EPIC (Journal of Electrical Power, Instrumentation and Control)
Teknik Elektro – Universitas Pamulang
Vol. 8, No. 2, Bulan Desember, Tahun 2025, Hal 322 – 329
http://openjournal.unpam.ac.id/index.php/jit
DOI: 10.32493/epic.v8i2.58669

pISSN 2615-0646
eISSN 2614-8595

Implementasi Framework Gophish Berbasis Cloud VPS untuk Simulasi Serangan Phishing Skala Laboratorium

Firman Maulana[1]

[1]*Teknik Elektro, Fakultas Teknik, Universitas Pamulang*
[1]*Jl. Witana Harja No.18b, Pamulang Bar., Kec. Pamulang, Kota Tangerang Selatan, Banten 15417, Indonesia*

[1]*maulana040052003@gmail.com*

INFORMASI ARTIKEL

diajukan : 23-11-2025
revisi : 01-12-2025
diterima : 25-12-2025
dipublish : 31-12-2025

ABSTRAK

Penelitian ini bertujuan untuk mensimulasikan *phishing* dengan *framework* Gophish yang diinstal di *Cloud Virtual Private Server* (*Cloud VPS*). Hal ini sangat penting agar hasil data pada pengujian penetrasi berbasis manusia lebih akurat, karena tidak terjadi putusnya konektivitas ke host, karena halaman arahan dari Gophish dapat diakses di mana saja tanpa harus berada di satu jaringan yang sama. Penelitian ini menggunakan metode eksperimen laboratorium terkontrol, di mana peneliti melakukan simulasi pengujian dengan target yang masih dalam kendali peneliti dan mengedepankan prinsip *Ethical Hacking*, dengan tujuan mengetahui hasil dari simulasi yang dilakukan. Template email dan halaman login menggunakan tiruan dari Instagram, dengan adanya tingkat fleksibilitas yang tinggi pada pengaturan template email dan *landing page* pada Gophish, simulasi ini berhasil menampilkan email dan halaman login yang sangat mirip dengan aslinya. Untuk kredensial simulasi pun dapat terkirim ke server Gophish. Selain itu, halaman loginnya pun dapat diakses di mana pun target berada, tidak harus di jaringan yang sama dengan server Gophish. Pada penelitian ini, dilakukannya simulasi bukan untuk disalahgunakan, tetapi untuk kebutuhan edukasi kepada pengguna internet, khususnya media sosial, agar keamanan data pribadi dapat lebih kuat.

Kata kunci : Phishing; Gophish; Etical Hacking; Cloud VPS

EPIC (Journal of Electrical Power, Instrumentation and Control)
Teknik Elektro – Universitas Pamulang
Vol. 8, No. 2, Bulan Desember, Tahun 2025, Hal 322 – 329
http://openjournal.unpam.ac.id/index.php/jit
DOI: 10.32493/epic.v8i2.58669
pISSN 2615-0646
eISSN 2614-8595

PENDAHULUAN

Saat ini kejahatan siber semakin meningkat (Ariyaningsih et al., 2023). Pada tahun 2025, Widya Security mengatakan secanggih apapun sistem kemanan yang digunakan masih bisa terjadi peretasan seperti pada Pusat Data Nasional Indonesia yang melumpuhkan berbagai layanan publik pada Juni 2024 (Eprianto et al., n.d.), terkadang faktor manusia menjadi penyebab lemahnya sistem keamanan informasi (Wijayanto, 2024).

Teknik serangan *Social Engineering* adalah cara yang sering digunakan untuk mengeksploitasi kelemahan tersebut (Sahay et al., 2025). Salah satu teknik ini yaitu serangan *phishing* (Uffi Novitasari, 2025). Menurut *Indonesian Data and Digital Exchange* (IDADX) Q2 2024–Q1 2025 menunjukkan peningkatan drastis laporan *phishing*: dari 1.598 menjadi 2.470 kasus (+54,5%) pada 2025 (Wahyuningtias, 2025). Serangan *phishing* ini biasanya melalui media sosial (Wibowo Noor Fikri et al., 2023), di mana pelaku memanipulasi agar korban memasukkan kredensialnya melalui *link* yang dikirimkan oleh pelaku (Sahay et al., 2025).

