Jurnal Pengabdian Masyarakat Sultan Indonesia Vol. 2, No. 1 Maret 2025, Hal. 1-9
DOI: https://doi.org/10.58291/abdisultan.v2i1.294

Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman Phishing di Lingkungan Perusahaan PT. XYZ

Budi Wibowo[1], Taufik Hidayat[2]
[1]Program Studi Teknik Informatika, Institut Teknologi Budi Utomo, Jakarta
[2]Program Studi Teknik Komputer, Fakultas Teknik, Universitas Wiralodra, Indonesia

*Penulis Korespondensi: Budi Wibowo (E-mail: budiwibowo1993@gmail.com)

Abstrak

Penelitian ini bertujuan untuk mengevaluasi strategi efektif dalam meningkatkan kesadaran keamanan siber terhadap ancaman phishing di lingkungan organisasi. Menggunakan Gophish sebagai alat utama, kami melaksanakan simulasi phishing untuk menilai tingkat kesadaran dan respons karyawan terhadap serangan phishing. Kampanye ini melibatkan perancangan email phishing, pengiriman kepada target, dan pemantauan hasilnya. Dari total 75 karyawan yang menjadi peserta simulasi, 13,3% membuka email phishing, 13,3% mengklik tautan di dalam email, dan 8% memasukkan informasi pribadi ke dalam halaman phishing palsu. Hasil simulasi menunjukkan bahwa meskipun ada tingkat kesadaran yang cukup, masih terdapat celah signifikan dalam kemampuan karyawan untuk mendeteksi serangan phishing. Hanya 86,7% dari karyawan yang dapat mengidentifikasi dan melaporkan email phishing dengan benar. Gophish terbukti efektif dalam mengelola dan memantau kampanye phishing, dengan fitur-fitur seperti pelacakan klik dan laporan analitik yang memberikan wawasan mendalam tentang interaksi karyawan dengan email phishing. Temuan ini menekankan perlunya pendekatan proaktif dalam pelatihan dan kampanye kesadaran phishing. Organisasi disarankan untuk mengimplementasikan pelatihan yang lebih intensif dan berulang, serta menggunakan alat seperti Gophish untuk meningkatkan kesiapan karyawan dalam menghadapi ancaman phishing. Penelitian ini menggarisbawahi pentingnya strategi yang terencana untuk memperkuat keamanan siber secara keseluruhan di lingkungan organisasi.

***Kata kunci**: phishing, gophish, keamanan siber*

Abstract

This research aims to evaluate effective strategies for raising cybersecurity awareness of phishing threats in organizational environments. Using Gophish as the main tool, we carried out a phishing simulation to assess the level of employee awareness and response to phishing attacks. The campaign involved designing phishing emails, sending them to targets, and monitoring the results. Out of a total of 75 employees who participated in the simulation, 13.3% opened the phishing email, 13.3% clicked on the link in the email, and 8% entered personal information into the fake phishing page. The simulation results show that while there is a sufficient level of awareness, there are still significant gaps in employees' ability to detect phishing attacks. Only 86,7% of employees were able to correctly identify and report phishing emails. Gophish proved effective in managing and monitoring phishing campaigns, with features such as click tracking and analytics reports providing deep insights into employee interactions with phishing emails. These findings emphasize the need for a proactive approach in phishing training and awareness campaigns. Organizations are advised to implement more intensive and repetitive training and use tools such as Gophish to improve employee preparedness for phishing threats. This research underscores the importance of a well-planned strategy to strengthen overall cybersecurity in organizational environments.

***Keywords**:phishing, gophish, cyber security*

1. PENDAHULUAN

Dengan kemajuan teknologi informasi yang serba digital, dunia bisnis telah mengalami revolusi digital yang menawarkan kemudahan, biaya rendah, kepraktisan, dan dinamika dalam berkomunikasi serta mendapatkan informasi. Namun, di balik semua manfaat tersebut, terdapat beberapa pihak yang menyalahgunakan teknologi informasi dan komunikasi (TIK), khususnya internet. Mereka dengan sengaja menyusup ke situs web instansi atau lembaga tertentu untuk

