



**ANALISIS KESADARAN KARYAWAN TERHADAP SERANGAN
PHISHING EMAIL DI PERUSAHAAN BERSERTIFIKASI ISO 27001 DAN
PCI DSS : STUDI KASUS PERUSAHAAN XYZ**

SKRIPSI

Disusun Oleh:

RIFKY HALSANDRIAN

NIM. 2110511094

PROGRAM STUDI S1 INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA

2025



**ANALISIS KESADARAN KARYAWAN TERHADAP SERANGAN
PHISHING EMAIL DI PERUSAHAAN BERSERTIFIKASI ISO 27001 DAN
PCI DSS : STUDI KASUS PERUSAHAAN XYZ**

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana
Komputer**

Disusun Oleh:

RIFKY HALSANDRIAN

NIM. 2110511094

PROGRAM STUDI S1 INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA

2025

PERNYATAAN ORISINALITAS

Tugas akhir ini adalah hasil karya sendiri dan semua sumber baik yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Rifky Halsandrian

NIM : 2110511094

Tanggal : 16 Juni 2025

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku

Jakarta, 16 Juni 2025

Yang Menyatakan



Rifky Halsandrian

**PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK
KEPENTINGAN AKADEMIS**

Sebagai civitas akademika Universitas Pembangunan Nasional Veteran Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Rifky Halsandrian
NIM : 2110511094
Fakultas : Ilmu Komputer
Program Studi : S-1 Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (Non - exclusive Royalty Free Right) atas skripsi saya yang berjudul:

Analisis Kesadaran Karyawan Terhadap Serangan Phishing Email di Perusahaan Bersertifikat ISO 27001 dan PCI DSS : Studi Kasus Perusahaan XYZ

Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/memformatkan, mengelola dalam bentuk pangkalan data (basis data), merawat dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya

Dibuat di: Jakarta

Pada tanggal: 16 Juni 2025

Yang Menyatakan



Rifky Halsandrian

LEMBAR PENGESAHAN

Judul : Analisis Kesadaran Karyawan Terhadap Serangan Phishing Email di
Perusahaan Bersertifikasi ISO 27001 dan PCI DSS : Studi Kasus
Perusahaan XYZ
Nama : Rifky Halsandrian
NIM : 2110511094

Disetujui oleh:

Penguji 1:
Indra Permata Solihin S.Kom., M.Kom.

Penguji 2:
Hamonangan Kinantan P., S.T, MT

Pembimbing 1:
Henki Bayu Seta, S.Kom, MTI.

Pembimbing 2:
Nurhuda Maulana, S.T., M.T.

Diketahui oleh:

Koordinator Program Studi:
Dr. Widya Cholil, M.I.T.
NIP. 2211122080

Dekan Fakultas Ilmu Komputer:
Prof. Dr. Ir. Supriyanto, S.T., M.Sc., IPM
NIP. 197605082003121002

Tanggal Ujian Tugas Akhir:
02 Juni 2025



**ANALISIS KESADARAN KARYAWAN TERHADAP SERANGAN
PHISHING EMAIL DI PERUSAHAAN BERSERTIFIKASI ISO 27001 DAN
PCI DSS : STUDI KASUS PERUSAHAAN XYZ**

RIFKY HALSANDRIAN

ABSTRAK

Serangan phishing melalui email masih menjadi salah satu ancaman utama dalam keamanan informasi perusahaan, meskipun telah menerapkan sertifikasi ISO 27001 dan PCI DSS. Penelitian ini bertujuan untuk mengukur tingkat kesadaran karyawan terhadap ancaman phishing serta mengidentifikasi faktor-faktor yang memengaruhinya. Metode penelitian yang digunakan adalah simulasi email phishing kepada karyawan dari berbagai divisi menggunakan tools Gophish dan wawancara mendalam. Hasil penelitian menunjukkan bahwa sebanyak 43% karyawan membuka email phishing, 29% mengklik tautan berbahaya, dan hanya 6% yang melaporkan adanya percobaan serangan. Temuan ini mengindikasikan perlunya peningkatan edukasi dan program pelatihan keamanan informasi secara berkelanjutan untuk meminimalisir risiko serangan siber pada organisasi.

