BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dan pembahasan penelitian yang telah dijelaskan pada bab sebelumnya, dapat dilihat bahwasannya:

1. Implementasi Gophish sebagai salah satu alat untuk membuat serangan *phishing* dalam rangka pengukuran tingkat kesadaran keamanan siber karyawan terhadap serangan *phishing* berhasil dikonfigurasi dan terbukti efektif dijalankan di lingkungan internal perusahaan PT XYZ.
2. Penerapan skenario rekayasa sosial yang digunakan dalam serangan *phishing* pada penelitian ini memiliki tingkatan *entry-level* (pemula). Hal ini disesuaikan dengan ruang lingkup yang diberikan oleh pihak perusahaan.
3. Distribusi serangan *phishing* dilakukan melalui sistem *email* perusahaan yang dilakukan selama tiga hari kerja. Hasil distribusi tersebut berupa respon target dengan rincian 115 *email sent*, 4 *email reported*, 0 *email opened*, 2 *clicked link*, dan 1 *submitted data.*
4. Perhitungan data hasil simulasi serangan *phishing* menggunakan TOPSIS dan metode statistika tambahan dengan total sebanyak 122 data menunjukkan bahwa dengan nilai preferensi tertinggi sebesar 0,93 dan rata-rata nilai preferensi sebesar 0,79.

Berdasarkan uraian di atas dan penelitian yang telah dilakukan dapat dinyatakan bahwa tingkat kesadaran keamanan siber karyawan terhadap serangan *phishing* di lingkungan PT XYZ tergolong ke dalam kategori “Tinggi”.

5.2 Saran

Berdasarkan hasil penelitian implementasi simulasi serangan *phishing* berkarakteristik pemula (*entry-level*) menggunakan Gophish di lingkungan

internal PT XYZ dan analisis hasil simulasi menggunakan TOPSIS, peneliti memberikan beberapa saran sebagai berikut:

1. Peningkatan Kompleksitas Skenario

   Penelitian selanjutnya disarankan untuk menggunakan skenario rekayasa sosial dengan tingkat kompleksitas yang lebih tinggi (*intermediate hingga advanced*) guna mengukur tingkat kewaspadaan karyawan secara lebih mendalam dan realistis terhadap serangan *phishing* yang lebih canggih.

2. Perluasan Sampel dan Durasi

   Untuk memperoleh hasil yang lebih representatif, studi lanjutan disarankan melibatkan jumlah responden yang lebih besar, dengan proporsi minimal 50% dari total karyawan perusahaan, serta memperpanjang durasi distribusi email *phishing* menjadi lebih dari tiga hari kerja.

3. Integrasi Pelatihan Keamanan Siber

   Penelitian mendatang dapat menggabungkan simulasi *phishing* dengan program pelatihan keamanan siber sebelum dan sesudah uji coba, guna mengukur perubahan tingkat *awareness* secara kuantitatif.

4. Penggunaan Metode Analisis Lain

   Disarankan untuk menggabungkan metode analisis lain seperti AHP atau fuzzy TOPSIS agar dapat dibandingkan efektivitasnya dalam mengolah dan menginterpretasikan data kesadaran keamanan siber.