ini menjadikan Instagram pilihan favorit bagi pengguna media sosial untuk berekspresi dan berbagi Informasi (Taufiq *et al.*, n.d.). Namun banyak dari masyarakat Indonesia kurang memahami dengan baik ancaman yang mungkin terjadi terhadap mereka di media sosial sehingga banyak dari mereka yang menjadi korban peretasan data, mulai dari data pribadi hingga data keuangan mereka.

Pada tahun 2021, BSSN Indonesia mencatat setidaknya 264 kasus *phishing*. Menurut data tahunan BSSN, *phishing* terbagi menjadi lima jenis, yaitu: Email *Phishing, Spear Phishing, Whaling, Vishing,* dan *Smishing*. Kejahatan ini dapat menyebabkan kerugian nyata karena data korban dapat disalahgunakan untuk melakukan tindakan negatif seperti pencurian dengan identitas korban, peretasan sistem komputer, dan tindakan merugikan lainnya dari segi keamanan (Dwi Prasetyo *et al.*, 2023).

Saat ini, aktivitas kriminal melalui jaringan komputer sedang marak terjadi. Seiring berjalannya waktu, aktivitas kriminal pun semakin meningkat di seluruh dunia. Ada begitu banyak ancaman yang datang melalui komputer saat ini. Salah satunya yang sangat marak terjadi di lingkungan media sosial yang merupakan tempat dimana masyarakat dapat berkomunikasi jarak jauh dan mendapatkan informasi dengan cepat. Hampir semua orang

di dunia menggunakan media sosial untuk bersosialisasi secara online sehingga tidak harus bertemu langsung (Koesyairy, 2019; Olkiewicz, 2019; Xuan, 2019).

Dalam penelitian ini akan dijelaskan mengenai *Phishing* di media sosial yang sering kali memanfaatkan kepercayaan dan ketidakwaspadaan pengguna. Pelaku biasanya membuat akun palsu yang menyerupai akun resmi atau menggunakan teknik rekayasa sosial untuk mengelabui korban. Mereka mengirim pesan atau tautan yang terlihat sah, yang ketika diklik, mengarahkan pengguna ke situs palsu yang meminta informasi pribadi. Serangan ini tidak hanya menargetkan individu, tetapi juga organisasi yang bisa mengalami kerugian finansial dan reputasi. Dampak dari serangan *phishing* bisa sangat merugikan, mengakibatkan pencurian identitas, penyalahgunaan data, dan kerugian finansial yang signifikan (Tri Wahyuni *et al.*, 2023).

Phishing tidak hanya menimbulkan kerugian finansial bagi individu dan organisasi, tetapi juga dapat merusak reputasi dan kepercayaan publik. Selain itu, serangan ini dapat menjadi pintu masuk bagi serangan siber yang lebih serius, seperti *ransomware* atau pengambilalihan akun. Studi menunjukkan bahwa sebagian besar serangan siber yang berhasil dimulai dengan serangan *phishing*, menunjukkan betapa pentingnya pemahaman dan penanganan yang efektif terhadap ancaman ini. Peretasan terhadap aplikasi media sosial, salah satunya seperti WhatsApp, sering terjadi di Indonesia. Sebagai contoh, pada tahun 2022, sebagian besar akun WhatsApp karyawan Narasi TV, sebuah perusahaan jurnalisme dan berita, diretas. Contoh lain terjadi pada tahun 2023, ketika akun WhatsApp selebriti Baim Wong diretas oleh pelaku yang menggunakan modus *phishing*, seperti mengirimkan tautan, gambar, atau aplikasi yang telah dimodifikasi dengan virus berbahaya (Pendidikan & Konseling, n.d.).

Di tengah ancaman yang semakin meningkat, penelitian tentang *phishing* menjadi sangat penting. Penelitian ini mencakup berbagai aspek, mulai dari teknik yang digunakan oleh pelaku, faktor psikologis yang mempengaruhi korban, hingga strategi pencegahan dan mitigasi yang dapat diterapkan. Dengan pemahaman yang lebih baik tentang bagaimana serangan *phishing* dilakukan dan bagaimana individu serta organisasi dapat melindungi diri, diharapkan dapat mengurangi dampak negatif dari serangan ini.

