BAB 4
HASIL PENELITIAN

4.1 Ringkasan Hasil Penelitian

Penelitian tingkat kesadaran keamanan siber karyawan terhadap serangan *phishing* ini dilakukan secara langsung di lingkungan PT XYZ. Penelitian ini berlangsung secara *on-site* dengan durasi total penelitian selama 30 hari kerja terhitung sejak 14 Maret 2025 sampai 02 Mei 2025. Penelitian ini menggunakan data perilaku nyata berdasarkan respon karyawan terhadap serangan *phishing* yang disimulasikan menggunakan Gophish. Proses penelitian ini berlangsung sesuai dengan ruang lingkup (batasan) yang diberikan oleh pihak perusahaan atas dasar kemungkinan risiko yang terjadi sehingga dalam penelitian ini seluruh aktivitas berada dibawah pengawasan Tim CSIRT perusahaan.

Jumlah sampel yang dilibatkan dalam penelitian ini sebanyak 122 karyawan yang terdiri dari divisi *Corporate Secretary, Corporate Safety & Security, Human Capital & General Affairs, Internal Audit,* dan *Marketing*. Proses penelitian ini mencakup tahapan sesi diskusi dengan pihak perusahaan, konfigurasi dan perancangan pola skenario simulasi serangan *phishing*, dan pendistribusian serangan *phishing* yang dijalankan di sistem *email* perusahaan.

Implementasi rekayasa sosial yang digunakan dalam serangan *phishing* pada penelitian ini disesuaikan dengan fenomena aktual tentang pemberian promo kepada karyawan sebesar 25% untuk pembelian emas batangan sebanyak 5 gram. Pendistribusian serangan *phishing* dilakukan selama tiga hari kerja yang berlangsung pada 25 April 2025 s.d. 30 April 2025. Hasil distribusi serangan *phishing* didapatkan berdasarkan respon terakhir target dengan rincian sebanyak 115 *email sent*, 4 *email reported*, 0 *email opened*, 2 *clicked link*, dan 1 *submitted data*.

Hasil tersebut kemudian dilakukan analisis dan perhitungan TOPSIS untuk menormalisasi data, menentukan solusi ideal, dan mendapatkan nilai preferensi.

Kemudian, untuk menginterpretasi hasil secara umum dan deskriptif dilakukannya penyesuaian berdasarkan nilai rata-rata (*mean*) dari nilai preferensi TOPSIS dengan kategori tinggi, sedang, dan rendah. Kategori tersebut dihitung secara statistik menggunakan *equal interval methode* sehingga menghasilkan rentang nilai yang nantinya digunakan sebagai acuan dalam pengambilan kesimpulan.

4.2 Pembahasan

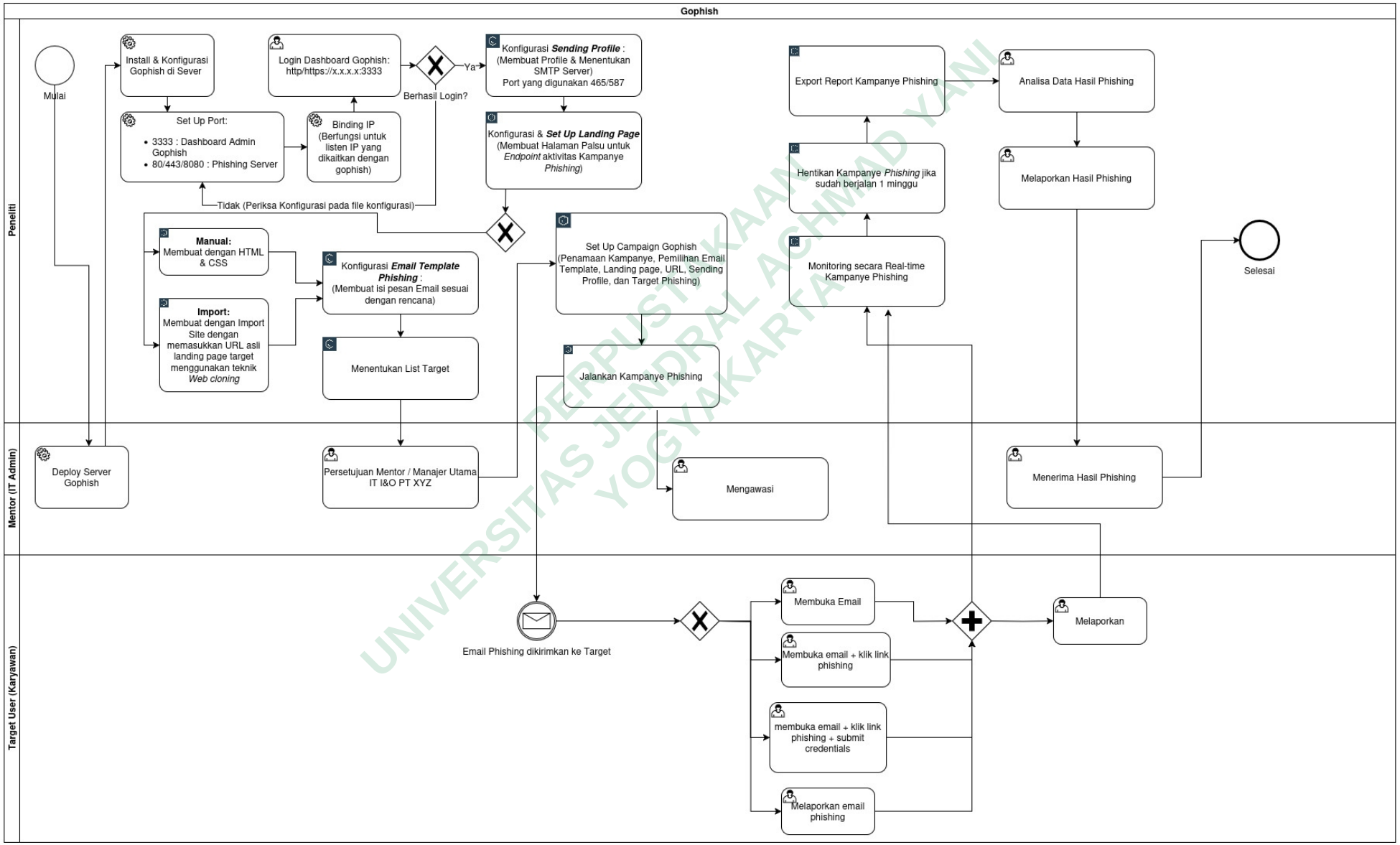
4.2.1 Konfigurasi dan Perancangan Pola Simulasi Serangan *Phishing*

1) Reconnaissance

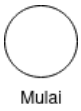
Tahap awal dalam penelitian ini merupakan proses yang bertujuan untuk memperoleh informasi pendukung yang relevan dalam menunjang kelancaran kegiatan penelitian. Pada tahap ini, dilakukan pertemuan antara peneliti dan pihak perusahaan, yang diwakili oleh General Manager Unit IT *Infrastructure & Operation* PT XYZ serta seorang karyawan yang ditunjuk sebagai pendamping penelitian.