Untuk mengatasi kelemahan pada faktor manusia, edukasi terhadap serangan *phishing* ini perlu ditingkatkan guna meminimalisir bocornya data sensitif pengguna internet, khususnya di media sosial (Putri et al., 2024). Selain itu, harus dilakukan pengujian terhadap manusianya guna mengetahui hasil dari edukasi yang diterapkan (Fikrah Kristo Fotriman Waruwu et al., 2025).

Untuk melakukan pengujian tersebut, tentunya dibutuhkan alat yang digunakan dalam pembuatan kampanye *phishing*. Ada beberapa alat yang dapat digunakan dalam pembuatan kampanye *phishing*, salah satunya adalah Gophish . Gophish adalah alat yang sangat mudah digunakan untuk pengujian dikarenakan banyak fitur yang sangat membantu untuk kebutuhan analisis kampanye *phishing* (Wibowo & Hidayat, 2024). Pada penelitian (Wibowo & Hidayat, 2024) Pengujian terhadap SDM dilakukan menggunakan Gophish, pada penelitian tersebut pengujian berhasil dilakukan, hasil kesimpulan peneliti tersebut sebanyak 86,7% karyawan berhasil mengidentifikasi dan melaporkan email phishing secara benar, 13,3% membukanya, 13,3% mengeklik tautan didalamnya, dan 8% memasukan kredensialnya, tetapi pada penelitian tersebut, pengujian menggunakan jaringan local, dimana yang di uji belum tentu memakai jaringan yang sama secara terus-menerus, dan hal ini bisa mempengaruhi validnya hasil dari pengujian, karena jika tidak terhubung dengan jaringan yang sama dengan server Gophish, target tidak akan bisa mengakses atau mengirim kredensial ke server Gophish dan Gophish tidak bisa mengetahui status dari kampanye karena terputusnya jaringan target, selain itu klaim peneliti tersebut jika 86,7 % berhasil melaporkan dengan baik tidak sesuai dengan timeline yang di hasilkan pada pengujiannya, dimana timeline tersebut tidak ada status terkena laporan, pada email yang dikirimkan.

Pada penelitian (Boy Setyawan Zalukhu et al., 2025), simulasi kampanye phishing dapat dilakukan dengan baik menggunakan alat Zphisher dan server Ngrok. Link phishing dapat diakses dari mana-mana tanpa harus menghidupkan laptop penguji 24 jam. Tetapi pengujian

EPIC (Journal of Electrical Power, Instrumentation and Control)
Teknik Elektro – Universitas Pamulang
Vol. 8, No. 2, Bulan Desember, Tahun 2025, Hal 322 – 329
http://openjournal.unpam.ac.id/index.php/jit
DOI: 10.32493/epic.v8i2.58669
pISSN 2615-0646
eISSN 2614-8595

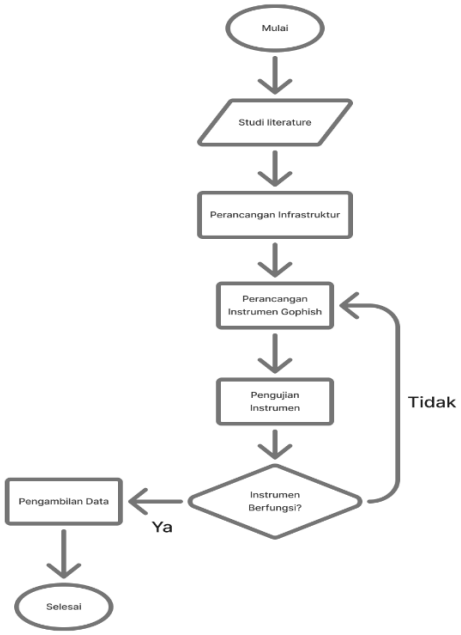
menggunakan Zphisher dinilai kurang efektif jika untuk pengujian massal, karena tidak dapat mengirim kampanye *phishing* secara serentak dan alat ini hanya membantu dalam pembuatan link *phishing* saja.