Percobaan dan simulasi dalam penelitian ini dilakukan dengan menggunakan Kali Linux sebagai perangkat lunak pengujian penetrasi pada komputer. Sistem operasi *opensource* ini tersedia secara bebas untuk umum, dirancang khusus untuk berbagai kegiatan keamanan informasi seperti pengujian penetrasi, riset keamanan, forensik komputer, dan rekayasa balik (Mamuriyah *et al.*, 2024). Adapun *tools* dalam Kali Linux yang digunakan ialah Zphisher yang merupakan alat *phishing open-source* yang kuat dan sangat populer saat ini untuk melakukan serangan *phishing* terhadap target. Zphisher lebih mudah digunakan dibandingkan dengan *Social Engineering Toolkit*. Alat ini menyediakan berbagai

template yang memungkinkan pengguna membuat halaman *web phishing* untuk 18 situs populer, termasuk Facebook, Instagram, Google, Snapchat, GitHub, Yahoo, Protonmail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, dan Microsoft. Zphisher juga menawarkan opsi untuk menggunakan *template* khusus sesuai kebutuhan pengguna. Alat ini memudahkan pelaksanaan serangan *phishing* dan dapat digunakan untuk mendapatkan kredensial seperti ID dan kata sandi pada jaringan area luas (Tri Wahyuni *et al.*, 2023).

Tahap awal kegiatan web *phishing* dimulai dengan menentukan calon korban. Biasanya, korban yang disasar adalah pengguna platform pembayaran online seperti Ovo, PayPal, dan lainnya. Selain itu, banyak pelaku *phishing* juga menargetkan pengguna platform dengan celah keamanan. Contoh terbaru adalah pada platform komunikasi Zoom, yang mengalami lebih dari 1000 upaya *phishing* hanya dalam bulan April 2020. Setelah menentukan calon korban potensial, pelaku akan merencanakan tujuan dari kegiatan web *phishing* yang akan dilakukan (Tri Wahyuni *et al.*, 2023).

Metode

Metode penelitian ini menggunakan metode penelitian literatur. Metode ini dipilih untuk mengumpulkan dan menganalisis berbagai sumber pustaka yang relevan dengan topik penelitian. Melalui penelitian literatur, peneliti dapat mengkaji teori, konsep, dan hasil penelitian sebelumnya yang berkaitan dengan topik yang dibahas. Dalam praktik penelitian, tinjauan literatur memiliki peran penting dalam pengembangan ilmu berdasarkan dokumentasi penelitian sebelumnya (vom Brocke *et al.*, 2009). Seiring dengan pesatnya perkembangan ilmu pengetahuan dan pendalaman metode penelitian, khususnya dalam literatur akademik, metode penelitian seharusnya mengikuti perkembangan terbaru dan menghasilkan penelitian yang terdepan dengan nilai bukti kolektif (Yam, n.d.).

Pengumpulan data literatur adalah langkah penting dalam penelitian yang bertujuan untuk mengidentifikasi, menilai, dan mensintesis penelitian yang sudah ada mengenai topik tertentu. Metode ini digunakan untuk mengumpulkan informasi dari berbagai sumber yang relevan dan kredibel, termasuk jurnal ilmiah, buku, laporan, dan sumber online. Tujuannya adalah untuk membangun landasan teori yang kuat, mengidentifikasi celah dalam penelitian sebelumnya, dan mendapatkan wawasan yang mendalam tentang topik yang diteliti (Robin Butarbutar, A., Syamsuddin, A., Bigrit Cleveresty, T., 2024).