Pertemuan yang dilaksanakan pada Jumat, 14 Maret 2025, diawali dengan pemaparan maksud dan tujuan penelitian sebagaimana tercantum dalam proposal. Selain itu, peneliti juga menjelaskan gambaran umum proses bisnis yang menjadi ruang lingkup dalam pelaksanaan tugas akhir ini. Gambar 4.1 menyajikan ilustrasi proses bisnis simulasi serangan *phishing* yang menjadi dasar pelaksanaan penelitian di lingkungan perusahaan. Penjelasan terhadap gambar tersebut bertujuan untuk menyelaraskan pemahaman antara peneliti dan pihak perusahaan terkait arah dan metode pelaksanaan penelitian.

Gambar 4.1 Proses Bisnis Simulasi Serangan *Phishing*



Keterangan legenda BPMN proses bisnis simulasi serangan *phishing* yang digunakan adalah sebagai berikut:



Memulai *event.*

Service task digunakan untuk proses yang dilakukan di server atau komputer.

User task digunakan untuk proses yang dilakukan oleh aktor.

Gophish *task* digunakan untuk proses yang dilakukan pada *dashboard* admin Gophish.

Exlusive gateway digunakan untuk memastikan berbagai kondisi dan respon yang berbeda.

Parallel gateway digunakan untuk menjalankan secara bersamaan.

Event selesai.

Selanjutnya, sesi diskusi dilaksanakan untuk membahas kebutuhan data yang diperlukan dalam proses penelitian. Data sekunder yang dibutuhkan meliputi:

- Data karyawan berupa daftar alamat *email* yang akan dijadikan target dalam simulasi serangan *phishing*;
- Dokumen-dokumen internal yang relevan (studi dokumen);
- Estimasi durasi pendistribusian simulasi *phishing*.

Sebagai hasil dari sesi diskusi ini, perusahaan menetapkan ruang lingkup (batasan) penelitian sebagai berikut:

1. Seluruh perangkat dan komponen penelitian dipasang pada sistem internal perusahaan dengan pengawasan dari mentor dan Tim CSIRT.
2. Penelitian melibatkan 122 karyawan yang tersebar di lima divisi, yaitu *Corporate Secretary, Corporate Safety & Security, Human Capital & General Affairs, Internal Audit, dan Marketing.*
3. Simulasi serangan *phishing* dilakukan satu kali dengan konten berkarakteristik pemula (*entry-level*), untuk mengukur tingkat kesadaran awal tanpa mengganggu operasional perusahaan.

Selain itu, studi dokumen yang dilakukan mencakup analisis terhadap desain dan struktur aplikasi *web* internal serta pola komunikasi *email* yang umum digunakan dalam perusahaan. Informasi ini digunakan sebagai referensi dalam perancangan konten dan skenario simulasi serangan *phishing*.

Berdasarkan hasil diskusi, perusahaan memberikan fleksibilitas kepada peneliti dalam menentukan durasi pelaksanaan simulasi. Dengan mempertimbangkan kondisi operasional dan efektivitas pengujian, pendistribusian simulasi serangan *phishing* dilakukan selama tiga hari kerja.

2) Weaponization

Tahap persiapan dalam penelitian ini mencakup serangkaian kegiatan untuk memfasilitasi pelaksanaan simulasi serangan *phishing* yang sesuai dengan ruang lingkup dan ketentuan dari pihak perusahaan. Kegiatan utama pada tahap ini meliputi konfigurasi sistem, perancangan skenario, serta penyiapan media dan data yang akan digunakan dalam simulasi.

(1) Konfigurasi Sistem Gophish

Untuk keperluan simulasi, sistem *Gophish* diimplementasikan pada lingkungan *virtual machine* (VM) yang

disediakan oleh pihak perusahaan. Sistem ini dikonfigurasi agar dapat berjalan secara stabil di lingkungan internal, menggunakan sistem operasi berbasis Linux. Seluruh konfigurasi dan pengujian sistem dilakukan dengan pengawasan mentor perusahaan. Tabel 4.1 merupakan spesifikasi VM yang diberikan oleh perusahaan.

Tabel 4.1 Spefisikasi *Virtual Machine*

Komponen	**Spesifikasi**
Sistem Operasi	Ubuntu Server 20.04 LTS
CPU	4 vCPU
RAM	4 GB
Storage	50 GB SSD
IP *Address* (Internal)	192.168.XXX.XX

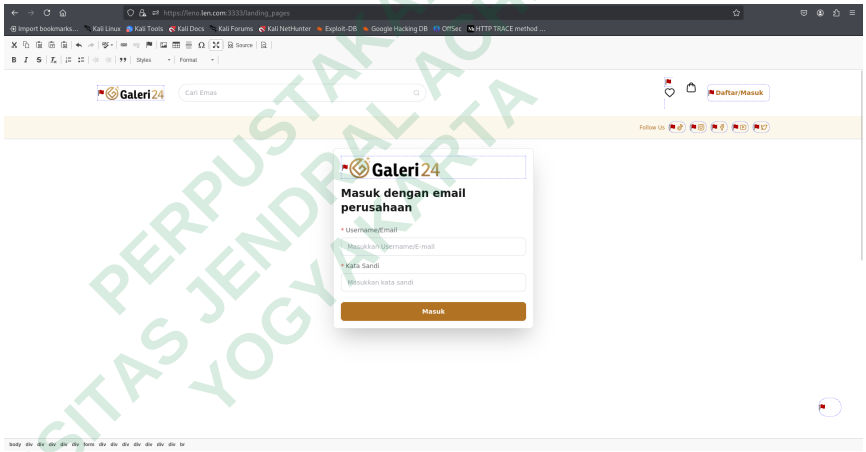
Pengaturan meliputi instalasi perangkat lunak, konfigurasi parameter sistem seperti *port* akses dan autentikasi, serta pendaftaran Gophish sebagai layanan sistem agar dapat berjalan otomatis. Detail teknis terkait konfigurasi perangkat lunak dan skrip sistem tidak disajikan dalam bab ini dan dapat dilihat pada lampiran 1.