DOI: https://doi.org/10.58291/abdisultan.v2i1.294

melakukan kejahatan, seperti pencurian atau pengacakan data, bahkan hingga mencuri uang melalui internet dengan cara membobol nomor PIN ATM [1]. Phishing adalah salah satu jenis serangan siber yang melibatkan upaya pemalsuan atau penipuan untuk mendapatkan informasi rahasia, seperti kata sandi, informasi kartu kredit, atau data pribadi dari korban yang tidak curiga [2]. Serangan phishing ini sering terjadi melalui email, pesan instan, atau situs web palsu yang terlihat sah. Beberapa contoh bahaya phishing meliputi: Email Phishing, Spear Phishing, dan Pharming, di mana penyerang mengarahkan lalu lintas internet korban ke server palsu untuk mencuri data seperti kata sandi [3]. Dampak dari serangan phishing terhadap organisasi dapat sangat merugikan, baik dari segi finansial maupun reputasi, yang pada akhirnya mengurangi tingkat kepercayaan pengguna. Oleh karena itu, penting bagi para pegawai PT. XYZ untuk dilindungi dan diberikan edukasi mengenai tindakan phishing yang berpotensi atau telah terjadi, terutama mengingat ekspektasi klien terhadap kredibilitas PT. XYZ dalam pencegahan, deteksi, dan investigasi terhadap ancaman yang berkaitan dengan sumber daya manusia [4].

Penelitian ini bertujuan untuk mengembangkan dan mengimplementasikan kampanye phishing terkontrol guna mengevaluasi dampaknya terhadap perusahaan dan karyawannya yang rentan terhadap ancaman siber ini [5]. Tujuan dari penelitian ini adalah untuk meningkatkan kesadaran keamanan siber dan melatih karyawan dalam mendeteksi email berbahaya, serta merancang protokol tanggap darurat yang efektif dalam menghadapi insiden phishing. Penelitian ini menggabungkan teknik rekayasa sosial dalam pembuatan email berbahaya dan memanfaatkan perangkat lunak sumber terbuka untuk pelaksanaan kampanye phishing [6][7].

Kami menganggap bahwa phishing adalah masalah nyata dalam dunia bisnis karena secara langsung menyerang bagian perusahaan yang dianggap paling rentan, yaitu karyawannya, dengan cara ini serangan ini mem-bypass semua tindakan anti-malware yang dapat diterapkan perusahaan untuk melawan serangan siber dan penjahat siber mendapatkan akses ke informasi rahasia atau menyuntikkan kode berbahaya ke perusahaan-perusahaan di seluruh dunia [8]. Menurut FBI, phishing adalah jenis kejahatan siber yang paling umum terjadi pada tahun 2020- dan insiden phishing hampir dua kali lipat frekuensinya, dari 114.702 insiden pada 19 tahun 2019, menjadi 241.324 insiden pada tahun 2020 [9][10].

Langkah awal dalam penelitian ini adalah mengidentifikasi urgensi dan pentingnya tindakan pencegahan guna menghindari risiko menjadi korban phishing. Selanjutnya, penelitian ini akan menguraikan prosedur pengembangan kampanye kesadaran keamanan siber, dimulai dari perencanaan hingga implementasi, dengan fokus pada pelatihan karyawan untuk mengenali potensi ancaman [11][12]. Penelitian ini juga mencakup seluruh tahapan penting dalam pelaksanaan kampanye phishing yang efektif, meliputi perancangan strategi rekayasa sosial untuk menguji kesiapsiagaan karyawan, pengembangan serta konfigurasi infrastruktur teknis seperti server email (SMTP), hingga penggunaan alat untuk otomatisasi dan pemantauan kampanye phishing, termasuk pembuatan email dan halaman web yang relevan [13] [14].

2. METODE PENELITIAN

Penelitian ini akan menggunakan metode campuran yang menggabungkan pendekatan kuantitatif dan kualitatif untuk mengevaluasi efektivitas kampanye kesadaran keamanan siber di kalangan karyawan. Kampanye ini akan terdiri dari tiga komponen utama: Sesi Pelatihan, Simulasi Email, dan Materi Edukasi.

1. Sesi Pelatihan

Sesi pelatihan akan dirancang untuk memberikan pemahaman mendalam tentang phishing, mencakup definisi, contoh-contoh umum, dan strategi untuk menghindari serangan phishing. Dalam Pelaksanaan ini akan dilakukan dalam format tatap muka dan virtual, dan akan diikuti oleh semua karyawan yang terlibat. Sesi akan berlangsung selama 1-2 jam dengan penyampaian materi interaktif dan studi kasus.Jumlah karyawan yang berpartisipasi dan durasi kehadiran mereka dalam sesi pelatihan akan dicatat dan dianalisis.

