DOI: https://doi.org/10.62017/tektonik

Simulasi Dan Upaya Edukasi Keamanan Siber Menggunakan Situs Web Phishing

Muhammad Ifan Al Aziz *[1]
Muhammad Raihan Afarel N.B [2]
Muhammad Fakhri Alauddin [3]
Shelvie Nidya Neyman [4]

[1,2,3,4] IPB University
*e-mail: ifanalaziz@apps.ipb.ac.id[1], hanfrellraihan@apps.ipb.ac.id[2], fakhri17muhammad@apps.ipb.ac.id[3], shelvie@apps.ipb.ac.id[4]

Abstrak

Serangan phishing telah menjadi ancaman utama dalam dunia cyber. Pendekatan proaktif seperti simulasi phishing kini penting. Simulasi ini memungkinkan organisasi mengukur kesadaran dan kewaspadaan pengguna terhadap serangan phishing serta mengidentifikasi area rentan dalam keamanan informasi. Prosesnya dimulai dengan membuat web kloning dari situs resmi yang sering digunakan. Web kloning tersebut mereplikasi tampilan dan fungsi situs asli untuk meningkatkan keberhasilan simulasi. Pengguna diundang untuk mengakses situs kloning dan diminta memasukkan informasi pribadi. Data yang dikumpulkan kemudian dianalisis untuk mengidentifikasi pola serangan mencurigakan. Analisis melibatkan segmentasi pengguna berdasarkan karakteristik demografis. Evaluasi dilakukan untuk mengukur tingkat kesadaran keamanan pengguna. Hasil simulasi disusun dalam laporan rinci yang mencakup temuan, analisis, dan rekomendasi. Dengan demikian, organisasi dapat mengambil langkah proaktif untuk mengatasi ancaman phishing dan meningkatkan kesadaran pengguna terhadap keamanan informasi.

***Kata kunci**: Phishing, Simulasi , Web Kloning*

Abstract

Phishing attacks have become a major threat in the cyber world. Proactive approaches like phishing simulation are now crucial. This simulation enables organizations to gauge users' awareness and vigilance against phishing attacks, as well as identify vulnerable areas in information security. The process begins with creating a clone website from frequently used official sites. This clone replicates the appearance and functionality of the original site to enhance simulation success. Users are invited to access the clone site and prompted to input personal information. Data collected is then analyzed to identify suspicious attack patterns, involving user segmentation based on demographic characteristics. Evaluation measures users' security awareness levels. Simulation results are compiled into detailed reports encompassing findings, analysis, and recommendations. Consequently, organizations can take proactive steps to address phishing threats and enhance user awareness of information security.

***Keywords**: Phishing, Simulation, Web Cloning*

PENDAHULUAN

Teknologi informasi memiliki potensi untuk merubah realitas ekonomi, budaya, politik, dan hukum. Seiring dengan kemajuannya, teknologi informasi membawa dampak positif atau negatif bagi banyak orang (Kadek Odie Kharisma Putra et al., 2022). Perkembangan internet berjalan seiring dengan kemajuan perangkat lunak yang semakin canggih. Internet berfungsi sebagai media informasi yang berguna untuk mencari informasi terbaru dan dapat diakses secara global. Namun, internet juga bisa dimanfaatkan oleh pelaku kejahatan siber (*cybercrime*) untuk mencuri data pribadi pengguna melalui teknik *phishing* (Aprelia Windarni et al., 2023). Tindakan mengirim email kepada pengguna yang secara palsu mengaku sebagai perwakilan perusahaan sah merupakan upaya untuk menipu pengguna agar menyerahkan informasi pribadi yang kemudian akan digunakan untuk pencurian identitas (Singh, 2007). Kejahatan ini tentu sangat meresahkan masyarakat, karena pelaku phishing adalah pihak yang tidak berwenang. Masyarakat yang menjadi korban phishing akan mengalami kerugian besar terkait privasi, penyalahgunaan (eksploitasi) akibat tindakan peretasan, serta kerugian finansial. Salah satu faktor penyebab

DOI: https://doi.org/10.62017/tektonik

terjadinya phishing adalah kurangnya pemahaman masyarakat tentang keamanan informasi. (Fikri et al., 2022).

