

**ANALISIS TINGKAT KESADARAN KEAMANAN SIBER KARYAWAN
TERHADAP SERANGAN *PHISHING* MENGGUNAKAN GOPHISH DAN
*TECHNIQUE FOR ORDER PREFERENCE BY SIMILARITY TO IDEAL
SOLUTION* (TOPSIS)**

TUGAS AKHIR

Diajukan sebagai salah satu syarat memperoleh gelar Sarjana
Program Studi S-1 Teknologi Informasi



Disusun oleh:

YONGKI DANIL SAPUTRA

212104013

**PROGRAM STUDI S-1 TEKNOLOGI INFORMASI
FAKULTAS TEKNIK & TEKNOLOGI INFORMASI
UNIVERSITAS JENDERAL ACHMAD YANI YOGYAKARTA**

2025

HALAMAN PENGESAHAN

TUGAS AKHIR

ANALISIS TINGKAT KESADARAN KEAMANAN SIBER KARYAWAN TERHADAP SERANGAN *PHISHING* MENGGUNAKAN GOPHISH DAN *TECHNIQUE FOR ORDER PREFERENCE BY SIMILARITY TO IDEAL SOLUTION (TOPSIS)*

Diajukan oleh:

YONGKI DANIL SAPUTRA

212104013

Telah dipertahankan di depan dewan penguji dan dinyatakan sah
sebagai salah satu syarat untuk memperoleh gelar Sarjana
di Fakultas Teknik & Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta

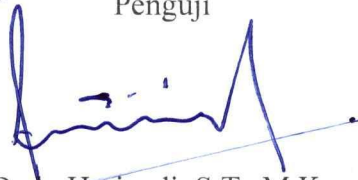
Tanggal: 18 Juni 2025

Mengesahkan:

Pembimbing

Penguji


Chanief Budi Setiawan, S.T., M.Eng.
NIDN: 0514068101


Ir. Dedy Hariyadi, S.T., M.Kom.
NIDN: 0518108001

Mengetahui

Ketua Program Studi S-1 Teknologi Informasi
Fakultas Teknik & Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta




Rama Sahtyawan, S.T., M.Cs.
NPP: 2019.13.00150

HALAMAN PERNYATAAN

Saya yang bertanda tangan di bawah ini, adalah mahasiswa Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta,

Nama : Yongki Danil Saputra
NPM : 212104013
Program Studi : S-1 Teknologi Informasi
Judul Tugas Akhir : Analisis Tingkat Kesadaran Keamanan Siber Karyawan Terhadap Serangan *Phishing* Menggunakan Gophish dan *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS)

Menyatakan bahwa hasil penelitian dengan judul tersebut di atas adalah asli karya saya sendiri dan bukan hasil plagiarisme. Semua referensi dan sumber terkait yang dikutip dalam karya ilmiah ini telah ditulis sesuai dengan kaidah penulisan ilmiah yang berlaku. Dengan ini, saya menyatakan untuk menyerahkan hak cipta penelitian kepada Universitas Jenderal Achmad Yani Yogyakarta guna kepentingan ilmiah.

Demikian surat pernyataan ini dibuat dengan sebenar-benarnya tanpa ada paksaan dari pihak mana pun. Apabila terdapat kekeliruan atau ditemukan adanya pelanggaran akademik di kemudian hari, maka saya bersedia menerima konsekuensi yang berlaku sesuai ketentuan akademik.

Yogyakarta, 18 Juni 2023



Yongki Danil Saputra

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul: “Analisis Tingkat Kesadaran Keamanan Siber Karyawan Terhadap Serangan *Phishing* Menggunakan Gophish dan *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS)”. Penyusunan laporan ini merupakan salah satu persyaratan untuk menyelesaikan studi di Program Studi S-1 Teknologi Informasi Fakultas Teknik & Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta. Laporan ini dapat diselesaikan atas bimbingan, arahan, dan bantuan dari berbagai pihak. Pada kesempatan ini penulis dengan rendah hati mengucapkan terima kasih dengan setulus-tulusnya kepada:

1. Ibunda dan nenek tercinta, perempuan hebat yang pernah penulis temui di dunia ini. Kedua perempuan hebat yang dengan tulus senantiasa memberikan kasih sayang dan kehangatan dalam kehidupan ini. Terima kasih atas segala dedikasi, doa, dan sejuta pengorbanannya yang ditujukan untuk kehidupan penulis selama ini. Terima kasih atas segala hal-hal baik yang selama ini telah diberikan. Berpijak diatas pengorbanan kalian, penulis harap sehatlah selalu agar bisa hidup lebih lama dan selalu ada di setiap pencapaian penulis;
2. Bapak Rama Sahtyawan, S.T., M.Cs. selaku Ketua Program Studi S-1 Teknologi Informasi Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
3. Bapak Chanief Budi Setiawan, S.T., M.Eng. selaku Dosen Pembimbing Tugas Akhir;
4. Bapak Ir. Dedy Hariyadi, S.T., M.Kom., selaku Dosen Pembimbing Akademik selama perkuliahan berlangsung;