DOI: https://doi.org/10.58291/abdisultan.v2i1.294

2. Simulasi Email Phishing

Simulasi ini akan melibatkan pengiriman email phishing yang didesain secara khusus untuk tujuan pendidikan. Email ini akan diidentifikasi sebagai latihan untuk menghindari dampak negatif pada karyawan. Dalam Pelaksanaanya akan dilakukan secara acak dan berulang selama periode kampanye, dengan setiap karyawan menerima satu atau lebih email simulasi. Setelah menerima simulasi, karyawan akan diberikan umpan balik yang mencakup analisis terhadap respons mereka dan tips untuk menghindari serangan phishing di masa mendatang [15].

Pengukuran Keberhasilan Kampanye

1. Partisipasi Karyawan

Partisipasi karyawan dalam sesi pelatihan dan simulasi email akan diukur melalui jumlah kehadiran dan keterlibatan aktif mereka [3]. Data ini akan dianalisis untuk melihat tingkat partisipasi dan keterlibatan karyawan dalam kampanye.

2. Peningkatan Kesadaran

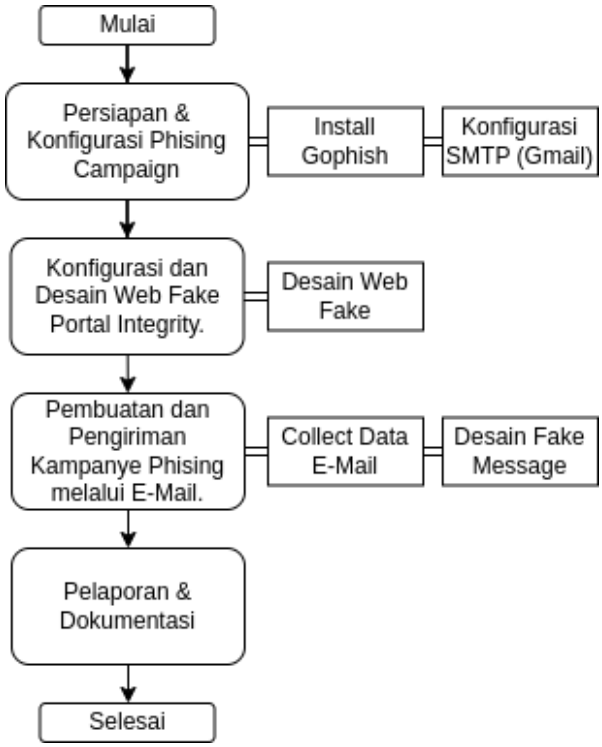
Sebelum kampanye dimulai, karyawan akan diminta untuk mengisi survei yang mengukur pengetahuan dan pemahaman mereka tentang phishing. Survei yang sama akan diberikan setelah kampanye selesai untuk menilai peningkatan kesadaran karyawan terhadap ancaman phishing. Data dari survei pre-test dan post-test akan dianalisis menggunakan metode statistik untuk mengukur peningkatan signifikan dalam kesadaran dan pemahaman karyawan [15].

Bagian ini akan menguraikan secara rinci prosedur yang dilakukan dalam melaksanakan Kampanye Phishing ini. Kami akan menjelaskan tahapan-tahapan dalam membangun kampanye phishing dari awal, termasuk semua elemen yang diperlukan, seperti pembuatan dan konfigurasi server SMTP, penggunaan perangkat lunak GoPhish untuk merancang kampanye, serta pembuatan email dan halaman web. Selain itu, bagian ini juga akan membahas langkah-langkah yang diambil untuk berurusan dengan sistem antispam perusahaan dan faktor-faktor kunci yang diperlukan untuk menghindari penolakan email. Langkah-langkah yang diuraikan meliputi:

1. Konfigurasi Email Phishing
   Penyiapan dan pengaturan server SMTP serta pembuatan email yang digunakan dalam kampanye [8].
2. Desain dan Konfigurasi Portal Web Palsu
   Pengembangan portal web yang dirancang untuk meniru situs web resmi sebagai bagian dari kampanye phishing [16].
3. Pembuatan dan Pengiriman Kampanye Phishing melalui Email
   Proses pengembangan kampanye phishing, termasuk pembuatan dan pengiriman email phishing kepada target[7].
4. Hasil dan Laporan
   Analisis hasil kampanye dan penyusunan laporan berdasarkan data yang diperoleh.
5. Pelatihan
   Program pelatihan yang dirancang untuk meningkatkan kesadaran karyawan terhadap ancaman phishing dan mengajarkan langkah-langkah mitigasi yang efektif [17].