Phishing adalah aktivitas yang bertujuan mengancam atau menjebak seseorang dengan metode memancing (MOHD. Yusuf DM et al., 2022). *Phishing* merupakan salah satu bentuk kejahatan siber, di mana pelaku menipu seseorang sehingga tanpa disadari orang tersebut memberikan semua informasi yang diinginkan oleh pelaku. Saat ini, kejahatan siber semakin marak terjadi melalui jaringan komputer. (M. H. Wibowo & Fatimah, 2017). Aksi *phishing* semakin sering terjadi, berdasarkan data global, penipuan bermodus *phishing* mencakup 42% dari semua modus penipuan yang dilaporkan oleh Anti-*Phishing Working Group* (*APWG*) dalam laporan bulanannya (Rustam, 2018). *Phishing* merupakan upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan, data yang dijadikan sasaran dari kegiatan phishing meliputi data pribadi, data akun, dan data finansial seperti nomor rekening maupun kartu kredit, dan lain-lain (Nur et al., 2022). Inilah sebabnya mengapa diperlukan pengukuran tingkat kesadaran pengguna untuk mempertimbangkan langkah selanjutnya dalam membentuk *human firewall* (Daila Sari et al., 2023). Serangan *phishing* telah berkembang di seluruh dunia selama bertahun-tahun, mengalami peningkatan sebesar 65%, dengan jumlah kasus mencapai 1.220.523 pada tahun 2016 dibandingkan dengan tahun sebelumnya APWG, 2017 (Sari & Sutabri, 2023).

Phishing tidak terbatas hanya di Indonesia. Menurut laporan EMC, serangan phishing pada tahun 2013 menyebabkan kerugian finansial global mencapai $5,9 miliar (Rp 80,328 triliun). Serangan phishing ini tidak hanya menimbulkan kerugian finansial. (Radiansyah & Priyadi, 2016). Keamanan terhadap korban kejahatan siber berupa phishing diatur dalam UU ITE dengan sanksi pidana atau denda bagi pelakunya. Perlindungan khusus bagi korban diberikan melalui Undang-Undang Perlindungan Saksi dan Korban, yang memungkinkan korban memperoleh kompensasi setelah mengajukan permohonan yang dipertimbangkan oleh pengadilan (Trisnawati et al., 2023). Topik penelitian *phishing* di media sosial menjadi salah satu publikasi ilmiah yang cukup banyak ditemui, Serangan *phishing* adalah salah satu kasus kejahatan siber yang marak terjadi di kalangan masyarakat, dengan jumlah kasus di Indonesia mencapai 20.330 pada kuartal dua tahun 2023 (R. D. I. P. Sari et al., 2023). Dampaknya terasa signifikan dalam berbagai aspek kehidupan, terutama dalam berbagai media seperti media sosial (Agustian Akbar et al., 2024). Banyaknya kejahatan phishing berpotensi menimbulkan beberapa kerugian, salah satunya adalah kerugian privasi seseorang atau Perusahaan (Subarkah & Ikhsan, 2021).

Website adalah halaman informasi yang menampilkan teks, data gambar diam atau gerak, data animasi, suara, video atau gabungan dari semuanya baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait dimana masing-masing dihubungkan dengan jaringan- jaringan halaman (Agil Nofiyan & Mushlihudin, 2020). *Phishing* adalah penyerangan dengan teknik memanipulasi psikologis target untuk mendapatkan informasi penting. Penyerangan ini berupa penipuan dengan menyebar pesan-pesan palsu yang disisipkan *URL* berbahaya (Wahyuni et al., 2022). Salah satu cara untuk melawan phishing adalah dengan meningkatkan kesadaran dan pendidikan masyarakat (Tabrani et al., 2024). Sehubungan dengan pentingnya kesadaran akan ancaman phishing, peneliti akan melakukan analisis pada kesadaran masyarakat pengguna internet di Indonesia. Penelitian ini akan membahas bagaimana kesadaran terhadap ancaman phishing di kalangan Masyarakat dan diharapkan penelitian ini dapat memberikan informasi mengenai tingkat kesadaran masyarakat Indonesia terhadap ancaman *phishing* (A. Wibowo et al., 2023).