Dari kedua penelitian tersebut memiliki beberapa hal yang harus diperbaiki, dimana proses suatu pengujian harus berjalan secara efektif dan efisien serta mendapatkan hasil uji yang valid, maka dari itu, penelitian ini bertujuan untuk mensimulasikan kampanye phishing agar lebih efektif dan efisien serta lebih valid hasil ujinya jika akan dilakukan pengujian secara serentak, untuk meningkatkan keamanan data pribadi. Pada simulasi ini akan menggunakan *framework* Gophish yang di instalasi di *VPS*, sehingga penguji tidak perlu menyalakan leptop 24 jam, karena server Gophish berjalan 24 jam di *VPS* dan dapat diakses dimanapun berada (Gea et al., 2023). Pada simulasi yang akan dilakukan, peneliti tidak menyebarkan kampanye phishing secara publik. Peneliti menggunakan email yang masih dalam kendali peneliti agar dapat mengetahui langsung hasil dari Gophish ini. Selain itu, bertujuan mengedepankan prinsip *Ethical Hacking* dan untuk kepentingan edukasi, bukan untuk melakukan serangan terhadap orang lain.

METODOLOGI

A. Tahapan Penelitian

Penelitian ini menggunakan metode eksperimen laboratorium terkontrol, di mana peneliti melakukan simulasi pengujian dengan target yang masih dalam kendali peneliti, dengan tujuan mengetahui hasil dari alat yang digunakan, sehingga kredensial yang dikirimkan dari target adalah fiktif, untuk tahapan dalam penelitian ini, yaitu pada Gambar 1 berikut.



Gambar 1 Tahapan Penelitian

Penelitian diawali dengan studi literatur, kemudian perancangan infrastruktur, yaitu *VPS* dan server Gophish, kemudian perancangan instrumen pada Gophish untuk kebutuhan kampanye phishing, setelah perancangan instrumen selesai, dilakukan pengujian fungsional setiap instrumen guna mendapatkan hasil yang diinginkan, dan terakhir yaitu pengambilan data setelah seluruh instrumen dapat berfungsi sesuai yang diinginkan.

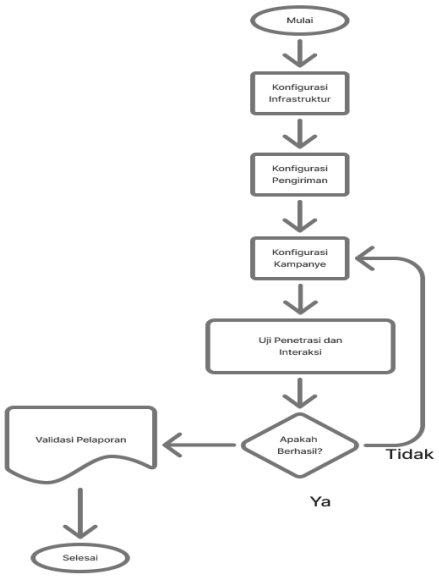
B. Tahapan Simulasi *Phishing*

Pada penelitian ini, alat yang digunakan untuk membuat kampanye *phishing* adalah Gophish. Alasan penggunaan Gophish ini adalah mudahnya dalam penggunaan (Sahay et al., 2025). Kita dapat mengatur *template* email, *template*

EPIC (Journal of Electrical Power, Instrumentation and Control)
Teknik Elektro – Universitas Pamulang
Vol. 8, No. 2, Bulan Desember, Tahun 2025, Hal 322 – 329
http://openjournal.unpam.ac.id/index.php/jit
DOI: 10.32493/epic.v8i2.58669
pISSN 2615-0646
eISSN 2614-8595

halaman login, dan profil pengirim. Selain itu, Gophish dapat mengirim kampanye secara serentak dalam jumlah banyak, sehingga jika akan dilakukan pengujian dengan jumlah target yang banyak dan secara massal, dapat dilakukan secara efektif (Wibowo & Hidayat, 2024) .