Teknik pengumpulan data dalam penelitian literatur ini melibatkan beberapa langkah. Pertama, mengidentifikasi dan menentukan sumber pustaka yang relevan dengan topik penelitian dari perpustakaan, basis data akademik seperti Google Scholar. Kedua, menilai kredibilitas dan relevansi sumber pustaka yang ditemukan, memastikan hanya sumber berkualitas tinggi yang digunakan. Terakhir, mengumpulkan data dari sumber terpilih dan mengorganisasikannya berdasarkan tema atau topik tertentu untuk

memudahkan analisis. Analisis data dalam penelitian literatur ini dilakukan melalui beberapa langkah. Langkah pertama yaitu menyederhanakan dan memilah data yang relevan dari berbagai sumber pustaka, memastikan hanya informasi yang memiliki kaitan langsung dengan tujuan penelitian yang dianalisis lebih lanjut. Lalu penyajian data dalam bentuk narasi yang terstruktur, seperti ringkasan konsep, teori, dan temuan dari penelitian sebelumnya, yang dapat disajikan dalam bentuk paragraf, tabel, atau diagram jika diperlukan. Terakhir, penarikan kesimpulan dari data yang telah dianalisis untuk menjawab rumusan masalah penelitian, dan mengaitkan temuan-temuan dari literatur dengan tujuan penelitian.

Hasil dan Pembahasan

Ada beberapa faktor yang dapat menyebabkan terjadinya insiden keamanan siber. Pertama, faktor manusia sangat berpengaruh karena manusia rentan melakukan kesalahan yang bisa menimbulkan celah keamanan. Kedua, meskipun teknologi keamanan siber sudah sangat canggih, keterbatasan sumber daya manusia yang mengelolanya masih menjadi titik lemah. Ketiga, penjahat dunia maya memiliki keuntungan strategis yang memungkinkan mereka menemukan dan mengeksploitasi kelemahan dalam sistem. Keempat, kejahatan dunia maya menawarkan peluang yang menguntungkan bagi pelakunya. Kelima, kecenderungan manusia untuk lengah dalam mengelola keamanan siber meningkatkan risiko serangan. Terakhir, perkembangan teknologi yang pesat sering kali sulit diimbangi oleh upaya keamanan manusia, menimbulkan pertanyaan apakah AI dapat mengambil alih tugas-tugas keamanan ini (Ferdiansyah *et al*., 2023).

Pengujian penetrasi adalah alat penilaian jaminan yang sangat berharga, memberikan manfaat bagi bisnis dan operasionalnya. Dari perspektif operasional, pengujian penetrasi membantu merumuskan strategi keamanan informasi dengan mengidentifikasi kerentanan secara cepat dan akurat. Pengujian ini menyediakan informasi rinci tentang ancaman keamanan yang aktual, yang dapat dieksploitasi jika tidak ditangani dalam aliran dan proses keamanan organisasi (Hasibuan & Elhanafi, 2022).

Tahapan pengujian pada penelitian ini dilakukan menggunakan *software* Kali Linux. Kali Linux merupakan *software* jenis Linux bersifat *open-source* atau dapat digunakan oleh siapa saja tanpa berbayar (Fadhilah & Adrian, 2023). Maka sangat penting bagi kita untuk mengidentifikasi dan mempelajari suatu kejahatan siber dengan melakukan simulasi atau percobaan, salah satunya dengan menggunakan Kali Linux.

Zphisher adalah alat *phishing open-source* yang sangat kuat dan populer untuk melancarkan serangan *phishing* terhadap target. Zphisher lebih mudah digunakan dibandingkan dengan *Toolkit* Rekayasa Sosial. Zphisher menggunakan port forwarding

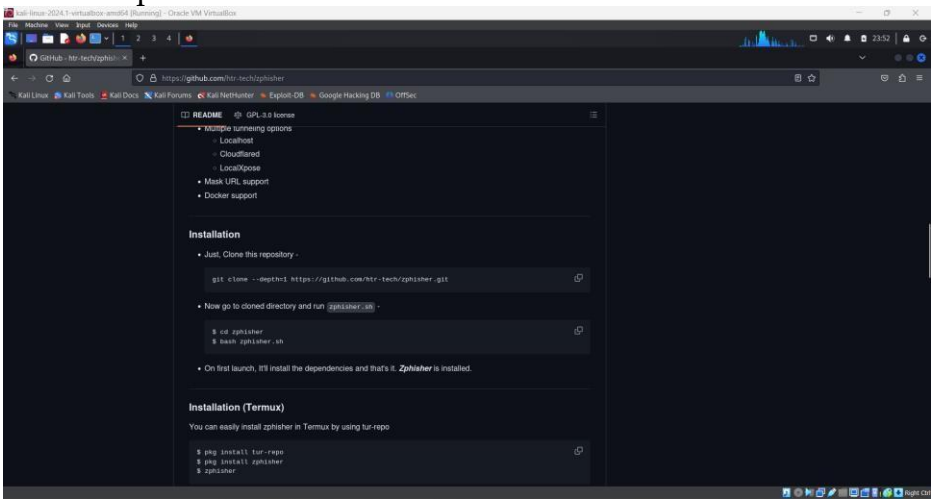
seperti Local Host, Ngrok, dan Cloudflare untuk meningkatkan efisiensi serangan. Alat ini dapat diinstal pada platform Linux dan Android, dan terkenal dengan kemudahan penggunaannya. Menurut penelitian, Zphisher terbukti efektif dalam memperoleh informasi sensitif seperti user ID dan password, menjadikannya alat favorit di kalangan penguji keamanan untuk mengidentifikasi kerentanan dalam sistem. (Erdiyanto, 2023).