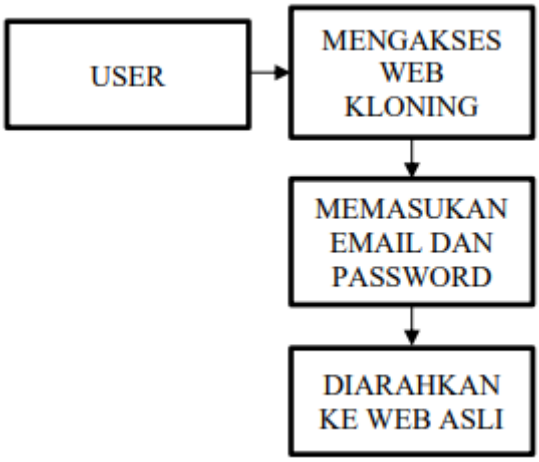
METODE

Metode penelitian merupakan pendekatan yang digunakan untuk menyelesaikan masalah yang sedang diteliti sepanjang proses penelitian (Muftiadi Amin et al., 2022). Metode penelitian ini melibatkan subjek penelitian yang terdiri dari pengguna internet yang sering menggunakan situs web perbankan, email, dan media sosial, khususnya karyawan sebuah organisasi yang menjadi target simulasi phishing. Prosedur penelitian dimulai dengan pembuatan situs web kloning yang menyerupai situs resmi yang sering digunakan oleh target pengguna. Situs kloning ini dirancang untuk terlihat identik dengan situs asli, mencakup tata letak, desain visual, dan fitur

DOI: https://doi.org/10.62017/tektonik

interaktif. Selanjutnya, dilakukan simulasi phishing dengan mengirimkan undangan kepada pengguna untuk mengakses situs kloning dan memasukkan informasi pribadi seperti email dan kata sandi. Data yang dikumpulkan dari pengguna yang terjebak dalam simulasi ini disimpan dalam database yang aman, dan pengguna kemudian diarahkan ke situs web resmi yang asli tanpa menyadari bahwa mereka telah terlibat dalam simulasi phishing. Selama simulasi, aktivitas server dicatat untuk mengidentifikasi pola serangan yang mencurigakan dan perilaku pengguna terhadap serangan phishing.

Instrumen pengumpulan data dalam penelitian ini meliputi simulasi phishing, observasi, wawancara, dan sistem basis data untuk menyimpan informasi yang dimasukkan oleh pengguna selama simulasi phishing. Analisis data dilakukan menggunakan prosedur analisis deskriptif kualitatif dan kuantitatif. Analisis deskriptif kualitatif melibatkan reduksi data, penyajian data, dan penarikan kesimpulan berdasarkan observasi dan wawancara dengan pengguna untuk memahami pola perilaku dan respon mereka terhadap simulasi phishing. Sementara itu, analisis deskriptif kuantitatif menghitung persentase pengguna yang terjebak dalam simulasi phishing dan menganalisis data demografis untuk mengidentifikasi kelompok pengguna yang rentan. Data kuantitatif juga digunakan untuk mengukur efektivitas simulasi phishing dalam meningkatkan kesadaran pengguna terhadap serangan phishing. Hasil dari kedua analisis ini disusun dalam laporan rinci yang mencakup temuan, analisis, dan rekomendasi untuk peningkatan keamanan siber, sehingga organisasi dapat mengambil langkah-langkah proaktif untuk mengatasi ancaman phishing dan meningkatkan kesadaran pengguna terhadap keamanan informasi.