DOI: https://doi.org/10.58291/abdisultan.v2i1.294

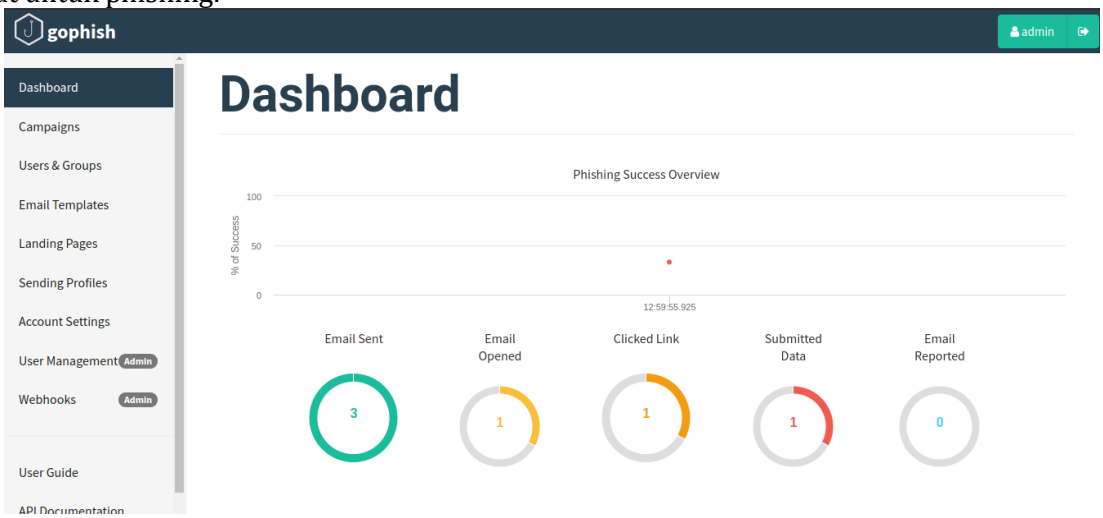
Diagram berikut ini menunjukkan alur proses percobaan Kampanye Phising dan semua komponen yang terlibat:



Gambar 1. Alur Proses Kampanye Phishing

3. HASIL DAN PEMBAHASAN

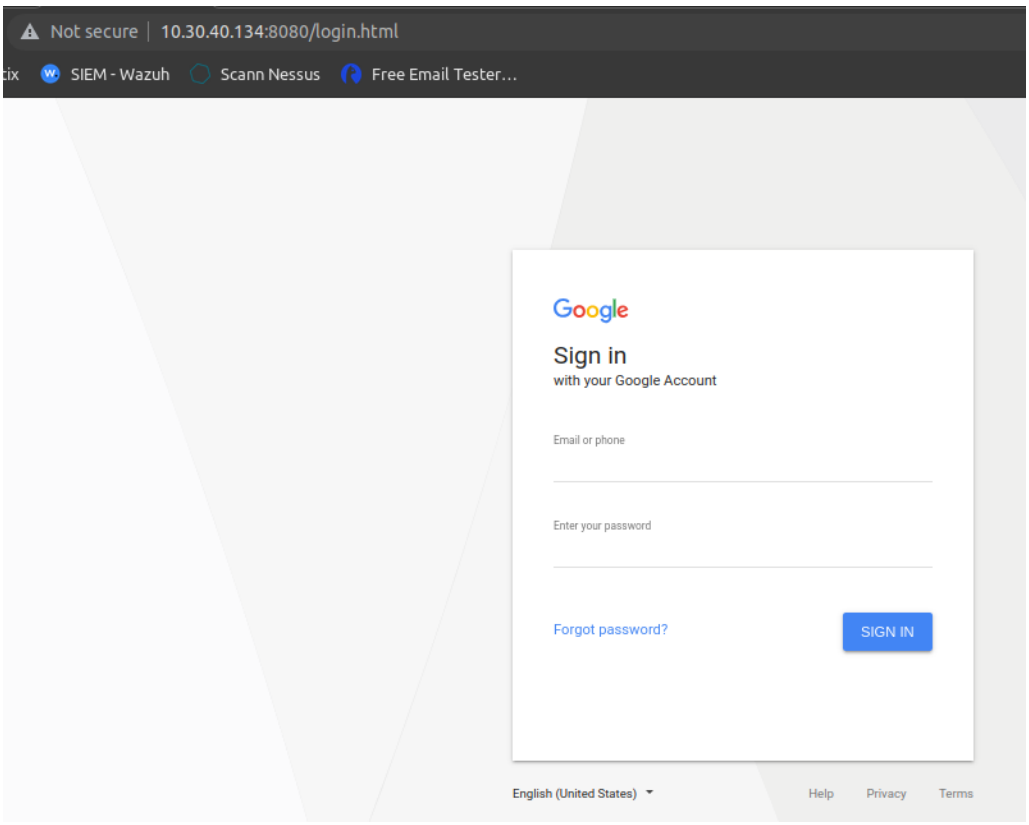
Dalam pembuatan dan pemantauan kampanye phishing, kami akan menggunakan layanan Gophish, sebuah perangkat lunak gratis dengan berbagai utilitas yang mendukung pelaksanaan kampanye secara menyeluruh. Aplikasi ini memiliki server administrasi yang dapat diakses secara lokal, serta memberikan opsi untuk meng-host halaman web yang khusus dibuat untuk phishing.