Pada simulasi ini, Gophish diinstal di dalam *VPS* dari Biznet. Penggunaan *VPS* ini bertujuan agar simulasi serangan bisa dilakukan 24 jam tanpa menghidupkan laptop, karena Gophish berjalan di server Biznet (Gea et al., 2023). Hal ini sangat penting jika akan dilakukan pengujian secara langsung ke target, karena tidak akan terjadi terputusnya jaringan, di mana target yang diuji tidak lagi menggunakan jaringan yang sama dan terputusnya akses komunikasi host dengan client, sehingga target tidak bisa mengakses website dan kredensial tidak bisa terkirim ke host (server Gophish). Hal ini akan membuat hasil analisis dari pengujian penetrasi berbasis manusia menjadi kurang akurat. Proses simulasi *phishing* ini memiliki beberapa tahap, yaitu pada Gambar 2 berikut.



Gambar 2 Tahapan Simulasi *Phishing*

1. Konfigurasi Infrastruktur

   Pada proses ini dilakukan persiapan Ubuntu di *VPS* Biznet, kemudian instalasi Gophish dan konfigurasi file *config.json* pada Gophish, agar server Gophish dapat diakses secara publik dengan ip *VPS*, karena *VPS* Biznet ini hanya menyediakan *terminal* saja. Tujuan penggunaan Gophish ini adalah karena mudahnya penggunaan dan efektivitas yang tinggi, di mana template email dan *landing page* dapat dibuat sesuai keinginan penguji karena fitur HTML editor dan import *website*. Selain itu, Gophish ini dapat mengirimkan kampanye secara serentak.

2. Konfigurasi Pengiriman

   Pada proses ini, peneliti melakukan konfigurasi server SMTP menggunakan server Gmail. Peneliti membuat *password* untuk aplikasi pada halaman Kelola Akun Google, kemudian melakukan konfigurasi profil pengirim pada Gophish.

3. Konfigurasi Kampanye

   Pada proses ini, peneliti melakukan konfigurasi beberapa bagian pada Gophish sebelum meluncurkan kampanye, yang terdiri dari template email, template *landing page*, dan email target yang akan dikirimkan dalam kampanye phishing. Pada konfigurasi template email dan *landing page* ini, peneliti menggunakan tiruan dari Instagram, di mana target akan menerima peringatan agar melakukan perubahan *password* melalui link yang dikirim lewat email.

EPIC (Journal of Electrical Power, Instrumentation and Control)
Teknik Elektro – Universitas Pamulang
Vol. 8, No. 2, Bulan Desember, Tahun 2025, Hal 322 – 329
http://openjournal.unpam.ac.id/index.php/jit
DOI: 10.32493/epic.v8i2.58669
pISSN 2615-0646
eISSN 2614-8595

4. Uji Penetrasi dan Interaksi

   Pada tahap ini, peluncuran kampanye *phishing* dilakukan. Target pada uji coba ini menggunakan email yang masih dalam kendali peneliti guna mengamati hasil dari Gophish. Jika terjadi eror, peneliti akan mengonfigurasi ulang Gophish hingga dapat mengirimkan kredensial target.

5. Validasi Pelaporan

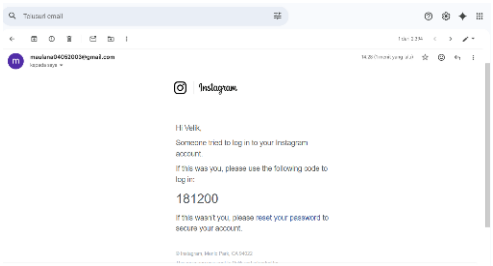
   Pada tahap akhir simulasi ini, peneliti melakukan validasi apakah kredensial sesuai dengan yang diisi pada halaman login atau tidak dan mengambil kesimpulan dari simulasi ini.