Gambar 1. Flowchart

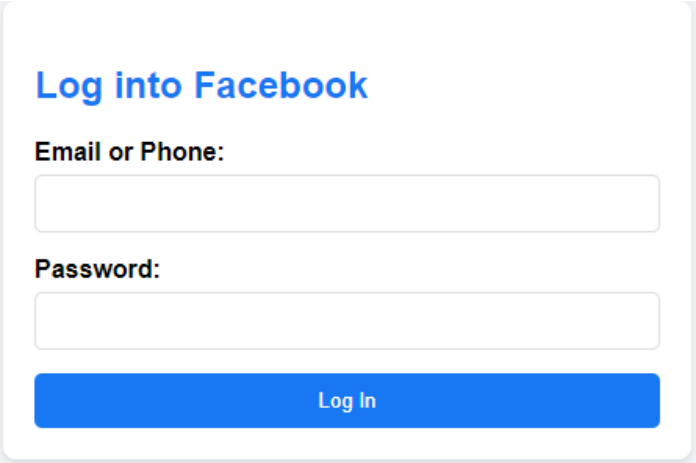
Diagram alir yang ditampilkan menggambarkan proses simulasi phishing yang dilakukan dalam penelitian ini. Proses dimulai dengan pengguna, yang merupakan target dari simulasi phishing, mengakses situs web kloning. Situs web kloning ini adalah replika dari situs web resmi yang sering digunakan oleh target pengguna, seperti situs perbankan, email, atau media sosial. Situs kloning dirancang untuk terlihat identik dengan situs asli guna meningkatkan tingkat keberhasilan simulasi phishing. Setelah mengakses situs web kloning, pengguna diminta untuk memasukkan informasi pribadi mereka, seperti email dan kata sandi, ke dalam formulir login palsu yang disediakan di situs kloning tersebut. Setelah pengguna memasukkan informasi pribadi mereka, mereka akan diarahkan ke situs web resmi yang asli. Proses pengalihan ini dilakukan agar pengguna tidak menyadari bahwa mereka telah terjebak dalam simulasi phishing. Seluruh rangkaian proses ini bertujuan untuk mengukur kesadaran dan kewaspadaan pengguna terhadap serangan phishing, serta untuk mengumpulkan data yang akan dianalisis guna meningkatkan strategi keamanan dan edukasi pengguna tentang ancaman phishing.

HASIL DAN PEMBAHASAN

Ini merupakan tampilan halaman login dari situs phishing yang telah dibuat. Dalam penelitian ini, peneliti membuat kloning dari situs web Facebook. Pengguna akan diminta untuk

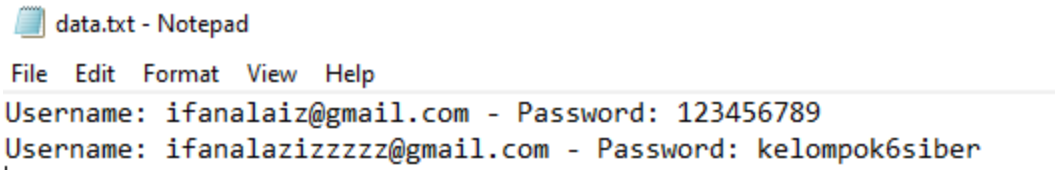
DOI: https://doi.org/10.62017/tektonik

memasukkan email dan kata sandi mereka untuk login ke akun. Jika pengguna memasukkan data email dan kata sandi mereka, maka dapat dipastikan bahwa mereka telah terjebak oleh situs phishing tersebut.



Gambar 2. Tampilan Login

Setelah pengguna melakukan login, data pribadi seperti email dan kata sandi yang mereka masukkan akan tersimpan dalam database yang telah dibuat tanpa sepengetahuan mereka. Selanjutnya, pengguna akan diarahkan ke situs resmi Facebook agar tidak mencurigai bahwa situs sebelumnya yang mereka akses adalah hasil dari kloning.



Gambar 3. Tampilan Data Phishing

Data yang telah diinput oleh pengguna pada situs web kloning akan tersimpan dalam database. Email dan kata sandi yang dimasukkan oleh pengguna dapat diakses oleh pembuat situs web kloning dan berpotensi digunakan untuk kegiatan yang tidak baik, seperti penipuan atau memperoleh akses ke akun bank atau akun lainnya dari pengguna.