Gambar 2 .Tool Software Kampanye Phising

Konfigurasi dan Desain Web Fake Login Portal Organisasi yang terintegrasi dengan Akun Gmail Fake.

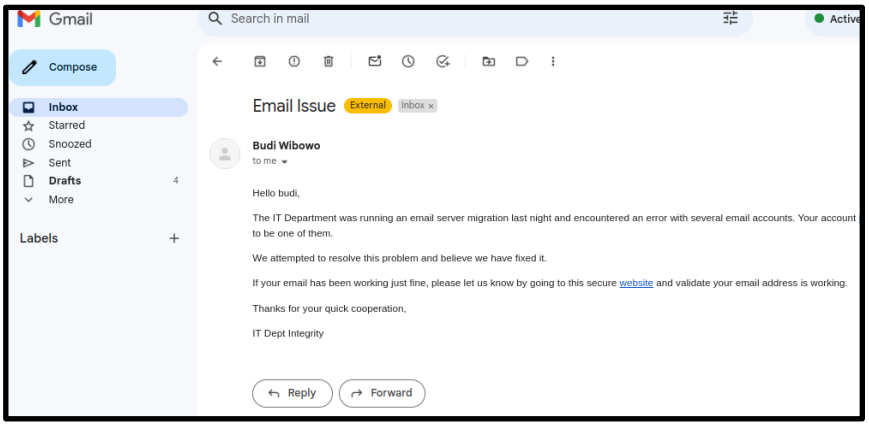
DOI: https://doi.org/10.58291/abdisultan.v2i1.294



Gambar 3 .Tampilan Akses Fake Gmail

Pembuatan dan Pengiriman Kampanye Phising melalui E-Mail.

Pada bagian template email, dapat menambahkan email yang akan digunakan untuk realisasi kampanye, disarankan untuk menggunakan email dalam format html, dapat menggunakan code editor GoPhish yang akan menampilkan preview kode html yang ditambahkan.