(2) Perancangan Skenario Pola Simulasi Serangan *Phishing*

Skenario simulasi dirancang dengan pendekatan rekayasa sosial (*social engineering*) berdasarkan isu yang sedang relevan di masyarakat, yakni promosi investasi emas. Dalam skenario ini, peneliti menyusun narasi seolah-olah perusahaan PT XYZ bekerja sama dengan PT Pegadaian Galeri 24 memberikan penawaran khusus kepada karyawan. Konten email menyertakan promosi fiktif

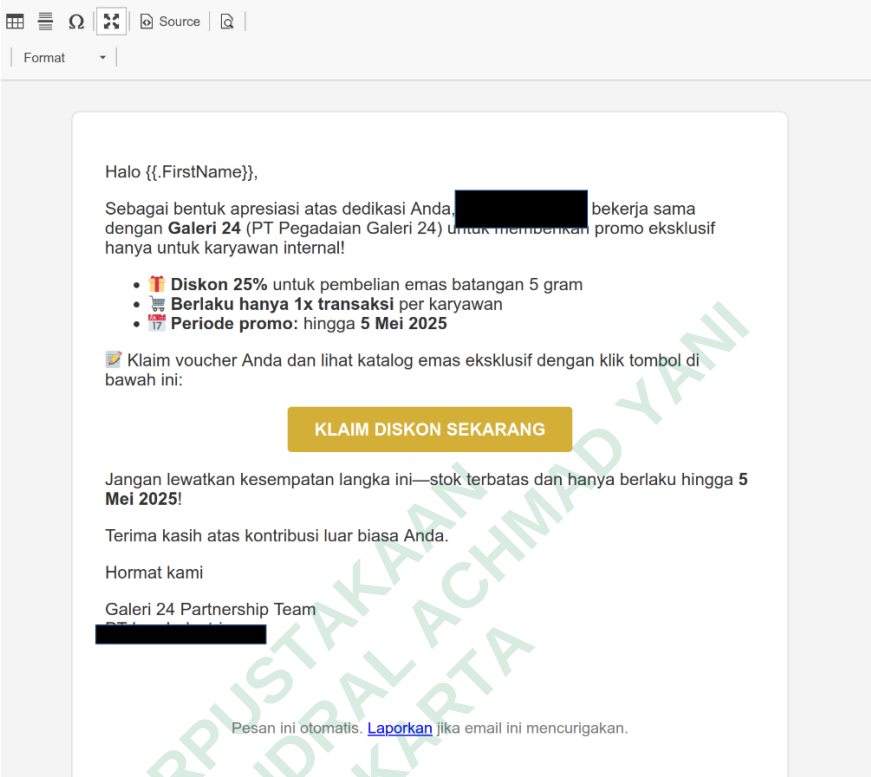
berupa potongan harga 25% untuk pembelian emas sebanyak lima gram.

Skenario ini disesuaikan dengan kebijakan perusahaan, yakni bersifat *entry-level* dan tidak mengandung risiko tinggi. Tujuan utamanya adalah mengukur kesadaran pengguna terhadap potensi ancaman *phishing* tanpa mengganggu operasional perusahaan. Dalam perancangan ini terdapat dua aktivitas utama yaitu pembuatan desain halaman *phishing* dan *email phishing* yang digunakan. Tampilan secara grafis dari kedua aktivitas itu dapat dilihat pada gambar 4.2 dan gambar 4.3 berikut ini.



Gambar 4.2 Tampilan Halaman Palsu yang Dibuat

Gambar 4.2 merupakan halaman palsu yang digunakan dalam simulasi serangan *phishing* yang dibuat menggunakan teknik *cloning* yang tersedia di fitur Gophish.



Gambar 4.3 Isi *email* yang digunakan dalam Simulasi Serangan *Phishing*

Gambar 4.3 merupakan gambaran isi *email* yang telah disesuaikan dengan ruang lingkup sebagai email *phishing* yang digunakan. Isi *email* ini dibuat menggunakan kombinasi HTML dan CSS.

(3) Persiapan Infrastruktur Simulasi

Dalam tahap ini, peneliti melakukan konfigurasi terhadap tiga komponen utama dalam sistem *Gophish*:

- Profil Pengirim (*Sending Profile*): Disesuaikan agar dapat mengirim *email phishing* secara massal menggunakan layanan SMTP dan menerima umpan balik melalui IMAP. *Email* pribadi yang dihosting melalui penyedia layanan profesional digunakan sebagai media pengiriman.

- Halaman *Phishing* (*Phishing Page*): Peneliti memanfaatkan fitur kloning halaman dari Gophish untuk mereplikasi tampilan halaman *login* PT Pegadaian Galeri24. Namun, fitur *capture submitted data* tidak diaktifkan demi menjaga aspek etika dan keamanan data.
- *Template Email: Template* disusun dalam format HTML, dengan gaya komunikasi menyerupai *email* resmi. Penyesuaian dilakukan agar sesuai dengan pola komunikasi umum di lingkungan perusahaan.

(4) Penyiapan Data Target

Data target yang digunakan dalam simulasi diperoleh dari pihak perusahaan dan terdiri dari 122 entri karyawan dari lima divisi. Informasi mencakup nama, *email*, dan unit kerja. Data ini diolah dalam format standar (.CSV) untuk proses impor ke sistem Gophish melalui fitur *Users & Groups*.

Distribusi data berdasarkan unit kerja disajikan pada tabel 4.2, sedangkan tampilan antarmuka pengelompokan data dalam sistem dapat dilihat pada gambar 4.4. Data ini kemudian digunakan dalam proses pendistribusian *email* simulasi pada tahap selanjutnya.

Tabel 4.2 Distribusi Rincian Data Target

Unit Kerja	Jumlah
Corporate Secretary	27
Corporate Safety & Security	16
Human Capital & General Affairs	38
Internal Audit	16
Marketing	25

Unit Kerja	Jumlah
Total	122

Gambar 4.4 Data yang telah diimpor ke Gophish

4.2.2 Pelaksanaan Simulasi Serangan *Phishing*

1) Distribution

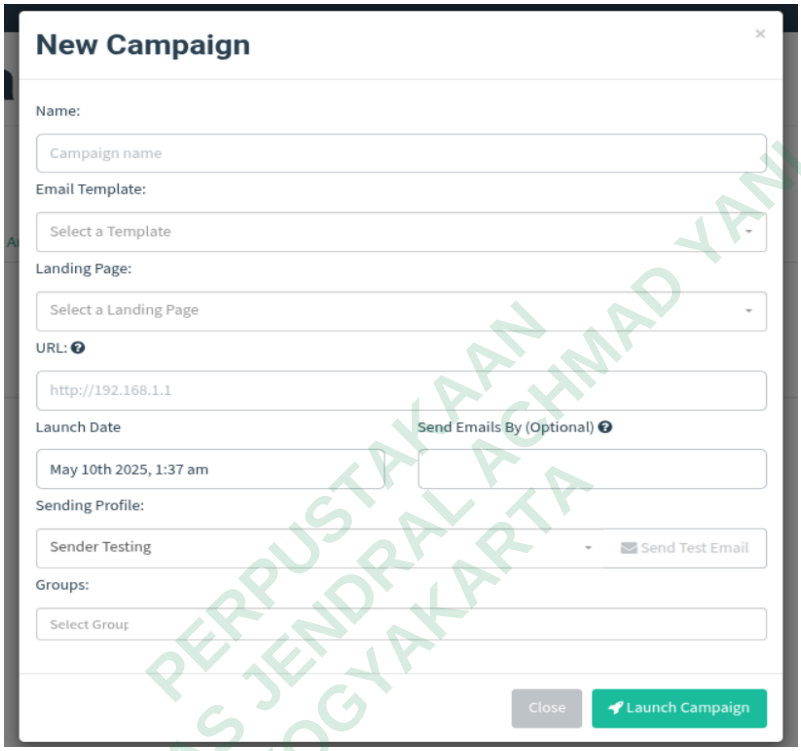
Tahap distribusi merupakan inti dari implementasi simulasi serangan *phishing*, yang menjadi dasar pengukuran tingkat kesadaran keamanan siber karyawan. Pada tahap ini, seluruh elemen yang telah disiapkan sebelumnya—meliputi profil pengirim, halaman *phishing*, *template email*, dan data target—digabungkan ke dalam sistem simulasi melalui fitur *campaign management* pada *platform* Gophish.