Untuk memberikan kesan bahwa website kloning yang telah dibuat mirip seperti tampilan asli dari situs website tersebut maka peneliti membuat tampilan index html yang mirip dengan tampilan website aslinya pada kasus ini peneliti membuat kloning tampilan media sosial yaitu facebook.

```
<body>
    <div class="container">
        <h2>Log into Facebook</h2>
        <form action="login.php" method="POST">
            <label for="username">Email or Phone:</label>
            <input type="text" id="username" name="username" required>
            <label for="password">Password:</label>
            <input type="password" id="password" name="password" required>
            <input type="submit" value="Log In">
        </form>
    </div>
</body>
```

Gambar 4. Code Program HTML

Vol. 1, No. 4 Juli 2024, Hal. 74-80
DOI: https://doi.org/10.62017/tektonik

Kode yang ditampilkan di atas adalah bagian dari halaman web yang dirancang untuk meniru halaman login Facebook. Kode ini menggunakan HTML untuk membuat formulir login yang meminta pengguna memasukkan alamat email atau nomor telepon dan kata sandi mereka. Bagian `<div class="container">` digunakan untuk mengelompokkan elemen-elemen dalam wadah yang rapi. Tag `<h2>` menampilkan judul "Log into Facebook" yang memberi tahu pengguna bahwa mereka sedang berada di halaman login Facebook.

Formulir ini menggunakan metode "POST" untuk mengirim data yang dimasukkan pengguna ke server, yang ditentukan oleh atribut `action="login.php"`. Elemen `<label>` dan `<input>` digunakan untuk membuat dua bidang input: satu untuk alamat email atau nomor telepon dan satu lagi untuk kata sandi. Setiap bidang input diberi atribut `required`, yang berarti pengguna harus mengisi kedua bidang ini sebelum dapat mengirim formulir. Input pertama, dengan `type="text"`, adalah untuk email atau nomor telepon pengguna, sedangkan input kedua, dengan `type="password"`, adalah untuk kata sandi pengguna. Atribut `for` pada label menghubungkan label dengan bidang input yang sesuai melalui id yang sama, seperti `id="username"` dan `id="password"`, untuk memudahkan aksesibilitas dan navigasi.

Terakhir, tombol submit dibuat dengan elemen `<input type="submit">` yang memiliki nilai "Log In", sehingga ketika pengguna mengklik tombol ini, data dari formulir akan dikirim ke server untuk diproses. Namun, dalam konteks penelitian ini, halaman web ini adalah kloning palsu yang digunakan dalam simulasi phishing. Data yang dimasukkan pengguna pada halaman ini akan dikirim ke server yang dijalankan oleh peneliti, bukan ke server Facebook yang asli, dan kemudian data ini akan disimpan di database tanpa sepengetahuan pengguna. Setelah pengiriman data, pengguna akan diarahkan ke situs web Facebook yang asli untuk menyembunyikan fakta bahwa mereka telah memasukkan informasi mereka ke situs web phishing.

```php
<?php
if ($_SERVER["REQUEST_METHOD"] == "POST") {
    $username = $_POST['username'];
    $password = $_POST['password'];

    // Menyimpan data ke dalam file teks
    $file = fopen("data.txt", "a");
    fwrite($file, "Username: " . $username . " - Password: " . $password . "\n");
    fclose($file);

    // Redirect ke halaman login Facebook asli
    header("Location: https://www.facebook.com/login");
    exit();
}
?>
```

Gambar 5. Code Program PHP

Kode PHP yang ditampilkan merupakan bagian dari skrip serangan phishing yang bertujuan untuk menangkap dan menyimpan informasi login pengguna tanpa sepengetahuan mereka. Pertama, skrip memeriksa apakah metode permintaan HTTP yang digunakan adalah "POST", yang menandakan bahwa formulir login telah dikirim oleh pengguna. Kemudian, data `username` dan `password` yang dikirim melalui formulir login diambil dan disimpan dalam variabel `$username` dan `$password`. Selanjutnya, data tersebut disimpan ke dalam file teks bernama `data.txt` dalam mode "append", sehingga data baru akan ditambahkan ke akhir file tanpa menghapus data yang sudah ada. Data `username` dan `password` ditulis ke file tersebut dalam format yang mudah dibaca, dan file ditutup kembali setelahnya. Setelah data disimpan, skrip mengalihkan pengguna ke halaman login Facebook yang asli menggunakan fungsi `header()`. Pengalihan ini dilakukan untuk mengurangi kecurigaan pengguna dengan membuat mereka berpikir bahwa mereka hanya salah memasukkan kredensial dan perlu mencoba lagi di situs resmi. Skrip ini adalah contoh serangan phishing yang sederhana namun efektif, yang

DOI: https://doi.org/10.62017/tektonik

menekankan pentingnya kesadaran dan kewaspadaan terhadap serangan phishing serta praktik keamanan yang baik saat memasukkan informasi pribadi secara online.