Kata Kunci: Phishing, Kesadaran Karyawan, Keamanan Informasi, ISO 27001, PCI DSS

ANALYSIS OF EMPLOYEE AWARENESS TOWARDS EMAIL PHISHING ATTACKS IN ISO 27001 AND PCI DSS CERTIFIED COMPANIES: CASE STUDY OF XYZ COMPANY

RIFKY HALSANDRIAN

ABSTRACT

Email phishing attacks are still one of the main threats to information security in organisations, despite the implementation of ISO 27001 and PCI DSS certifications. This research aims to measure the level of employee awareness of phishing threats and identify the factors that influence it. The research method used is a phishing email simulation for employees from different departments using the Gophish tool and in-depth interviews. The results showed that 43% of employees opened phishing emails, 29% clicked on malicious links and only 6% reported attempted attacks. These findings highlight the need for ongoing education and information security training programmes to minimise the risk of cyber-attacks on organisations.

Keywords: Phishing, employee awareness, information security, ISO 27001, PCI DSS

KATA PENGANTAR

Puji dan Syukur penulis panjatkan kepada Tuhan Yang Maha Esa, berkat rahmat dan karunianya penulis dapat melaksanakan dan menyelesaikan tugas akhir yang berjudul “Analisis Kesadaran Karyawan Terhadap Serangan Phishing Email Di Perusahaan Bersertifikasi ISO 27001 Dan PCI DSS : Studi Kasus Perusahaan XYZ”. Selama pelaksanaan perkuliahan dan penyelesaian tugas akhir ini, tentu tak lepas dari pengarahan dan bimbingan berbagai pihak, sehingga penulis mengucapkan terimakasih kepada :

1. Kedua orang tua dan seluruh keluarga besar. Terima kasih atas support dan bimbingannya selama ini.
2. Bapak Henki Bayu Seta, S.Kom., MTI. selaku dosen pembimbing 1 dan Bapak Nurhuda Maulana, S.T., M.T. selaku dosen pembimbing 2 yang telah memberikan masukan, saran, dan motivasi dalam penyusunan penelitian ini.
3. Ibu Widya selaku Kepala Program Studi S1 Informatika di Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta.
4. Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta yang selama ini memberikan kesempatan kepada penulis untuk mengikuti perkuliahan.
5. Sahabat penulis yang selalu kebersamai di segala situasi, kondisi, dan selama perkuliahan. Terima kasih atas segala waktu dan support yang diluangkan untuk penulis.
6. Teman-teman seperjuangan di Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta yang selalu kebersamai selama ini.

Akhir kata penulis mengucapkan terimakasih kepada seluruh pihak yang terlibat dan berharap semoga Tuhan Yang Maha Esa membalas semua bimbingan yang bantuan yang telah diberikan.

Jakarta, September 2024

Rifky Halsandrian

NIM. 2110511094

DAFTAR ISI

PERNYATAAN ORISINALITAS.....	i
PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS.....	ii
LEMBAR PENGESAHAN	iii
ABSTRAK.....	iv
<i>ABSTRACT</i>	v
KATA PENGANTAR.....	vi
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xii
DAFTAR LAMPIRAN	xiii
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	3
1.3. Batasan Masalah.....	3
1.4. Tujuan dan Manfaat Penelitian.....	4
1.5. Sistematika penulisan	5
BAB II TINJAUAN PUSTAKA.....	6
2.1. Penelitian Terdahulu.....	6
2.2. Teori	10
2.2.1. Kesadaran Karyawan	10
2.2.2. Google Workspace	11
2.2.3. Standar Keamanan ISO/IEC 27001 dan PCI DSS	11
2.2.3.1. ISO/IEC 27001.....	11
2.2.3.2. PCI DSS	13
2.2.4. <i>Cyber Security Awareness</i>	14
2.2.5. Gophish	15
2.2.6. <i>Port Forwarding</i>	16
2.2.6.1. Serveo.net.....	17
2.2.7. <i>Phishing Attack</i> Email.....	19
2.2.7.1. Karakteristik <i>Phishing</i> Email	19