Pendistribusian dilakukan secara tersegmentasi berdasarkan unit kerja untuk mempermudah proses *monitoring* dan analisis hasil. Oleh karena itu, lima kampanye dibuat terpisah, masing-masing mewakili satu dari lima divisi yang dilibatkan dalam penelitian.

Setiap kampanye mencakup pengaturan:

- Nama kampanye sesuai unit kerja,
- Template *email* berdasarkan skenario rekayasa sosial,
- Halaman *phishing* (*landing page*),
- Profil pengirim,

- Daftar target yang disesuaikan berdasarkan data karyawan,
- Jadwal distribusi dan notifikasi ke tim pengawas internal.



Gambar 4.5 Pembuatan serangan *phishing* di Gophish

Gambar 4.5 memperlihatkan tampilan antarmuka *dashboard* Gophish pada saat konfigurasi kampanye dilakukan.

Tabel 4.3 Skenario Serangan *Phishing*

Indikator	Keterangan
Waktu Pendistribusian Kampanye Simulasi Serangan *Phishing*	• 13.35 WIB untuk Divisi *Corporate Safety & Security* • 13.52 WIB untuk Divisi *Corporate Secretary* • 13.54 WIB untuk Divisi *Human Capital & General Affairs* • 13.57 WIB untuk Divisi *Internal*

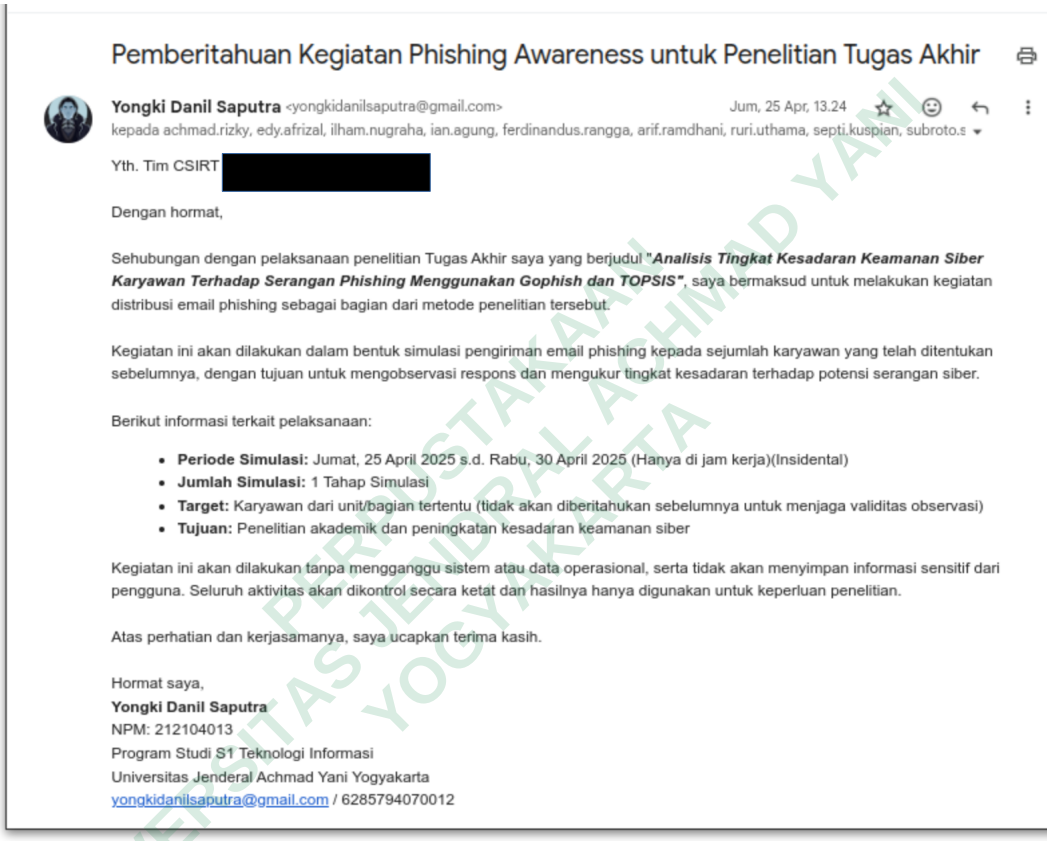
Indikator	Keterangan
	Audit • 13.58 WIB untuk Divisi *Marketing*
Durasi	3 hari (72 jam) (hari kerja)
Platform Phishing	*Email* masing-masing karyawan
Link Phishing	http[redacted]m
Pola Rekayasa Sosial yang digunakan dalam *Phishing*	Pemberian Hadiah dalam bentuk potongan 25% kepada seluruh karyawan (target) saat pembelian Emas sebanyak 5 gram di Galeri24
Waktu konfirmasi ke Tim CSIRT Perusahaan	Sebelum dan Sesudah Kampanye Simulasi *Phishing* diselenggarakan.

Skenario distribusi disusun secara sistematis dan terdokumentasi dalam Tabel 4.3, yang merinci waktu pelaksanaan, metode distribusi, dan format pelaporan kepada Tim CSIRT perusahaan. Distribusi *email* dilakukan selama tiga hari kerja, dimulai pada Jumat, 25 April 2025 pukul 13.00 WIB dan berakhir pada Selasa, 29 April 2025 pukul 15.00 WIB. Proses ini dilakukan menggunakan sistem *Gophish* dan dikirimkan kepada 122 alamat *email* bisnis yang telah ditentukan.

Skenario serangan *phishing* memanfaatkan tema promosi pembelian emas sebagai teknik rekayasa sosial. Tema ini dipilih berdasarkan fenomena aktual yang tengah berkembang di masyarakat terkait peningkatan minat terhadap investasi emas di tengah tekanan inflasi ekonomi. Pendekatan ini dipertimbangkan untuk meningkatkan realisme simulasi dan relevansi kontekstual.

Seluruh aktivitas distribusi dilakukan sesuai dengan prosedur etis yang telah disepakati dan berada di bawah pengawasan langsung Tim

CSIRT perusahaan. Untuk memastikan pelaksanaan berjalan sesuai rencana, peneliti melakukan konfirmasi kepada pihak internal melalui komunikasi resmi, sebagaimana didokumentasikan dalam gambar 4.6 dan gambar 4.7.