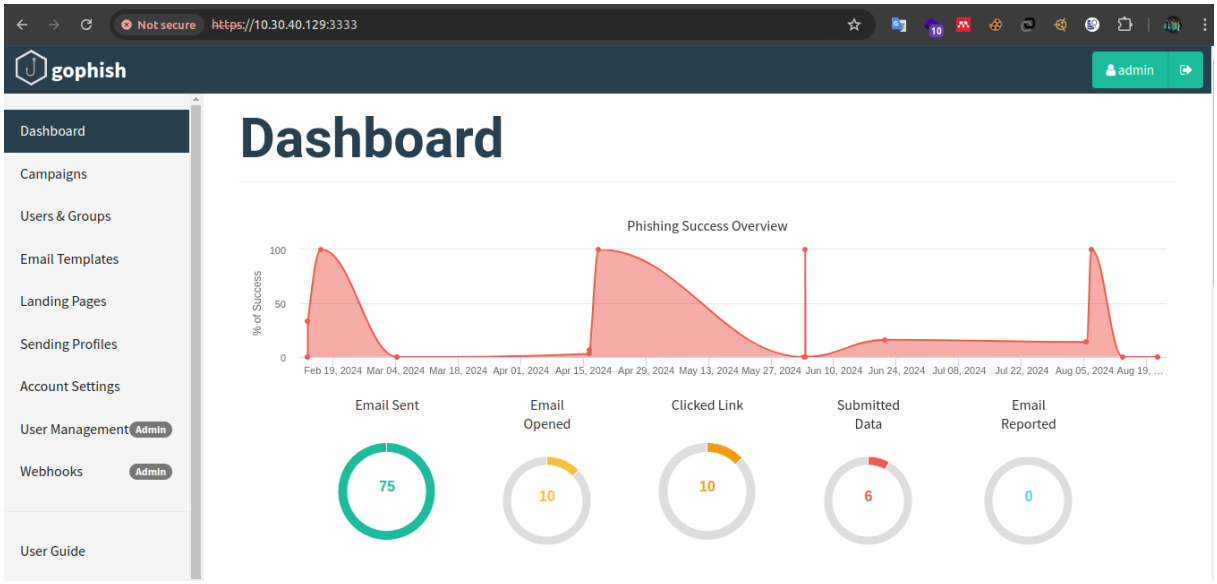


Gambar 4 .Tampilan Email Masuk

Dalam penelitian ini, simulasi phishing dilaksanakan dengan memanfaatkan Gophish sebagai platform utama. Tujuan dari kampanye ini adalah untuk mengevaluasi tingkat kesadaran dan respons karyawan terhadap ancaman phishing. Simulasi ini dilakukan pada bulan Februari 2024 s/d Agustus 2024 pengiriman dilakukan secara random di setiap departemen. Proses simulasi melibatkan beberapa langkah kritis, termasuk perancangan email phishing,

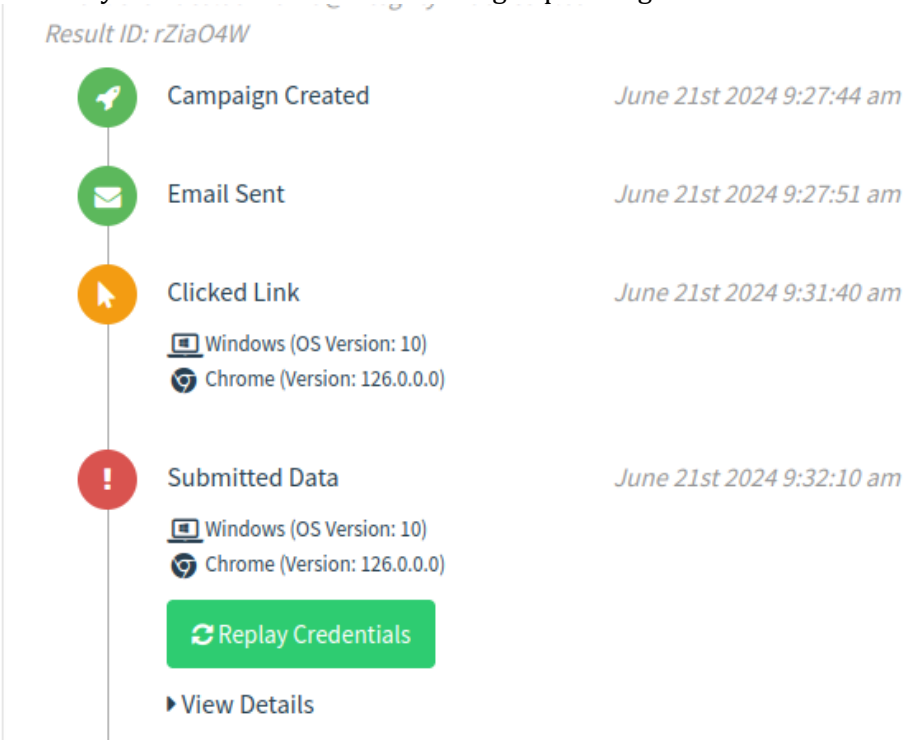
DOI: https://doi.org/10.58291/abdisultan.v2i1.294

pengiriman email kepada target, dan pemantauan hasil yang diperoleh. Dari sampel yang terdiri atas 75 karyawan sebagai target simulasi, ditemukan bahwa 13,3% di antaranya membuka email phishing yang dikirim. Dari kelompok ini, 13,3% mengklik tautan yang terdapat dalam email phishing tersebut, sedangkan 8% memasukkan informasi pribadi ke dalam halaman phishing palsu yang disajikan.



Gambar 5 .Tampilan Hasil Phising

86,7% karyawan yang berhasil mengidentifikasi email tersebut sebagai upaya phishing dan melaporkannya sesuai dengan prosedur yang telah ditetapkan. Hal ini mengindikasikan bahwa meskipun terdapat tingkat kesadaran, masih terdapat kerentanan yang signifikan dalam kemampuan karyawan untuk mendeteksi serangan phishing.



Gambar 6 .Tampilan informasi Karyawan yang berhasil terkena *phishing campaign*

DOI: https://doi.org/10.58291/abdisultan.v2i1.294

Setelah simulasi, umpan balik disampaikan kepada seluruh peserta, yang menekankan kesalahan yang terjadi dan memberikan panduan untuk meningkatkan kewaspadaan mereka. Karyawan yang tidak terjebak dalam serangan phishing menunjukkan pemahaman yang baik mengenai indikator phishing, seperti alamat email yang mencurigakan, tautan yang tidak relevan, dan urgensi yang tidak biasa dalam pesan.