Konfigurasi Awal

Pasang Kali Linux di VirtualBox untuk memulai instalasi Zphisher. Setelah masuk Kali Linux melalui VirtualBox dan login maka di bawah ini adalah tampilan awal dari Kali Linux.

Gambar 1. Tampilan Awal Kali Linux

Buka browser dan cari laman "https://github.com/htr-tech/zphisher" untuk melakukan instalasi Zphisher.



Gambar 2. Laman Unduhan Zphisher

Unduh zphisher menggunakan kode yang tertera pada github di atas.

```
┌──(kali㉿kali)-[/home/kali]
└─PS> git clone --depth=1 https://github.com/htr-tech/zphisher.gits
```

Gambar 3. Unduh Zphisher

Untuk menggunakan Zphisher, perlu masuk ke dalam direktori yang sudah dibuat secara otomatis saat instalasi Zphisher tadi, kemudian jalankan perintah bash pada file zphisher.sh.

```
$ cd zphisher
$ bash zphisher.sh
```

Gambar 4. Perintah Menjalankan Zphisher

Penggunaan Zphisher untuk *Phishing* Akun Media Sosial

Tampilan awal dari Zphisher adalah seperti gambar di bawah ini, banyak fitur yang dapat digunakan untuk meniru *template* dari berbagai media sosial yang biasa digunakan. Pada penelitian ini akan dicontohkan menggunakan *template* dari facebook. Untuk itu dapat dipilih nomor 1 untuk tampilan di facebook.

```
 _____     _     _     _
|__  /    | |   (_)   | |
  / / _ __ | |__  _ ___| |__   ___ _ __
 / / | '_ \| '_ \| / __| '_ \ / _ \ '__|
/ /__| |_) | | | | \__ \ | | |  __/ |
/_____| .__/|_| |_|_|___/_| |_|\___|_|
      | |
      |_|                Version : 2.3.5

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch       [21] DeviantArt
[02] Instagram     [12] Pinterest    [22] Badoo
[03] Google        [13] Snapchat     [23] Origin
[04] Microsoft     [14] Linkedin     [24] DropBox
[05] Netflix       [15] Ebay         [25] Yahoo
[06] Paypal        [16] Quora        [26] Wordpress
[07] Steam         [17] Protonmail   [27] Yandex
[08] Twitter       [18] Spotify      [28] StackoverFlow
[09] Playstation   [19] Reddit       [29] Vk
[10] Tiktok        [20] Adobe        [30] XBOX
[31] Mediafire     [32] Gitlab       [33] Github
[34] Discord       [35] Roblox

[99] About         [00] Exit

[-] Select an option :
```

Gambar 5. Tampilan Awal Zphisher

Setelah memilih *template*, di sini terdapat beberapa *template* yang sudah disediakan oleh Zphisher sendiri, untuk contoh kali ini menggunakan *Traditional Login Page*.