Pemberitahuan Kegiatan Phishing Awareness untuk Penelitian Tugas Akhir

Yongki Danil Saputra <yongkidanilsaputra@gmail.com> Jum, 25 Apr, 13.24

kepada achmad.rizky, edy.afrizal, ilham.nugraha, ian.agung, ferdinandus.rangga, arif.ramdhani, ruri.uthama, septi.kuspian, subroto.s

Yth. Tim CSIRT [redacted]

Dengan hormat,

Sehubungan dengan pelaksanaan penelitian Tugas Akhir saya yang berjudul "***Analisis Tingkat Kesadaran Keamanan Siber Karyawan Terhadap Serangan Phishing Menggunakan Gophish dan TOPSIS***", saya bermaksud untuk melakukan kegiatan distribusi email phishing sebagai bagian dari metode penelitian tersebut.

Kegiatan ini akan dilakukan dalam bentuk simulasi pengiriman email phishing kepada sejumlah karyawan yang telah ditentukan sebelumnya, dengan tujuan untuk mengobservasi respons dan mengukur tingkat kesadaran terhadap potensi serangan siber.

Berikut informasi terkait pelaksanaan:

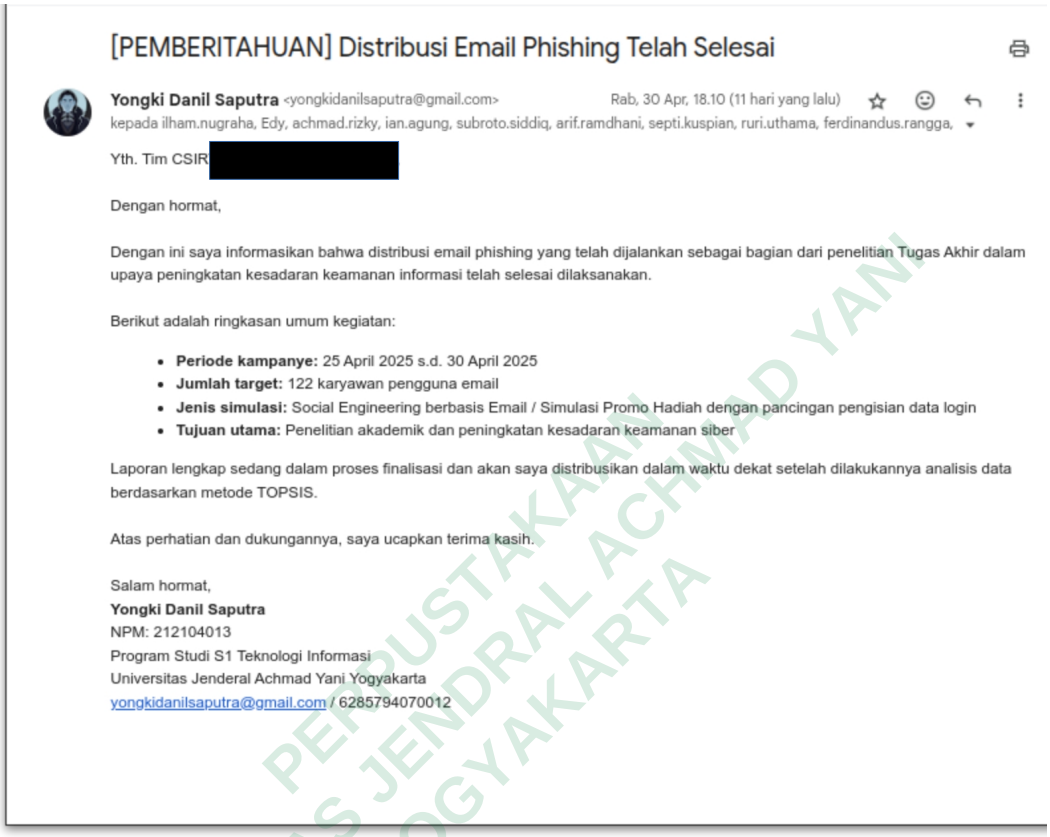
- **Periode Simulasi:** Jumat, 25 April 2025 s.d. Rabu, 30 April 2025 (Hanya di jam kerja)(Insidental)
- **Jumlah Simulasi:** 1 Tahap Simulasi
- **Target:** Karyawan dari unit/bagian tertentu (tidak akan diberitahukan sebelumnya untuk menjaga validitas observasi)
- **Tujuan:** Penelitian akademik dan peningkatan kesadaran keamanan siber

Kegiatan ini akan dilakukan tanpa mengganggu sistem atau data operasional, serta tidak akan menyimpan informasi sensitif dari pengguna. Seluruh aktivitas akan dikontrol secara ketat dan hasilnya hanya digunakan untuk keperluan penelitian.

Atas perhatian dan kerjasamanya, saya ucapkan terima kasih.

Hormat saya,
Yongki Danil Saputra
NPM: 212104013
Program Studi S1 Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta
yongkidanilsaputra@gmail.com / 6285794070012

Gambar 4.6 *Email* Konfirmasi Pendistribusian *Phishing* Dimulai



[PEMBERITAHUAN] Distribusi Email Phishing Telah Selesai

Yongki Danil Saputra <yongkidanilsaputra@gmail.com> Rab, 30 Apr, 18.10 (11 hari yang lalu)

kepada ilham.nugraha, Edy, achmad.rizky, ian.agung, subroto.siddiq, arif.ramdhani, septi.kuspian, ruri.uthama, ferdinandus.rangga,

Yth. Tim CSIR [redacted]

Dengan hormat,

Dengan ini saya informasikan bahwa distribusi email phishing yang telah dijalankan sebagai bagian dari penelitian Tugas Akhir dalam upaya peningkatan kesadaran keamanan informasi telah selesai dilaksanakan.

Berikut adalah ringkasan umum kegiatan:

- **Periode kampanye:** 25 April 2025 s.d. 30 April 2025
- **Jumlah target:** 122 karyawan pengguna email
- **Jenis simulasi:** Social Engineering berbasis Email / Simulasi Promo Hadiah dengan pancingan pengisian data login
- **Tujuan utama:** Penelitian akademik dan peningkatan kesadaran keamanan siber

Laporan lengkap sedang dalam proses finalisasi dan akan saya distribusikan dalam waktu dekat setelah dilakukannya analisis data berdasarkan metode TOPSIS.

Atas perhatian dan dukungannya, saya ucapkan terima kasih.

Salam hormat,
Yongki Danil Saputra
NPM: 212104013
Program Studi S1 Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta
yongkidanilsaputra@gmail.com / 6285794070012

Gambar 4.7 *Email* Konfirmasi Pendistribusian *Phishing* Ditutup

Distribusi *email* dilakukan satu kali untuk masing-masing target, dan status penerimaan *email* dikonfirmasi melalui koordinasi dengan administrator sistem email perusahaan. Langkah ini telah memperoleh persetujuan dari General Manager Unit IT *Infrastructure* & *Operation*.

