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

Yongki Danil Saputra, Chanief Budi Setiawan

INTISARI

Latar Belakang: Pesatnya perkembangan teknologi informasi telah meningkatkan efisiensi kerja, tetapi juga menimbulkan risiko baru seperti serangan *phishing* yang semakin marak di Indonesia. Serangan ini kerap menargetkan karyawan sebagai titik lemah dalam sistem keamanan perusahaan. Oleh karena itu, diperlukan pendekatan sistematis untuk mengukur tingkat kesadaran keamanan siber secara objektif, termasuk integrasi simulasi *phishing* menggunakan Gophish dengan metode analisis TOPSIS.

Tujuan: Penelitian ini bertujuan untuk mengukur tingkat kesadaran keamanan siber karyawan PT XYZ terhadap serangan *phishing* melalui simulasi menggunakan Gophish, serta menganalisis hasilnya dengan metode *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS).

Metode Penelitian: Penelitian ini menggunakan pendekatan kuantitatif deskriptif. Data dikumpulkan melalui simulasi serangan *phishing* dengan *platform* Gophish kepada 122 karyawan dari lima divisi di PT XYZ. Respon karyawan dikategorikan dalam lima indikator: *email sent, email opened, clicked link, submitted data*, dan *email reported*. Data hasil simulasi dianalisis menggunakan metode TOPSIS dan diklasifikasikan ke dalam kategori kesadaran (tinggi, sedang, rendah) menggunakan metode *equal interval*.

Hasil: Dari total 122 target, 115 *email* diabaikan, 0 *email* yang dibuka , 2 *email* berhasil mengarahkan pengguna untuk mengklik tautan *phishing*, 1 orang mengirimkan data, dan 4 orang melaporkan *email* sebagai *phishing*. Berdasarkan analisis TOPSIS dan nilai rata-rata yang diperoleh dari nilai preferensi sebesar 0.79, responden menunjukkan tingkat kesadaran pada kategori tinggi, dengan sedikit yang tergolong sedang atau rendah.

Kesimpulan: Tingkat kesadaran keamanan siber karyawan PT XYZ berada pada kategori tinggi, dengan indikasi bahwa meskipun terdapat pemahaman dasar mengenai ancaman *phishing*, masih diperlukan pelatihan berkelanjutan untuk memperkuat ketahanan terhadap serangan siber.

Kata-kunci: Kesadaran Keamanan Siber, Serangan *Phishing*, Gophish, TOPSIS.

ANALYSIS OF EMPLOYEES' CYBER SECURITY AWARENESS LEVEL TOWARDS PHISHING ATTACKS USING GOPHISH AND TECHNIQUE FOR ORDER PREFERENCE BY SIMILARITY TO IDEAL SOLUTION (TOPSIS)

Yongki Danil Saputra, Chanief Budi Setiawan

ABSTRACT

Background: *The rapid advancement of information technology has significantly enhanced work efficiency; however, it has also introduced new risks, such as the increasing prevalence of phishing attacks in Indonesia. These attacks often target employees as the weakest link in an organization's security system. Therefore, a systematic approach is required to objectively assess cybersecurity awareness levels, including the integration of phishing simulations using Gophish and analysis through the TOPSIS method.*

Objective: *This study aims to measure the level of cybersecurity awareness among employees of PT XYZ in relation to phishing attacks by conducting simulations using Gophish, and to analyze the results using the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) method.*

Method: *This study employs a descriptive quantitative approach. Data were collected through phishing attack simulations using the Gophish platform, targeting 122 employees across five divisions at PT XYZ. Employee responses were categorized into five indicators: email sent, email opened, link clicked, data submitted, and email reported. The simulation results were analyzed using the TOPSIS method and classified into awareness categories (high, medium, low) using the equal interval method.*

Result: *Out of a total of 122 targets, 115 emails were ignored, none were opened, 2 successfully led users to click on the phishing link, 1 individual submitted data, and 4 individuals reported the email as phishing. Based on the TOPSIS analysis and the average preference score of 0.79, the respondents demonstrated a high level of awareness, with only a few falling into the medium or low awareness categories.*

Conclusion: *The level of cybersecurity awareness among PT XYZ employees falls within the high category, indicating that while there is a basic understanding of phishing threats, continuous training is still necessary to strengthen resilience against cyberattacks.*

Keywords: *Cybersecurity Awareness, Phishing Attacks, Gophish, TOPSIS.*