BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil penelitian yang telah dibahas sebelumnya, dapat disimpulkan bahwa:

1. Serangan *phishing* berkedok perubahan tarif transfer bank BRI dilakukan melalui tahapan yang terstruktur berdasarkan model CKC mulai dari pengumpulan informasi (*reconnaissance*) terkait nomor telepon korban oleh pelaku, kemudian pembuatan senjata (*weaponization*) berupa situs *phishing* yang dibuat mirip dengan login BRImo dan pembuatan pesan pemberitahuan palsu. Kemudian pelaku melakukan pengiriman (*delivery*) dengan memanfaatkan aplikasi WhatsApp. Pada tahap eksploitasi (*exploitation*), korban akan secara sadar memasukkan kredensialnya karena dipengaruhi rasa takut. Data yang dimasukkan korban kemudain akan dikirimkan ke server pelaku (C2), sebelum akhirnya pelaku menguras saldo rekening korban (*action on objective*).
2. Faktor psikologis yang paling dominan untuk dieksploitasi berdasarkan prinsip Cialdini adalah faktor otoritas (*authority*) dimana pelaku bersikap seolah-olah sebagai pihak resmi dari bank dengan cara menggunakan foto profil logo dari bank BRI, faktor kelangkaan dan urgensi (*scarcity & urgency*) dimana factor ini terdapat pada pesan yang dikirimkan pelaku yang mengatakan perubahan tarif akan segera diterapkan. Faktor komitmen dan konsistensi (*commitment & consistency*) digambarkan pada korban yang mengikuti instruksi yang diberikan pelaku dari awal.

5.2. Saran

1. Masyarakat, khususnya nasabah perbankan, perlu diberikan edukasi berkelanjutan mengenai pentingnya keamanan digital dan pengenalan teknik-teknik penipuan *phishing* yang terus berkembang dengan modus operandi yang semakin canggih. Disarankan untuk menyelenggarakan kampanye edukasi, webinar, atau pelatihan yang berfokus pada cara mengidentifikasi tanda-tanda *phishing*, melakukan verifikasi authenticity pesan melalui channel resmi bank,

penggunaan tools pemeriksaan link seperti VirusTotal, dan praktik keamanan dasar seperti tidak membagikan kredensial sensitif dalam kondisi apapun.

2. Bank Rakyat Indonesia (BRI) dan platform perbankan digital lainnya perlu meningkatkan sistem keamanan data nasabah mengingat pelaku penipuan adalah pihak pertama yang menghubungi korban itu artinya pelaku penipuan mengetahui bahwa korban adalah nasabah dari bank tertentu dan pelaku memiliki data nasabah milik bank.