2) *Exploitation*

Tahap eksploitasi dalam penelitian ini merujuk pada proses pemantauan secara langsung terhadap respon karyawan terhadap simulasi serangan *phishing* yang telah didistribusikan. Pemantauan dilakukan untuk memastikan bahwa proses berjalan lancar dan untuk mengumpulkan data yang menjadi dasar evaluasi tingkat kesadaran keamanan siber.

Pemantauan dilakukan melalui dua pendekatan:

- Antarmuka *dashboard Gophish*, yang menampilkan data statistik *real-time* dari setiap kampanye.
- *Monitoring log system*, untuk mendeteksi adanya gangguan teknis yang dapat menghambat pelaksanaan kampanye dengan menjalankan perintah:

```
sudo journalctl -u gophish -f
```

Gambar 4.8 Pemantauan melalui CLI

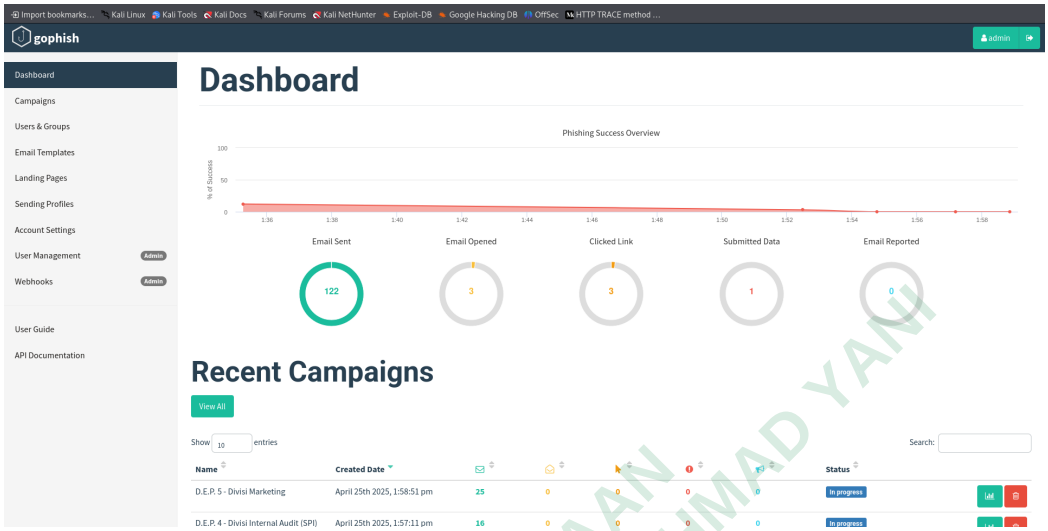
Dalam pemantauan ini parameter utama yang menjadi pusat *monitoring* secara *backend* dan *real-time* ini ditunjukkan dengan bagian gambar 4.8 yang dianotasikan garis kotak merah. Parameter tersebut berupa *timestamp* (waktu) aktivitas *client* yang sedang berlangsung, *level* atau jenis informasi yang diberikan berdasarkan aktivitas *client*, serta *message* atau keterangan berdasarkan level informasi yang didapatkan. Dalam parameter *message* ini, terdapat informasi berupa IP *client*, *Request path* yang terdapat di log HTTP dan respon yang diberikan oleh server.

Respon target terhadap simulasi direkam berdasarkan indikator yang digunakan untuk menilai tingkat kesadaran pengguna terhadap potensi ancaman *phishing*. Dalam penelitian ini, penilaian difokuskan pada status akhir dari setiap email yang diterima oleh target. Berdasarkan hasil pemantauan terhadap total 122 *email phishing* yang dikirimkan selama periode 25–29 April 2025, diperoleh hasil sebagai berikut:

Tabel 4.4 Hasil Simulasi Serangan *Phishing* berdasarkan Respon Target

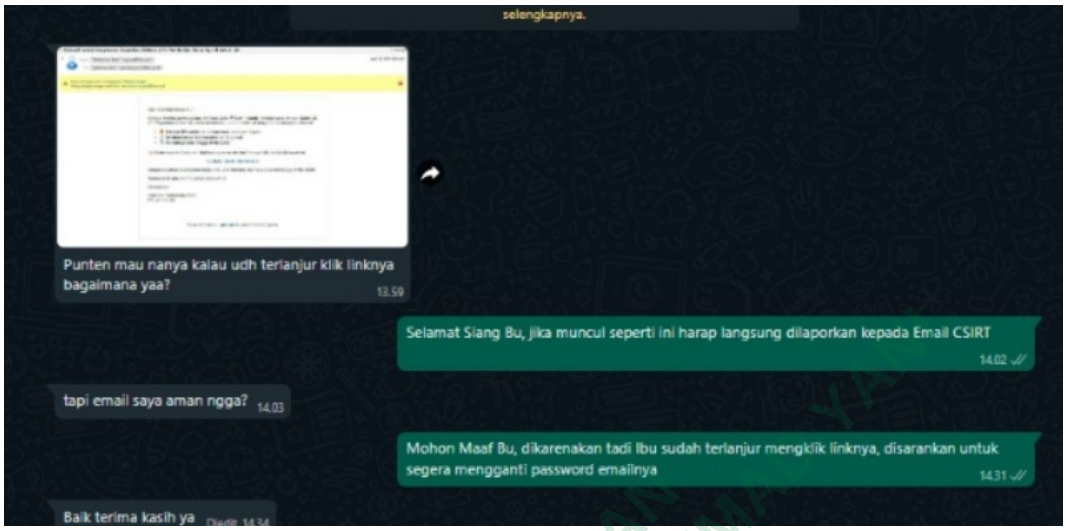
Status	**Jumlah *Email***
Email Sent	115
Email Opened	0
Clicked Link	2
Submitted Data	1
Email Reported	4

Gambar 4.9 menunjukkan aktivitas pemantauan yang dilakukan peneliti selama pendistribusian serangan *phishing* berlangsung. Gambar tersebut menampilkan grafik jumlah respon target secara umum dan keseluruhan berdasarkan serangan *phishing* yang sedang di distribusikan.



Gambar 4.9 Dashboard Kampanye Serangan *Phishing* secara Keseluruhan

Meskipun terdapat 4 laporan *phishing*, pada praktiknya, laporan tersebut tidak semuanya dilakukan melalui fitur pelaporan langsung dalam *mail client*. Sebagian besar target yang menyadari adanya aktivitas mencurigakan melaporkannya melalui *WhatsApp Helpdesk IT* dan sebagian lainnya melalui *email* ke Tim CSIRT perusahaan. Gambar 4.10 dan gambar 4.11 menunjukkan pelaporan *email* yang dikirimkan melalui *WhatsApp Helpdesk IT* dan *email* Tim CSIRT perusahaan.