Untuk menghindari phishing, penting bagi pengguna untuk memahami dan menerapkan langkah-langkah pencegahan berikut:

1) Pastikan periksa URL situs web dimulai dari https
2) Jangan pernah memasukan informasi pribadi pada situs web yang mencurigakan
3) Jika setelah memasukan data pribadi diarahkan ke situs web lain periksa kembali URL pastikan berada pada web asli dimulai dengan https
4) Gunakan autentikasi dua faktor
5) Perbarui perangkat lunak

KESIMPULAN

Penelitian ini menunjukkan bahwa simulasi phishing menggunakan situs web kloning efektif dalam mengukur kesadaran dan kewaspadaan pengguna terhadap serangan phishing. Dengan mereplikasi halaman login Facebook, peneliti berhasil mengumpulkan data pengguna yang kemudian dianalisis untuk memahami perilaku dan respons terhadap ancaman phishing. Hasil penelitian mengungkapkan bahwa meskipun tampilan situs web kloning sangat mirip dengan aslinya, banyak pengguna masih terjebak dan memasukkan informasi pribadi mereka tanpa menyadari risiko yang ada.

Namun, penelitian ini belum menyentuh beberapa aspek penting. Salah satunya adalah analisis mendalam mengenai faktor psikologis yang mempengaruhi keputusan pengguna untuk memasukkan informasi mereka di situs kloning. Selain itu, penelitian ini juga belum mengeksplorasi sejauh mana edukasi sebelumnya tentang keamanan siber mempengaruhi hasil simulasi phishing. Serta, penelitian ini belum membahas dampak jangka panjang dari pengalaman simulasi phishing terhadap perilaku pengguna di masa mendatang.

Untuk penelitian selanjutnya, disarankan agar peneliti melakukan studi longitudinal yang mengevaluasi perubahan perilaku pengguna setelah berpartisipasi dalam simulasi phishing. Penelitian juga dapat diperluas untuk mencakup analisis terhadap berbagai jenis situs web kloning lainnya, seperti situs perbankan atau e-commerce, guna mendapatkan gambaran yang lebih komprehensif tentang kerentanan pengguna. Selain itu, integrasi pendekatan psikologis dan edukasi keamanan siber yang lebih intensif dapat memberikan wawasan lebih dalam mengenai cara terbaik untuk meningkatkan kesadaran dan kewaspadaan pengguna terhadap serangan phishing.

DAFTAR PUSTAKA

Agil Nofiyan, & Mushlihudin. (2020). *Analisis Forensik pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST)*.

Agustian Akbar, D., Rahdian, M., Kurnia, E., Genggam, R. M., Bintang, S., Purwoko, R., Siber, P., & Negara, S. (2024). *ANALISIS WEB PHISHING MENGGUNAKAN METODE OSCAR FORENSIC (STUDI KASUS : FOLLOWER INSTAGRAM GRATIS) PHISHING WEB ANALYSIS USING THE OSCAR FORENSIC METHOD (CASE STUDY: FREE INSTAGRAM FOLLOWERS)*. *3*(1).

Aprelia Windarni, V., Ferdita Nugraha, A., Tri Atmaja Ramadhani, S., Anisa Istiqomah, D., Mahananing Puri, F., & Setiawan, A. (2023). DETEKSI WEBSITE PHISHING MENGGUNAKAN TEKNIK FILTER PADA MODEL MACHINE LEARNING. In *Information System Journal (INFOS)* | (Vol. 6, Issue 1).