5. Para dosen yang telah memberikan banyak bekal ilmu pengetahuan kepada penulis selama menjadi mahasiswa di Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
6. Bapak Ida Casninda, S.Pd. Pembina OSIS SMA Negeri 1 Beber pada masanya, yang telah memberikan banyak nasehat, motivasi serta pandangan masa depan yang cerah kepada penulis. Berkatnya, penulis bisa merasakan betapa indahnya perjuangan dalam pendidikan di bangku perkuliahan;
7. Keluarga dan sahabat-sahabat penulis yang senantiasa memberikan doa dan semangat di setiap perjuangan sehingga dapat menyelesaikan Tugas Akhir ini dengan tepat waktu;
8. Teman-teman seperjuangan, mahasiswa Teknologi Informasi 2021 yang selalu berjuang bersama dalam menempuh pendidikan di Universitas Jenderal Achmad Yani Yogyakarta;
9. Semua pihak yang tidak dapat penulis cantumkan satu persatu yang selalu memberikan dukungan positif selama ini;
10. Serta kepada sosok terhebat yang selama ini mampu tetap berdiri tegap di segala rintangan perjuangannya – Yongki Danil Saputra, dan ya! diri saya sendiri. Apresiasi setinggi-tingginya karena telah bertanggung jawab atas segala kewajibannya dalam menuntaskan pendidikan Sarjana di Universitas Jenderal Achmad Yani Yogyakarta dengan sangat baik.

Penulis menyadari bahwa laporan tugas akhir ini masih jauh dari kata sempurna. Maka dari itu dengan segala kerendahan hati penulis sangat menghargai adanya kritik dan saran yang membangun dari semua pihak yang bersedia meluangkan waktu untuk membaca laporan tugas akhir ini.

Yogyakarta, 18 Juni 2025



Yongki Danil Saputra

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PENGESAHAN.....	ii
HALAMAN PERNYATAAN.....	iii
KATA PENGANTAR.....	iv
DAFTAR ISI.....	vi
DAFTAR TABEL.....	viii
DAFTAR GAMBAR.....	ix
DAFTAR LAMPIRAN.....	x
DAFTAR SINGKATAN.....	xi
INTISARI.....	xii
ABSTRACT.....	xiii
BAB 1 PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	4
1.3 Batasan Penelitian.....	4
1.4 Pertanyaan Penelitian.....	5
1.5 Tujuan Penelitian.....	5
1.6 Manfaat Hasil Penelitian.....	5
BAB 2 TINJAUAN PUSTAKA & LANDASAN TEORI.....	6
2.1 Tinjauan Pustaka.....	6
2.2 Landasan Teori.....	11
2.2.1 Kesadaran Keamanan Siber.....	11
2.2.2 <i>Phishing</i>	12
2.2.3 Gophish.....	13
2.2.4 <i>Technique for Order Preference by Similarity to Ideal Solution</i> (TOPSIS).....	14
2.2.5 <i>Equal Interval Methode</i>	17

BAB 3 METODE PENELITIAN.....	18
3.1 Bahan Penelitian.....	19
3.2 Alat Penelitian.....	20
3.3 Jalan Penelitian.....	20
BAB 4 HASIL PENELITIAN.....	25
4.1 Ringkasan Hasil Penelitian.....	25
4.2 Pembahasan.....	26
4.2.1 Konfigurasi dan Perancangan Pola Simulasi Serangan <i>Phishing</i>	26
4.2.2 Pelaksanaan Simulasi Serangan <i>Phishing</i>	34
4.2.3 Klasifikasi Data Hasil Simulasi.....	43
4.2.4 Analisis dan Perhitungan Data Menggunakan TOPSIS.....	44
4.2.5 Intrepetasi Hasil Berdasarkan Nilai Rata-Rata Preferensi dan <i>Equal Interval</i>	50
BAB 5 KESIMPULAN DAN SARAN.....	53
5.1 Kesimpulan.....	53
5.2 Saran.....	53
DAFTAR PUSTAKA.....	55
LAMPIRAN.....	59