Gambar 4.10 Bukti Pelaporan *Email Phishing* ke WA *Helpdesk* IT

Gambar 4.11 Bukti Pelaporan *Email Pishing* ke *Email* CSIRT

4.2.3 Klasifikasi Data Hasil Simulasi

Setelah tahap pemantauan dan pelaksanaan simulasi serangan *phishing* selesai, data yang diperoleh dari respon masing-masing target diklasifikasikan dan dikonversi ke dalam bentuk kuantitatif. Proses klasifikasi ini bertujuan untuk menyederhanakan data ke dalam format numerik yang dapat dianalisis lebih lanjut menggunakan metode *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS).

Dalam tahap ini, setiap unit kerja direpresentasikan melalui total jumlah target, dan dibagi berdasarkan lima kategori respon akhir, yaitu: *email sent, email reported, email opened, clicked link*, dan *submitted data*. Kategori tersebut menjadi indikator penilaian utama dalam metode TOPSIS. Data yang telah diklasifikasikan ini kemudian digunakan dalam proses normalisasi, pembobotan, dan perhitungan jarak terhadap solusi ideal (positif) dan solusi anti-ideal (negatif), sesuai dengan prinsip metode TOPSIS.

Tabel 4.5 menyajikan rincian data hasil simulasi *phishing* yang telah dikonversi untuk kebutuhan proses analisis.

Tabel 4.5 Data Hasil Serangan *Phishing* dalam Bentuk Kuantitatif

No	Nama Target	Divisi	*Email Sent*	*Email Reported*	*Email Opened*	*Clicked Link*	*Submitted Data*
1	Target A	*Health Safety & Environment*	1	0	0	0	0
2	Target B	*Health Safety & Environment*	0	1	0	0	0
3	Target C	*Corporate Security*	0	1	0	0	0
4	Target D	*Corporate Safety & Security*	0	0	0	0	1
5	Target E	*Health Safety*	1	0	0	0	0

No	Nama Target	Divisi	*Email Sent*	*Email Reported*	*Email Opened*	*Clicked Link*	*Submitted Data*
		& Environment					
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
121	Target DR	*Marketing & Sales - Air Force*	0	1	0	0	0
122	Target DS	*Marketing & Sales Center*	1	0	0	0	0
Jumlah			115	4	0	2	1

4.2.4 Analisis dan Perhitungan Data Menggunakan TOPSIS

Perhitungan dilakukan menggunakan aplikasi *LibreOffice Calc* untuk mempermudah pengolahan data. Implementasi rumus dalam perangkat lunak dijelaskan secara detail pada lampiran 3.

1) Menentukan Tipe dan Bobot Indikator Penilaian

Dalam penerapan metode *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS), langkah awal yang dilakukan adalah menentukan indikator atau kriteria yang merepresentasikan tingkat kesadaran karyawan terhadap simulasi serangan *phishing*. Indikator-indikator ini diturunkan dari status akhir hasil distribusi *email phishing* yang terekam melalui sistem Gophish.

TOPSIS mengklasifikasikan setiap indikator ke dalam dua tipe utama, yaitu:

- ***Benefit***, yaitu indikator yang nilainya semakin tinggi menunjukkan performa yang lebih baik.
- ***Cost***, yaitu indikator yang nilainya semakin rendah menunjukkan performa yang lebih baik (Putra dkk., 2020).

Klasifikasi indikator dalam penelitian ini disesuaikan dengan karakteristik respon terhadap serangan *phishing*:

- *Email reported* dan *email sent* dikategorikan sebagai indikator *benefit* karena menunjukkan tindakan proaktif atau kesadaran pasif dalam menghadapi potensi ancaman.
- *Email opened, clicked link*, dan *submitted data* dikategorikan sebagai indikator *cost* karena menunjukkan tingkat kerentanan yang berpotensi mengarah pada pelanggaran keamanan.

Selanjutnya, setiap indikator diberikan bobot berdasarkan tingkat kepentingannya terhadap evaluasi kesadaran keamanan. Pembobotan dilakukan dengan mempertimbangkan literatur serta penilaian subjektif-analitis yang mempertimbangkan konteks simulasi. Dalam teori TOPSIS, pembobotan ini penting untuk mencerminkan prioritas pengambilan keputusan secara proporsional (Hansen & Devlin, 2019).

Tabel 4.6 menyajikan daftar indikator, tipe klasifikasi, dan bobot yang digunakan dalam proses perhitungan TOPSIS.

Tabel 4.6 Tipe dan Bobot Indikator Penilaian

Indikator	Tipe	Bobot
Email Sent	*Benefit*	0.25
Email Reported	*Benefit*	0.15
Email Opened	*Cost*	0.15
Clicked Link	*Cost*	0.20
Submitted Data	*Cost*	0.25

Klasifikasi indikator tersebut memungkinkan pendekatan evaluasi yang komprehensif dan selaras dengan prinsip dasar TOPSIS, yaitu memilih alternatif yang paling dekat dengan solusi ideal positif dan terjauh dari solusi negatif (Kostelić, 2025). Dengan ini, setiap karyawan dapat dievaluasi secara objektif berdasarkan kombinasi respon yang paling aman dan paling berisiko dalam konteks simulasi *phishing*.

2) Menentukan Matriks Keputusan Ternormalisasi

Langkah selanjutnya dalam metode TOPSIS adalah melakukan normalisasi terhadap data mentah yang telah diklasifikasikan sebelumnya. Normalisasi bertujuan untuk menyetarakan skala antar indikator, sehingga tidak ada kriteria yang mendominasi akibat perbedaan satuan atau rentang nilai. Proses normalisasi dilakukan menggunakan rumus standar *Euclidean normalization* sebagaimana diterapkan dalam metode TOPSIS (Putra dkk., 2020).

$$X_{ij} = \frac{X_{ij}}{\sqrt{\sum_{n=1}^{m} X_{nj}^2}}$$

Rumus ini dihitung dengan membagi setiap nilai pada kolom kriteria terhadap akar kuadrat dari jumlah kuadrat seluruh nilai pada kolom tersebut. Hal ini memastikan bahwa setiap nilai berada dalam rentang 0 hingga 1.

Hasil dari proses normalisasi disajikan dalam bentuk matriks keputusan ternormalisasi. Tabel 4.7 berikut menyajikan cuplikan hasil normalisasi dari beberapa target untuk setiap indikator:

Tabel 4.7 Cuplikan Matriks Ternormalisasi

No	Nama Target	*Email Sent*	*Email Reported*	*Email Opened*	*Clicked Link*	*Submitted Data*
1	Target A	0.093	0.000	0.000	0.000	0.000

No	Nama Target	*Email Sent*	*Email Reported*	*Email Opened*	*Clicked Link*	*Submitted Data*
2	Target B	0.000	0.500	0.000	0.000	0.000
3	Target C	0.000	0.500	0.000	0.000	0.000
4	Target D	0.000	0.000	0.000	0.000	1.000
5	Target E	0.093	0.000	0.000	0.000	0.000
. . .	. . .	. . .	. . .	. . .	. . .	. . .
. . .	. . .	. . .	. . .	. . .	. . .	. . .
. . .	. . .	. . .	. . .	. . .	. . .	. . .
121	Target DR	0.000	0.500	0.000	0.000	0.000
122	Target DS	0.093	0.000	0.000	0.000	0.000

Melalui tabel tersebut, terlihat adanya variasi nilai antar target berdasarkan masing-masing indikator. Nilai-nilai inilah yang akan digunakan dalam tahap selanjutnya, yaitu pembobotan dan pembentukan matriks keputusan ternormalisasi terbobot.