Tabel 1. Hasil Perhitungan Karyawan terkena phishing setiap departemen di Organisasi PT.XYZ

NO	Departement	Email Opened	Clicked Link	Submitted Data
1	Business Expansion in Marketing	2	2	1
2	Quality Control	1	1	0
3	Finance & Accounting	0	0	0
4	Operation	5	5	3
5	Human & Resources	1	1	1
6	Design & Development	1	1	1
7	Sales	0	0	0
8	Application Development	0	0	0
		10	10	6

Hasil simulasi menunjukkan bahwa kampanye phishing yang dirancang menggunakan Gophish efektif dalam menilai tingkat kesadaran keamanan siber di kalangan karyawan. Tingginya jumlah karyawan yang membuka email dan mengklik tautan mencerminkan adanya celah signifikan dalam pemahaman mereka mengenai risiko phishing. Meskipun terdapat tingkat kesadaran yang cukup, persentase karyawan yang terjebak dalam serangan phishing mengindikasikan bahwa banyak di antara mereka yang belum dapat mendeteksi tanda-tanda phishing dengan akurat. Hal ini menyoroti kebutuhan untuk pelatihan tambahan yang lebih fokus pada identifikasi ciri-ciri phishing dan tanggapan yang tepat terhadap serangan tersebut.

Gophish terbukti sebagai alat yang sangat berguna dalam mengelola dan memantau kampanye phishing. Fitur-fitur seperti pelacakan klik, pembuatan halaman phishing, dan laporan analitik memberikan wawasan mendalam mengenai interaksi karyawan dengan email phishing. Kemampuan untuk menyesuaikan kampanye dan halaman web memungkinkan skenario phishing yang lebih realistis, yang mendukung penilaian yang lebih akurat terhadap reaksi karyawan.

Berdasarkan hasil simulasi ini, penting bagi organisasi untuk memperbaiki dan memperluas program pelatihan keamanan siber mereka. Pelatihan yang lebih intensif dengan simulasi realistis dan berulang dapat meningkatkan kemampuan karyawan dalam mengenali dan merespons serangan phishing. Secara keseluruhan, penelitian ini menegaskan perlunya pendekatan proaktif dalam pelatihan dan kampanye kesadaran phishing. Dengan menggunakan alat seperti Gophish, organisasi dapat secara efektif mengukur dan meningkatkan kesiapan karyawan dalam menghadapi ancaman phishing, yang pada akhirnya akan memperkuat keamanan siber mereka secara keseluruhan.

DOI: https://doi.org/10.58291/abdisultan.v2i1.294

4. KESIMPULAN

Penelitian ini menegaskan pentingnya strategi yang efektif dalam meningkatkan kesadaran keamanan siber terhadap ancaman phishing di lingkungan organisasi. Melalui simulasi phishing yang dilaksanakan dengan Gophish, ditemukan bahwa meskipun sebagian besar karyawan menunjukkan tingkat kesadaran yang cukup, masih terdapat celah signifikan dalam kemampuan mereka untuk mendeteksi dan merespons serangan phishing dengan tepat.

Hasil simulasi menunjukkan bahwa 13,3% dari karyawan membuka email phishing, 13,3% mengklik tautan di dalamnya, dan 8% memasukkan informasi pribadi ke dalam halaman phishing palsu. Selain itu, 86.7% karyawan yang dapat mengidentifikasi dan melaporkan email phishing secara benar. Ini menunjukkan bahwa ada kebutuhan mendesak untuk pelatihan keamanan siber yang lebih efektif dan berkelanjutan. Gophish terbukti sebagai alat yang sangat berguna untuk merancang, melaksanakan, dan memantau kampanye phishing. Fitur-fitur canggih dari Gophish, seperti pelacakan klik dan pembuatan halaman phishing, memberikan wawasan berharga tentang interaksi karyawan dengan serangan phishing.

Berdasarkan temuan ini, organisasi perlu memperkuat program pelatihan keamanan siber mereka dengan pendekatan yang lebih proaktif. Pelatihan yang melibatkan simulasi realistis dan berulang, serta penggunaan alat seperti Gophish, dapat membantu meningkatkan kemampuan karyawan dalam mendeteksi dan menangani ancaman phishing. Dengan langkah-langkah ini, organisasi dapat memperkuat keamanan siber mereka secara keseluruhan dan mengurangi risiko yang terkait dengan serangan phishing.

DAFTAR PUSTAKA

[1] R. J. van Geest, G. Cascavilla, J. Hulstijn, and N. Zannone, “The applicability of a hybrid framework for automated phishing detection,” *Comput. Secur.*, vol. 139, no. February 2023, p. 103736, 2024, doi: 10.1016/j.cose.2024.103736.