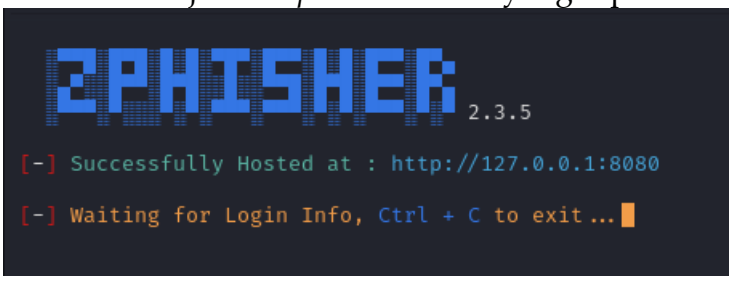
```
[-] Select an option : 1

[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page
```

Gambar 6. Opsi *Template*

Kemudian kita atur jalur ip yang akan menerima informasi korban dari *phishing* ini, contoh kali ini menggunakan *localhost*.

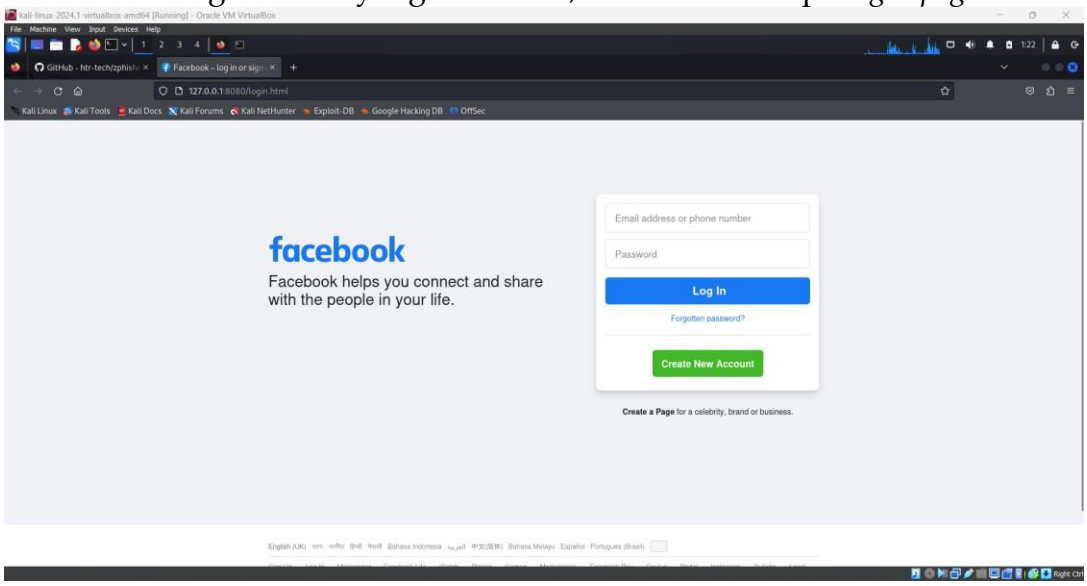
Gambar 7. Opsi IP

Setelah memilih *localhost* sudah dibuat, dan *link phishing* sudah bisa digunakan. IP *localhost* tadi sudah berubah menjadi *template* facebook yang dipilih sebelumnya.



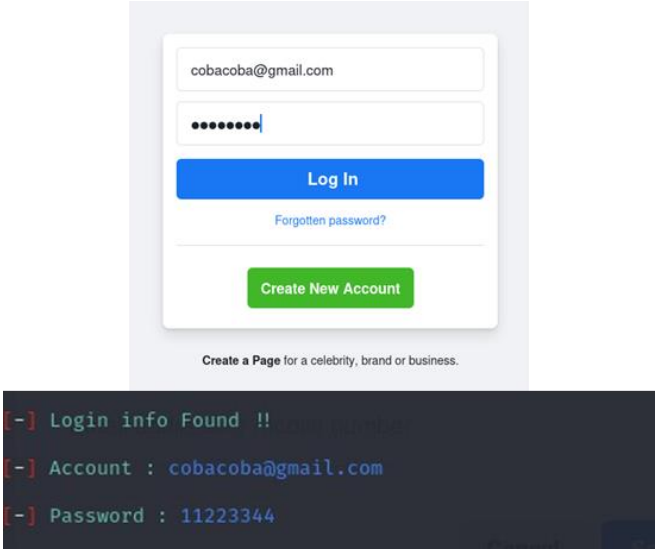
Gambar 8. *Server Phishing*

Jika korban meng-klik *link* yang diberikan, maka akan tampil *login page* dari facebook.