HASIL DAN PEMBAHASAN

Pada tahap ini akan dipaparkan hasil dari simulasi serangan *phishing* dengan menggunakan framework Gophish,yang terdiri dari seluruh hasil simulasi, yaitu sebagai berikut:

A. Hasil Template Email Gophish

Pada simulasi ini, template yang dibuat sangat mirip dengan aslinya, yaitu email peringatan dari Instagram. Hal ini menjadi sangat penting karena merupakan langkah awal untuk meyakinkan target agar mengeklik link pada email tersebut untuk diarahkan ke halaman login tiruan dari Instagram. Pada Gambar 3 berikut hasilnya.

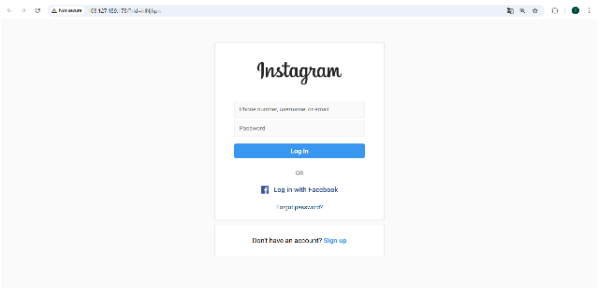


Gambar 3 Hasil Email Tiruan Instagram

Tetapi nama pengirim dari email tersebut kurang meyakinkan, karena pada penelitian ini menggunakan SMTP dari gmail, dimana adanya kebijakan keamanan ketat Google (*DMARC* dan *Anti-Spoofing*)(Google, 2024), sehingga tidak melakukan penyamaran pada profil pengirim di Gophish , agar email dapat dikirimkan.

B. Hasil Halaman Login Tiruan Instagram

Pada simulasi ini, hasil dari halaman login tiruan Instagram yang dibuat sangat mirip dengan aslinya, walaupun terbilang klasik, bukan model halaman login Instagram terbaru. Selain itu, halaman login ini berhasil diakses di semua jaringan, sehingga jika target tidak memakai jaringan yang sama, pengujian nantinya tetap bisa dilakukan tanpa harus menghidupkan komputer penguji, karena Gophish terinstal di *VPS* Biznet. Hasil dari *landing page* yaitu pada Gambar 4 berikut.



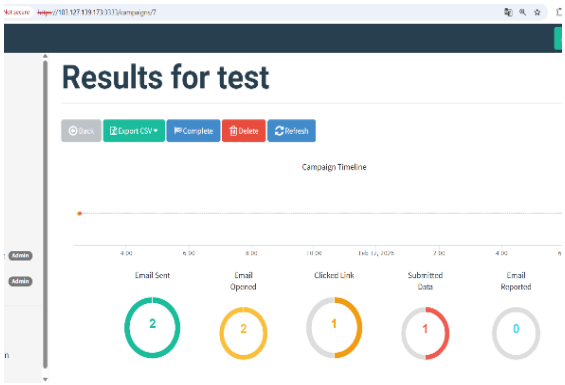
Gambar 4 Hasil Halaman Login Tiruan Instagram

Tetapi pada simulasi ini tidak

EPIC (Journal of Electrical Power, Instrumentation and Control)
Teknik Elektro – Universitas Pamulang
Vol. 8, No. 2, Bulan Desember, Tahun 2025, Hal 322 – 329
http://openjournal.unpam.ac.id/index.php/jit
DOI: 10.32493/epic.v8i2.58669
pISSN 2615-0646
eISSN 2614-8595

memakai domain *kustom* yang bersertifikat *SSL*, sehingga terdapat peringatan pada kolom *URL*-nya.