2.2.7.2.	Jenis-jenis <i>Phishing</i> Email	19
2.2.7.3.	Metode Penyebaran <i>Phishing</i> Email	20
2.2.7.4.	Dampak <i>Phishing</i> Email	21
2.2.7.5.	Alur dan Fase Proses <i>Phishing</i>	21
2.3.	Model Konseptual	22
BAB III METODE PENELITIAN.....		28
3.1.	Metode Penelitian.....	28
3.2.	Rancangan Solusi/Metode yang Diusulkan.....	31
3.3.	Teknik Pengumpulan Data (Eksperimen Desain)	32
3.4.	Metode Analisis.....	33
3.5.	Jadwal Penelitian	33
BAB IV HASIL DAN PEMBAHASAN.....		34
4.1.	Profil Perusahaan.....	34
4.1.1.	Analisis Kondisi Perusahaan.....	34
4.1.1.1.	Gambaran Umum Perusahaan.....	34
4.1.1.2.	Struktur Organisasi dan Keamanan.....	35
4.1.1.3.	Implementasi Standar Keamanan.....	36
4.1.2.	Analisis Karyawan & <i>Awareness</i>	37
4.1.2.1.	Proses Penerimaan Karyawan	37
4.1.2.2.	Program <i>Awareness</i>	39
4.2.	Deskripsi Objek Penelitian	43
4.3.	Analisis Deskripsi.....	43
4.3.1.	Perancangan Serangan <i>Phishing</i>	43
4.3.1.1.	<i>Users & Groups</i>	44
4.3.1.2.	<i>Email Templates</i>	45
4.3.1.3.	<i>Landing Pages</i>	48
4.3.1.4.	<i>Sending Profiles</i>	49
4.3.2.	Peluncuran <i>Campaign</i> Serangan <i>Phishing</i>	51
4.3.2.1.	Pengaturan Google Admin	51
4.3.2.2.	Peluncuran <i>Campaign</i>	52
4.4.	Analisis Penelitian	54
4.4.1.	Pengujian.....	54
4.4.2.	Evaluasi Serangan	55

4.4.3. Tindakan Perbaikan.....	55
4.5. Hasil dan Rekomendasi	62
4.5.1. Hasil penelitian.....	62
4.5.2. Rekomendasi	63
BAB V PENUTUP.....	55
5.1. Kesimpulan.....	55
5.2. Saran	56
DAFTAR PUSTAKA.....	57
RIWAYAT HIDUP	59
LAMPIRAN.....	60

DAFTAR GAMBAR

Gambar 2.1. Dashboard Gophish	16
Gambar 2.2. Diagram Port Forwarding Serveo.net pada Gophish	18
Gambar 2.3. Contoh penggunaan Serveo pada localhost.....	18
Gambar 2.4. Contoh Alur dan Fase Proses Phishing	22
Gambar 2.5. Model Konseptual	23
Gambar 3.1. Tahapan Penelitian	28
Gambar 3.2. Arsitektur Pengujian Phishing Email	30
Gambar 4.1. Struktur Organisasi PT XYZ.....	35
Gambar 4.2. Proses Upload SKCK.....	38
Gambar 4.3. Perjanjian Kerahasiaan (NDA).....	39
Gambar 4.4. Acknowledgement Form	39
Gambar 4.5. Monthly Information Security Awareness Poster.....	41
Gambar 4.6. Annually Information Security Awareness Training Material.....	41
Gambar 4.7. Annually Secure Coding Workshop for Developers	42
Gambar 4.8. Incident Response Training Material	42
Gambar 4.9. Dashboard Phishing Email Attack Simulation	43
Gambar 4.10. CSV Templates.....	44
Gambar 4.11. Import List of Users	45
Gambar 4.12. Section Email Templates	46
Gambar 4.13. Pengaturan Email Templates	46
Gambar 4.14. Source Code Email Templates	47
Gambar 4.15. Preview Email Templates.....	47
Gambar 4.16. Source Code Landing Pages.....	48
Gambar 4.17. Pengaturan Landing Pages pada Tools Gophish	49
Gambar 4.18. Preview Landing Pages	49
Gambar 4.19. Konfigurasi Sending Profile.....	50
Gambar 4.20. Test Email.....	50
Gambar 4.21. Pengaturan Bypass Google Admin.....	52
Gambar 4.22. Pengaturan Campaign Phishing	52
Gambar 4. 23. Serveo Forwarding HTTP IP Internal.....	53
Gambar 4.24. Phishing Attack Simulation Result.....	54

Gambar 4.25. Dashboard Visual Phishing Attack.....	62
--	----

DAFTAR TABEL

Tabel 2.1. Literature Review	6
Tabel 2.2. Information Security Control 6.3 (Badan Standardisasi Nasional dan Komite Teknis 35-04 Keamanan Informasi, 2023)	12
Tabel 2.3. Account Data	14
Tabel 3.1. Jadwal Penelitian	33

DAFTAR LAMPIRAN

Lampiran 1. Surat Permohonan Riset	60
Lampiran 2. Surat Pernyataan PT XYZ	61
Lampiran 3. Surat Permohonan Ketersediaan Dalam Wawancara.....	62
Lampiran 4. Surat Persetujuan Ketersediaan Sebagai Narasumber	63
Lampiran 5. Source Code Email Templates dan Landing Page	64
Lampiran 6. Information Security Awareness Training Material.....	70
Lampiran 7. Information Security Poster Phishing Email Attack.....	73
Lampiran 8. Laporan Phishing dan Rekomendasi Enkripsi AES	75
Lampiran 9. Hasil Cek Plagiarisme	76