Gambar 9. Laman Facebook Palsu

Setelah itu, ketika korban memasukkan email dan *password* pada *link phishing* ini, maka email dan *password* korban pun diketahui oleh peretas.



Gambar 10. Email dan *Password* Korban

Simpulan

Phishing merupakan ancaman keamanan siber yang signifikan, di mana penyerang menggunakan teknik rekayasa sosial untuk menipu individu agar mengungkapkan informasi pribadi atau kredensial sensitif. Untuk melindungi diri dari serangan *phishing*, langkah pertama adalah mengidentifikasi dan mengimplementasikan solusi keamanan siber yang tepat. Ini mencakup pemilihan alat dan strategi yang efektif dalam mencegah dan mendeteksi serangan *phishing*. Langkah kedua adalah merancang dan melaksanakan simulasi pencegahan serangan *phishing*, yang bertujuan untuk menguji kesiapan dan respons sistem terhadap ancaman tersebut. Langkah ketiga adalah menganalisis dampak setelah implementasi dan simulasi pencegahan, untuk memahami efektivitas langkah-langkah yang diambil dan melakukan penyesuaian yang diperlukan untuk meningkatkan keamanan siber secara keseluruhan. Dengan mengikuti poin-poin ini, organisasi dapat meningkatkan perlindungan terhadap serangan *phishing* dan memperkuat ketahanan sistem mereka terhadap ancaman siber.

Daftar Pustaka

Arista Tri Wahyuni, Ni Komang., Putri Cahayani, Putu., Yogi Wicaksana, I Gusti Ngurah., Bintang Wijayantid, Ida Ayu Kadek. (2023). ANALISIS KERENTANAN KEJAHATAN ONLINE PHISING MENGGUNAKAN TOOLS ZPHISHER, SHELLPHISH DAN WHPHISHER. TEKNIK Vol 3 No. 1 Maret 2023 P-ISSN : 2809-9095 E-ISSN : 2809-9125, Hal 23-31.

Atanassov, N. (2021). Mobile Device Threat: Malware. *IEEE International Conference on Electro Information Technology*, *2021*, 7–13. https://doi.org/10.1109/EIT51626.2021.9491845

Dwi Prasetyo, A., Bayu Seta, H., Wayan Widi, I. P., Ilmu Komputer, F., Pembangunan Nasional Veteran Jakarta, U., Fatmawati No, J. R., Labu, P., & Selatan, J. (2023). JURNAL INFORMATIK Edisi ke-19, Nomor 1.

Fadhilah, F., & Adrian, R. (2023). Implementasi Modul Otomatisasi Penetration Testing Menggunakan Bourne Again Shell Scripting pada Website Aplikasi Stream PT. Intikom Berlian Mustika Berbasis Kali Linux. Jurnal Sistem Dan Teknologi Informasi (JustIN), 11(3), 554. https://doi.org/10.26418/justin.v11i3.67468

Ferdiansyah, D., Alas Majapahit, S., & Muttaqin, M. F. (2023). Rancangan Infrastruktur Virtual Lab Untuk Mendukung Praktikum Keamanan Informasi Berdasarkan National Institute of Standards and Technology (NIST). In Journal of Information Technology Ampera (Vol. 4, Issue 3). https://journal-computing.org/index.php/journal-ita/index

Hasibuan, M., & Elhanafi, A. M. (2022). Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box. Sudo Jurnal Teknik Informatika, 1(4), 171–177. https://doi.org/10.56211/sudo.v1i4.160

Kim, T. (2022). Phishing URL Detection: A Network-based Approach Robust to Evasion. *Proceedings of the ACM Conference on Computer and Communications Security*, 1769–1782. https://doi.org/10.1145/3548606.3560615

Koesyairy, A. A. (2019). Mapping Internal Control of Data Security Issues of BYOD Program in Indonesian Banking Sector. *5th International Conference on Computing Engineering and Design, ICCED 2019*. https://doi.org/10.1109/ICCED46541.2019.9161126