3) Membentuk Matriks Keputusan Ternormalisasi Terbobot

Tahapan selanjutnya dalam penerapan metode TOPSIS adalah membentuk matriks keputusan ternormalisasi terbobot. Matriks ini diperoleh dengan mengalikan setiap elemen dalam matriks keputusan ternormalisasi dengan bobot masing-masing indikator. Secara matematis, proses ini mengikuti prinsip dasar TOPSIS, di mana nilai normalisasi yang telah dihasilkan sebelumnya dikalikan dengan bobot penting dari masing-masing kriteria. Tujuannya adalah agar setiap kriteria berkontribusi secara

proporsional terhadap evaluasi akhir, sesuai dengan tingkat kepentingannya (Putra dkk., 2020).

Rumus umum yang digunakan adalah:

$V_{ij} = r_{ij} \cdot w_j$

di mana:

- V_{ij} = nilai keputusan ternormalisasi terbobot,
- r_{ij} = nilai hasil ternormalisasi,
- w_j = bobot dari indikator ke-j.

Sehingga, dari perhitungan matriks ternormalisasi terbobot diperoleh seperti pada tabel 4.8 berikut.

Tabel 4.8 Cuplikan Matriks Ternormalisasi Terbobot

No	Nama Target	*Email Sent*	*Email Reported*	*Email Opened*	*Clicked Link*	*Submitted Data*
1	Target A	0.023	0.000	0.000	0.000	0.000
2	Target B	0.000	0.075	0.000	0.000	0.000
3	Target C	0.000	0.075	0.000	0.000	0.000
4	Target D	0.000	0.000	0.000	0.000	0.250
5	Target E	0.023	0.000	0.000	0.000	0.000
. . .	. . .	. . .	. . .	. . .	. . .	. . .
. . .	. . .	. . .	. . .	. . .	. . .	. . .
. . .	. . .	. . .	. . .	. . .	. . .	. . .
121	Target DR	0.000	0.075	0.000	0.000	0.000
122	Target DS	0.023	0.000	0.000	0.000	0.000

4) Menentukan Nilai Solusi Ideal Positif dan Negatif

Kemudian dilakukan pencarian nilai solusi ideal positif dan negatif yang berdasarkan tipe dari masing-masing indikator sehingga diperoleh hasil seperti pada tabel 4.9 dibawah ini.

Tabel 4.9 Nilai Solusi Ideal Positif dan Negatif

Indikator	Ideal Positif	Ideal Negatif
Email Sent	0.023	0.000
Email Reported	0.075	0.000
Email Opened	0.000	0.000
Clicked Link	0.000	0.141
Submitted Data	0.000	0.250

5) Menghitung Jarak Setiap Alternatif ke Nilai Solusi Ideal

Selanjutnya dilakukan proses menentukan jarak ke Solusi Ideal Positif (D^+) dan Solusi Ideal Negatif (D^-) sehingga diperoleh hasil sebagai berikut:

Tabel 4.10 Hasil Jarak Setiap Alternatif ke Nilai Solusi Ideal

Nama Target	Jarak ke positif ideal (D^+)	Jarak ke negatif ideal (D^-)
Target A	0.075	0.288
Target B	0.023	0.297
Target C	0.023	0.297
Target D	0.262	0.141
Target E	0.075	0.288
...	...	...
...	...	...
...	...	...

Nama Target	Jarak ke positif ideal (D^+)	Jarak ke negatif ideal (D^-)
Target DR	0.023	0.297
Target DS	0.075	0.288

6) Menghitung Nilai Preferensi

Setelah mendapatkan nilai jarak ke solusi ideal positif dan solusi ideal negatif, langkah selanjutnya menghitung nilai preferensi sehingga diperoleh:

Tabel 4.11 Nilai Preferensi

Target B	0.93
Target C	0.93
Target DR	0.93
Target W	0.93
Target A	0.79
...	...
...	...
...	...
Target I	0.61
Target D	0.35

4.2.5 Intrepetasi Hasil Berdasarkan Nilai Rata-Rata Preferensi dan *Equal Interval*

Berdasarkan nilai preferensi yang telah diperoleh berdasarkan hitungan TOPSIS, untuk mendapatkan hasil secara umum dilakukannya perhitungan dan penyesuaian terhadap tingkat kesadaran yang mengacu pada nilai rata-rata yang diklasifikasikan berdasarkan hasil *equal interval*. Langkah ini bertujuan untuk

menyederhanakan pemaknaan data kuantitatif dan memberikan gambaran umum terkait tingkat kesadaran keamanan siber terhadap serangan *phishing* di lingkungan PT XYZ.

1) Nilai rata-rata dari nilai preferensi

   Nilai rata-rata diperoleh berdasarkan rumus :

$$mean = \frac{Jumlah\ Nilai\ Preferensi}{Banyaknya\ Data\ (n)}$$

   Sehingga, nilai rata-rata yang diperoleh:

$$mean = \frac{Jumlah\ Nilai\ Preferensi}{Banyaknya\ Data\ (n)} = \frac{96.525}{122} = 0.79$$

2) Penentuan Interval Klasifikasi

   Penentuan interval klasifikasi ini berdasarkan nilai preferensi yang telah diperoleh pada TOPSIS dan tiga kelas kategori (tinggi, sedang, rendah) sesuai dengan asumsi tingkatan secara umum sehingga diketahui:

   - Nilai maksimum = 0.93
   - Nilai minimum = 0.35
   - Banyaknya kelas (n) = 3 (tinggi, sedang, rendah)

   Dan diperoleh nilai *equal interval* :

$$equal\ interval = \frac{Nilai\ Maksimum - Nilai\ minimum}{Banyaknya\ kelas\ (n)}$$

$$equal\ interval = \frac{0.93 - 0.35}{3} = 0.193333333 \approx 0.19$$

   Dari hasil tersebut, klasifikasi kategori tingkat kesadaran keamanan siber dibagi seperti pada tabel 4.12 berikut:

Tabel 4.12 Rentang Nilai Klasifikasi Berdasarkan Kategori

Kategori	Rentang Nilai
Tinggi	0.74 – 0.93
Sedang	0.55 – 0.73
Rendah	0.35 – 0.54

Berdasarkan nilai rata rata dari hasil preferensi TOPSIS sebesar 0.79 dan rentang nilai yang telah diperoleh sesuai pada tabel 4.12, tingkat kesadaran keamanan siber karyawan terhadap serangan *phishing* di lingkungan PT XYZ tergolong tinggi.