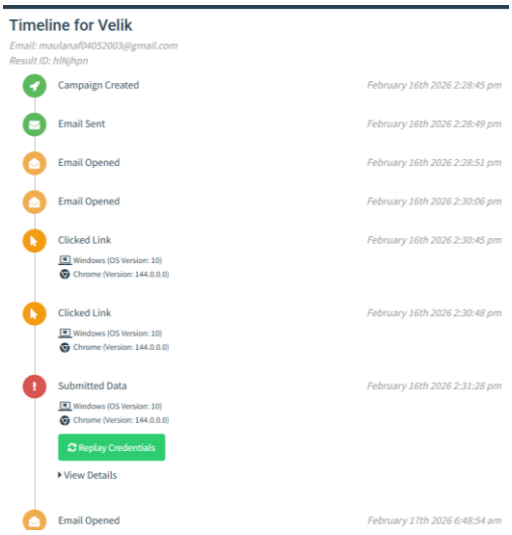
C. Hasil Kampanye *Phishing*



Gambar 5 Dashboard Gophish

Gambar 5 merupakan hasil kampanye yang dibuat. Simulasi berhasil dilakukan, di mana kredensial target dapat terkirim ke server Gophish. Penguji dapat melihat langsung timeline kampanye setiap target, dari kapan email terkirim hingga target mengirimkan kredensialnya ke server Gophish.

Timeline Gophish ini dapat dieksport dalam bentuk CSV, yang akan mempermudah analisis dalam pengujian penetrasi berbasis manusia dan dapat diolah lebih lanjut nantinya. Timeline dari kampanye *phishing* ini berada pada Gambar 6 berikut.



Gambar 6 Time Line Kampanye *Phishing*

Penelitian ini tidak dilakukan secara publik karena bertujuan untuk edukasi. Bagaimana simulasi pengujian penetrasi berbasis manusia dengan Gophish ini dilakukan secara efektif, dan jika dilakukan pengujian, nantinya data pengujian lebih akurat karena tidak terputusnya koneksi target ke server Gophish. Selain itu, simulasi ini dilakukan sesuai prinsip *Ethical Hacking* di lingkungan yang terkontrol.

KESIMPULAN

Dalam penelitian ini, simulasi kampanye *phishing* dengan framework Gophish yang diinstal di *VPS* berhasil dilakukan. *Link* yang dikirim melalui email tiruan Instagram dapat *dihosting* agar tidak terjadi terputusnya jaringan target ke server Gophish, dan kredensial pun dapat terkirim secara real time.

Tetapi pada penelitian ini tidak menggunakan domain yang memiliki sertifikat *SSL* agar tidak ada peringatan pada kolom *link*, dan tidak memakai email

EPIC (Journal of Electrical Power, Instrumentation and Control)
Teknik Elektro – Universitas Pamulang
Vol. 8, No. 2, Bulan Desember, Tahun 2025, Hal 322 – 329
http://openjournal.unpam.ac.id/index.php/jit
DOI: 10.32493/epic.v8i2.58669
pISSN 2615-0646
eISSN 2614-8595

relay agar email bisa dikustom dan meningkatkan tingkat keberhasilan simulasi.

Pada dasarnya, penelitian ini bertujuan untuk melakukan simulasi *phishing* dengan *VPS* agar jaringan target tidak terputus dari server Gophish dan meningkatkan efisiensi dalam pengujian. Maka dari itu, jika ke depannya akan dilakukan simulasi secara langsung untuk pengujian secara *real*, penguji dapat menggunakan server email lain selain Gmail dan menggunakan domain *kustom* yang bersertifikat *SSL,* agar hasilnya lebih baik lagi.