DAFTAR TABEL

Tabel 2.1 Ringkasan Tinjauan Pustaka.....	9
Tabel 4.1 Spesifikasi <i>Virtual Machine</i>	30
Tabel 4.2 Distribusi Rincian Data Target.....	33
Tabel 4.3 Skenario Serangan <i>Phishing</i>	35
Tabel 4.4 Hasil Simulasi Serangan <i>Phishing</i> berdasarkan Respon Target.....	40
Tabel 4.5 Data Hasil Serangan <i>Phishing</i> dalam Bentuk Kuantitatif.....	43
Tabel 4.6 Tipe dan Bobot Indikator Penilaian.....	45
Tabel 4.7 Cuplikan Matriks Ternormalisasi.....	46
Tabel 4.8 Cuplikan Matriks Ternormalisasi Terbobot.....	48
Tabel 4.9 Nilai Solusi Ideal Positif dan Negatif.....	49
Tabel 4.10 Hasil Jarak Setiap Alternatif ke Nilai Solusi Ideal.....	49
Tabel 4.11 Nilai Preferensi.....	50
Tabel 4.12 Rentang Nilai Klasifikasi Berdasarkan Kategori.....	51

DAFTAR GAMBAR

Gambar 3.1 <i>Phishing Attack Life Cycle</i>	19
Gambar 3.2 <i>Flowchart</i> Jalan Penelitian.....	21
Gambar 4.1 Proses Bisnis Simulasi Serangan <i>Phishing</i>	27
Gambar 4.2 Tampilan Halaman Palsu yang Dibuat.....	31
Gambar 4.3 Isi <i>email</i> yang digunakan dalam Simulasi Serangan <i>Phishing</i>	32
Gambar 4.4 Data yang telah diimpor ke Gophish.....	34
Gambar 4.5 Pembuatan serangan <i>phishing</i> di Gophish.....	35
Gambar 4.6 <i>Email</i> Konfirmasi Pendistribusian <i>Phishing</i> Dimulai.....	37
Gambar 4.7 <i>Email</i> Konfirmasi Pendistribusian <i>Phishing</i> Ditutup.....	38
Gambar 4.8 Pemantauan melalui CLI.....	39
Gambar 4.9 Dashboard Kampanye Serangan <i>Phishing</i> secara Keseluruhan.....	41
Gambar 4.10 Bukti Pelaporan <i>Email Phishing</i> ke WA <i>Helpdesk</i> IT.....	42
Gambar 4.11 Bukti Pelaporan <i>Email Pishing</i> ke <i>Email</i> CSIRT.....	42

DAFTAR LAMPIRAN

Lampiran 1 Konfigurasi Sistem dan Implementasi Gophish.....	60
Lampiran 2 Skenario Simulasi <i>Phishing</i> dan <i>Template Email</i>	63
Lampiran 3 Formula Perhitungan di <i>LibreOffice Calc</i>	69
Lampiran 4 Tabel Hasil Simulasi Serangan <i>Phishing</i> dalam Bentuk Numerik....	72
Lampiran 5 Tabel Hasil Matriks Normalisasi.....	85
Lampiran 6 Tabel Hasil Matriks Normalisasi Terbobot.....	91
Lampiran 7 Tabel Hasil Jarak ke Solusi Ideal.....	97
Lampiran 8 Tabel Hasil Nilai Preferensi.....	103
Lampiran 9 Surat Izin Penelitian.....	109
Lampiran 10 Surat Balasan Izin Penelitian.....	110
Lampiran 11 Dokumen <i>Non-Disclosure Agreement</i> (NDA).....	111
Lampiran 12 <i>Checklist Setup</i> Instalasi dan Konfigurasi Gophish.....	116
Lampiran 13 <i>Checklist Setup</i> Distribusi Simulasi Serangan <i>Phishing</i>	119
Lampiran 14 Dokumentasi Kegiatan di Lapangan.....	121
Lampiran 15 Jadwal Penelitian.....	123
Lampiran 16 Kartu Bimbingan Skripsi.....	124
Lampiran 17 Hasil Cek Plagiarisme.....	125

DAFTAR SINGKATAN

AHP	<i>Analytical Hierarchy Process</i>
APWG	<i>Anti-Phishing Work Group</i>
BSSN	Badan Siber dan Sandi Negara
CKC	<i>Cyber Kill Chain</i>
CSIRT	<i>Computer Security Incident Respons Team</i>
CSS	<i>Cascading Style Sheets</i>
DBIR	<i>Data Breach Investigations Report</i>
HAIS-Q	<i>Human Aspect of Information Security Questionnaire</i>
HTML	<i>Hypertext Markup Language</i>
IMAP	<i>Internet Message Access Protocol</i>
IP	<i>Internet Protocol</i>
KAB	<i>Knowledge, Attitude, Behaviour</i>
MCDA	<i>Multi-Criteria Decision Analysis</i>
REST API	<i>Representational State Transfer Application Programming Interface</i>
SMTP	<i>Simple Mail Transfer Protocol</i>
SSL	<i>Secure Socket Layer</i>
TOPSIS	<i>Technique for Order Preference by Similarity to Ideal Solution</i>
URL	<i>Uniform Resource Locator</i>
VM	<i>Virtual Machine</i>