Daila Sari, I., Hariyadi, D., Sahtyawan, R., Indi Kusumaningtyas, N., Informasi, T., & Unjaya, F. (2023). *Analisis Tingkat Security Awareness-Personal Threat Terhadap Ancaman Phishing Dengan Metode Technology Threat Avoidance Theory (TTAT)* (Vol. 16, Issue 2). http://ejournal.unjaya.ac.id/index.php/Teknomatika/

Fikri, A. M., Pertiwibowo, B., Fachrureza, F., Fahri, M. I., & Setyorini, R. I. (2022). Edukasi Kepada Masyarakat Terkait Cara Menghindari Phishing Melalui Pengadaan Webinar. *JPPM (Jurnal Pengabdian Dan Pemberdayaan Masyarakat)*, *6*(1), 113. https://doi.org/10.30595/jppm.v6i1.7543

DOI: https://doi.org/10.62017/tektonik

Kadek Odie Kharisma Putra, I., Made Adi Darmawan, I., Putu Gede Juliana, I., Kunci, K., & Crime, C. (2022). *TINDAKAN KEJAHATAN PADA DUNIA DIGITAL DALAM BENTUK PHISING CRIMINAL ACTS IN THE DIGITAL WORLD WITH A FORM OF PHISHING* (Vol. 5, Issue 2).

MOHD. Yusuf DM, Addermi, & Jasmine Lim. (2022). *Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia* (Vol. 4).

Muftiadi Amin, Agustina Tri Putri Mulyani, & Evi Margaretha. (2022). *Studi kasus keamanan jaringan komputer: analisis ancaman phising terhadap layanan online banking*.

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*.

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/

Rustam, S. (2018). *ANALISA CLUSTERING PHISING DENGAN K-MEANS DALAM MENINGKATKAN KEAMANAN KOMPUTER*.

Sari, P., & Sutabri, T. (2023). Analisis kejahatan online phising pada institusi pemerintah/pendidik sehari-hari. *Jurnal Digital Teknologi Informasi*, *6*(1), 29. https://doi.org/10.32502/digital.v6i1.5620

Sari, R. D. I. P., Rahmah, A., Zuhroh, F., Hidayat, T. R. P., & Rakhmawati, N. A. (2023). ANALISIS BIBLIOMETRIK MENGENAI SERANGAN PHISHING PADA MEDIA SOSIAL MENGGUNAKAN VOSVIEWER. *Jurnal Ilmiah Informatika Komputer*, *28*(3), 230–240. https://doi.org/10.35760/ik.2023.v28i3.9514

Singh, N. P. (2007). *Article in The Journal of Internet Banking and Commerce*. http://www.arraydev.com/commerce/jibc/

Subarkah, P., & Ikhsan, A. N. (2021). Identifikasi Website Phishing Menggunakan Algoritma Classification And Regression Trees (CART). *Jurnal Ilmiah Informatika*, *6*(2), 127–136. https://doi.org/10.35316/jimi.v6i2.1342

Tabrani, S., Safitri, V., Audy Nayla P, P., & Ul Hosnah, A. (2024). *KEJAHATAN PHISHING DITINJAU DARI PERSPEKTIF HUKUM DAN KEJAHATAN SIBER* (Vol. 3, Issue 1). http://jurnal.anfa.co.id

Trisnawati, V., Soesanto, E., Mutiara Tirta, S., & Setiawan, T. A. (2023). KESADARAN KORBAN CYBER CRIME DALAM KASUS PHISING. *JIP)*, *1*, 1093–1098.

Wahyuni, S., Raazi, I. M., & Dwitawati, D. I. (2022). Analisis Teknik Penyerangan Phishing Pada Social Engineering Terhadap Keamanan Informasi di Media Sosial Profesional Menggunakan Kombinasi Black Eye dan Setoolkit. *Jurnal Nasional Komputasi Dan Teknologi Informasi*, *5*(1).

Wibowo, A., Fikri, N., Fauzi, A., Rachman, A. A., Khaerunisa, A., Sari, D. P., Vernanda, P., Hikmah, R., & Fadyanti, T. P. (2023). *Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phishing dalam Layanan Online Banking*. *2*(1). https://doi.org/10.38035/jim.v2i1

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