DAFTAR PUSTAKA

Ariyaningsih, S., Andrianto, A. A., Kusuma, A. S., & Prastyanti, R. A. (2023). Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia. *Justisia: Jurnal Ilmu Hukum*, *1*(1), 1–11. https://doi.org/10.56457/jjih.v1i1.38

Boy Setyawan Zalukhu, Fredin Samohouni Zai, Elena Dementieva Lase, Rosania Waruwu, Markus Prayoga Telaumbanua, & Ofel, O. L. (2025). Simulasi Teknik Phishing terhadap Situs Tiruan Facebook dan SIAKAD UNIRAYA Menggunakan Zphisher dan Ngrok. *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)*, *4*(1), 236–246. https://doi.org/10.62712/juktisi.v4i1.390

Eprianto, I., Khairana, K. N., Azhara, N., & Azalia, S. (n.d.). *Ancaman Social Engineering dalam Komunikasi Bisnis dan Efektivitas Kebijakan Keamanan Informasi di Organisasi Modern*.

Fikrah Kristo Fotriman Waruwu, Aperius Gea, Ester Ratna Cahyani Zega, Yustri Mei Mendrofa, Hendrik Trymedia Laoli, & Ofelius Laia. (2025). SIMULASI PHISING PADA WEBSITE ONESKY.COM MENGUNAKAN KALI LINUX DAN NGROK: STUDI KASUS KEAMANAN SIBER. *Jurnal Riset Sistem Informasi Dan Teknologi Informasi (JURSISTEKNI)*, *7*(3), 813–827. https://doi.org/10.52005/jursistekni.v7i3.481

Gea, C., Lase, K. J. D., & Syamsudin, M. (2023). Implementasi Virtual Private Server untuk Mini Hosting. *JURNAL SAINS DAN KOMPUTER*, *7*(01), 5–9. https://doi.org/10.61179/jurnalinfact.v7i01.402

Google. (2024). *Email sender guidelines*. https://support.google.com/a/answer/81126?hl=en#zippy=%2Crequirements-for-sending-or-more-messages-per-day%2Crequirements-for-all-senders

Putri, A., Sari, N., Fajrina, P., & Aisyah, S. (2024). Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering). *Jurnal Pengabdian Nasional (JPN) Indonesia*, *6*(1), 38–52. https://doi.org/10.35870/jpni.v6i1.1097

Sahay, R., Meng, W., & Li, W. (2025). A Comparative Analysis of Phishing Tools: Features and Countermeasures. In Z. Xia & J. Chen (Eds.), *Information Security Practice and Experience* (Vol. 15053, pp. 365–382). Springer Nature Singapore. https://doi.org/10.1007/978-981-97-9053-1_21

pISSN 2615-0646
eISSN 2614-8595

Uffi Novitasari. (2025). Phishing Berbasis AI sebagai Serangan Social Engineering: Ancaman Baru di Dunia Keamanan Siber. *Jurnal Ilmu Hukum*, *14*(2), 154–171. https://doi.org/10.30652/h9g1cd34

Wahyuningtias, N. A. (2025). *ANALIS NORMATIF PERLINDUNGAN HUKUM TERHADAP* KORBAN *KEJAHATAN SIBER DALAM MODUS PHISHING REKENING BANK DI INDONESIA*. https://doi.org/doi.org/10.54209/judge.v6i06.1564

Wibowo, B., & Hidayat, T. (2024). Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman Phishing di Lingkungan Perusahaan PT. XYZ. *Jurnal Pengabdian Masyarakat Sultan Indonesia*, *2*(1), 1–9. https://doi.org/10.58291/abdisultan.v2i1.294

Wibowo Noor Fikri, A., Fauzi, A., Alfathur Rachman, A., Khaerunisa, A., Puspita Sari, D., Vernanda, P., Hikmah, R., & Putri Fadyanti, T. (2023). Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phishing dalam Layanan Online Banking. *Jurnal Ilmu Multidisplin*, *2*(1), 84–91. https://doi.org/10.38035/jim.v2i1.228

Wijayanto, A. (2024). *MENGENAL CYBERSECURITY: PERLINDUNGAN DATA PRIBADI* DAN *PRIVASI DI SMA NEGERI 1 SAMBOJA*. *3*(2).