Mamuriyah, N., Prasetyo, S. E., & Sijabat, A. O. (2024). Rancangan Sistem Keamanan Jaringan dari serangan DDoS Menggunakan Metode Pengujian Penetrasi. Jurnal Teknologi Dan Sistem Informasi Bisnis, 6(1), 162–167. https://doi.org/10.47233/jteksis.v6i1.1124

Moorthy, R. S. (2020). Optimal Detection of Phising Attack using SCA based K-NN. *Procedia Computer Science*, *171*, 1716–1725. https://doi.org/10.1016/j.procs.2020.04.184

Nielsen, K. (2021). End-to-end mapping of a spear-phishing attack on hei in eu. *EPiC Series in Computing*, *78*, 89–97. https://doi.org/10.29007/53wk

Olkiewicz, M. (2019). THE SECURITY OF INFORMATION CHANNELS IN BANKING SERVICES. *System Safety: Human - Technical Facility - Environment*, *1*(1), 112–119. https://doi.org/10.2478/czoto-2019-0014

Pendidikan, J., & Konseling, D. (n.d.). Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia (Vol. 4).

Prakoso, G., & Khamas Heikmakhtiar, A. (2024). Analisis Keamanan Jaringan: ARP Spoofing dan DNS Spoofing dengan Metode National Institute of Standards and Technology. Journal on Education, 06(02), 12895–12902.

Pratama Erdiyanto, Rizqy. (2023). PENIPUAN MENGATASNAMAKAN BANK BERBENTUK PHISING. Jurnal Inovasi Global Vol. 1, No. 2, Desember 2023.

Pérez, A. A. E. (2023). FINANCIAL INSTITUTIONS LIABILITY IN CASE OF BANK

ACCOUNTS HACKING. IN PARTICULAR, "PHISING" CASES. *Actualidad Juridica Iberoamericana*, *18*, 1590–1617.

Robin Butarbutar, A., Syamsuddin, A., Bigrit Cleveresty, T. (2024). PEMBUATAN METODE PENILAIAN OTENTIK GUNA MENGEVALUASI KEMAMPUAN BERPIKIR KRITIS MAHASISWA. Jurnal Review Pendidikan dan Pengajaran, Volume 7 Nomor 1, 2024.

Rubio-Laborda, J. F. (2021). Sexist relationships in Generation X and Millennials. *Atencion Primaria*, *53*(4). https://doi.org/10.1016/j.aprim.2021.101992

Rusdi, M. I., Prasti, D. (2019). Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux. Seminar Nasional Teknologi Informasi dan Komputer 2019.

Scharfman, J. (2023). The Cryptocurrency and Digital Asset Fraud Casebook. *The Cryptocurrency and Digital Asset Fraud Casebook*, 1–192. https://doi.org/10.1007/978-3-031-23679-2

Swarnalatha, K. S. (2021). Real-Time Threat Intelligence-Block Phising Attacks. *CSITSS 2021 - 2021 5th International Conference on Computational Systems and Information Technology for Sustainable Solutions, Proceedings*. https://doi.org/10.1109/CSITSS54238.2021.9683237

Tampati, I. F. (2023). Secure Mobile Application for Uniform Resource Locator (URL) Phising Detection based on Deep Learning. *2023 1st International Conference on Advanced Engineering and Technologies, ICONNIC 2023 - Proceeding*, 231–236. https://doi.org/10.1109/ICONNIC59854.2023.10467246

Taufiq, I., Pithaloka, D., Rahmadani, B., & Riau, I. (n.d.). Studi Fenomenologi Media Sosial Sebagai Media Komunikasi Pembangunan Daerah. 11(2), 20–35.

Xuan, C. D. (2019). A framework for vietnamese email phishing detection. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 2258–2264. https://doi.org/10.35940/ijitee.L4843.119119

Yahva, F. (2021). Detection of Phising Websites using Machine Learning Approaches. *2021 International Conference on Data Science and Its Applications, ICoDSA 2021*, 40–47. https://doi.org/10.1109/ICoDSA53588.2021.9617482

Yam, J. H. (n.d.). Kajian Penelitian: Tinjauan Literatur Sebagai Metode Penelitian.