[2] B. M. Berens, M. Mossano, and M. Volkamer, “Taking 5 minutes protects you for 5 months: Evaluating an anti-phishing awareness video,” *Comput. Secur.*, vol. 137, no. November 2023, p. 103620, 2024, doi: 10.1016/j.cose.2023.103620.

[3] H. Nugroho, M. N. Ihsan, A. Haryoko, F. Màarif, and F. Alifah, “Edukasi Keamanan Digital Untuk Meningkatkan Kewaspadaan Masyarakat Terhadap Link Phising,” *J. Pengabdi. Masy. Multidisiplin*, vol. 1, no. 2, pp. 28–40, 2023.

[4] N. Beu *et al.*, “Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation,” *Comput. Secur.*, vol. 131, p. 103313, 2023, doi: 10.1016/j.cose.2023.103313.

[5] R. Hoheisel, G. van Capelleveen, D. K. Sarmah, and M. Junger, “The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains,” *Comput. Secur.*, vol. 128, 2023, doi: 10.1016/j.cose.2023.103158.

[6] G. Wibisono, R. A. G. Gultom, and T. Mantoro, “Strategi Peningkatan Kapabilitas Satuan Siber Dispamsanau Melalui Pemanfaatan Artificial Intelligence Pada Keamanan Siber Berdasarkan National Institute of Standards and Technology Cybersecurity Framework Version 1.1,” *J. Rev. Pendidik. dan Pengajaran*, vol. 7, no. 1, pp. 968–975, 2024.

[7] D. J. Liu, G. G. Geng, X. B. Jin, and W. Wang, “An efficient multistage phishing website detection model based on the CASE feature framework: Aiming at the real web environment,” *Comput. Secur.*, vol. 110, p. 102421, 2021, doi: 10.1016/j.cose.2021.102421.

[8] L. Ribeiro, I. S. Guedes, and C. S. Cardoso, “Which factors predict susceptibility to phishing? An empirical study,” *Comput. Secur.*, vol. 136, no. March 2023, 2024, doi: 10.1016/j.cose.2023.103558.

[9] B. Wibowo, “Smart Home Security Analysis Using Arduino Based Virtual Private Network”.

[10] A. Yuswanto and B. Wibowo, “Pembangunan Pusat Pengendalian Operasional Keamanan

Informasi (Pusdalops Kami) guna Meningkatkan Pelayanan E-Gov dari Ancaman Kejahatan Siber," *Format J. Ilm. Tek. Inform.*, vol. 9, no. 2, p. 118, 2021, doi: 10.22441/format.2020.v9.i2.003.

[11] U. Ladayya, D. Prayitno, M. Syani, R. Hikmawan, and N. W. Abdulmajid, "Kesadaran Keamanan Informasi atas Phising , Smishing , dan Vishing pada Warga Kota Cimahi," vol. 18, pp. 109–119, 2024.

[12] A. Yuswanto, B. Wibowo, and L. Hafiz, "A Review Method for Analysis of the Causes of Data Breach in the Pasca Pandemic," *J. Komput. dan Elektro Sains*, vol. 3, no. 1, pp. 1–5, 2024, doi: 10.58291/komets.v3i1.205.

[13] S. R. Cahyani and L. A. Fauzan, "Jurnal Kreativitas Teknologi dan Komputer," vol. 15, no. 6, pp. 43–49, 2024.

[14] N. Thompson, T. McGill, and N. Narula, "'No point worrying' – The role of threat devaluation in information security behavior," *Comput. Secur.*, vol. 143, no. May, p. 103897, 2024, doi: 10.1016/j.cose.2024.103897.

[15] D. Baltuttis and T. Teubner, "Effects of visual risk indicators on phishing detection behavior: An eye-tracking experiment," *Comput. Secur.*, vol. 144, no. June, p. 103940, 2024, doi: 10.1016/j.cose.2024.103940.

[16] A. Chrysanthou, Y. Pantis, and C. Patsakis, "The anatomy of deception: Measuring technical and human factors of a large-scale phishing campaign," *Comput. Secur.*, vol. 140, no. February, p. 103780, 2024, doi: 10.1016/j.cose.2024.103780.

[17] A. Ramadhan, M. Alwi Alhafidh, and M. Diki Firmansyah, "Penyebaran Link Phising Kuota Kemendikbud Terhadap Kesadaran," *KAMPRET J.*, vol. 1, no. 2, pp. 11–16, 2022, [Online]. Available: https://plus62.isha.or.id/index.php/kampret/article/view/9