BAB V
PENUTUP

5.1 Kesimpulan

Dari penelitian ini penguji dapat menyimpulkan bahwa meskipun serangan *social engineering* di *game online*, khususnya PUBG Mobile dan Mobile Legends, menunjukkan tingkat keberhasilan yang signifikan, upaya perlindungan dapat dilakukan melalui peningkatan kesadaran dan penerapan langkah-langkah keamanan yang lebih baik. Penggunaan fitur keamanan seperti autentikasi dua faktor dan edukasi yang lebih mendalam terhadap pengguna dapat mengurangi potensi risiko serangan. Dengan demikian, penting bagi pengembang dan komunitas *game* untuk bersama-sama meningkatkan literasi keamanan dan menciptakan lingkungan *game* yang lebih aman bagi seluruh *player*.

5.2 Saran

Penguji memberikan beberapa rekomendasi untuk meningkatkan kesadaran dan perlindungan terhadap serangan *social engineering* seperti *pretexting*, *impersonation*, dan *phishing* dalam *game* PUBG Mobile dan Mobile Legends:

1. Membuat Edukasi Keamanan Siber bagi Pengguna
    a. Konten Edukasi:
        1. Pretexting: memberikan pemahaman tentang bagaimana penyerang dapat memanipulasi korban melalui *post*, cerita atau banyak cara lain untuk mendapatkan *player*.
        2. Impersonation: mengajari cara mengenali tanda-tanda peniruan identitas, seperti nama akun yang mirip dengan teman atau rekan tim, ataupun akun-akun store yang memiliki nama sama tetapi berbeda di beberapa bagiannya.
        3. Phishing: memberikan contoh tautan *phishing* di *game*, ataupun di beberapa akun palsu yang menawarkan hadiah eksklusif.
    b. Metode Implementasi:

1. Integrasikan panduan keamanan dalam *game* melalui notifikasi atau video singkat yang muncul di layar loading.
2. Kolaborasi dengan sekolah dan universitas untuk mengadakan seminar atau workshop tentang keamanan siber.
3. Jalankan kampanye edukasi di media sosial dan platform yang sering digunakan oleh para *player*.

2. Fitur Keamanan yang Ditingkatkan di Game
    a. Verifikasi Akun Ganda:

        Wajib menerapkan autentikasi dua faktor (2FA) untuk mengamankan akun *player*.

    b. Deteksi dan Peringatan Otomatis:

        Menggunakan algoritma untuk mendeteksi aktivitas mencurigakan, seperti tautan yang dikirim melalui obrolan atau *player* yang mengirim pesan *pretexting* serta jika ada perangkat baru yang mencoba *login* ke dalam akun.

    c. Notifikasi Bahaya:

        menambahkan peringatan otomatis jika *player* mengklik tautan eksternal yang belum diverifikasi oleh sistem keamanan *game*.

3. Sistem Pelaporan dan Penegakan Aturan
    a. Peningkatan Sistem Pelaporan:

        mempermudah *player* untuk melaporkan akun yang diduga melakukan *pretexting*, *impersonation*, atau *phishing*.

    b. Sertakan opsi pelaporan yang lebih spesifik untuk kategori "*Social Engineering*."
    c. Respons Cepat:

        Pastikan laporan ditindaklanjuti dengan cepat, dengan notifikasi kepada pelapor tentang status investigasi.

4. Kolaborasi dengan Komunitas dan Influencer
    a. Kerjasama dengan Influencer:
    b. Libatkan streamer dan influencer *game* untuk menyampaikan tips keamanan melalui konten mereka.
    c. Event Edukasi dalam Game:
    d. Adakan event khusus yang berfokus pada keamanan siber, seperti turnamen dengan sesi interaktif tentang bagaimana menghindari serangan.

5. Waspada terhadap Praktik Scam dan Serangan Social Engineering Lain

    A. Pengguna perlu meningkatkan kesadaran terhadap berbagai bentuk serangan yang mungkin terjadi, seperti pretexting, impersonation, dan phishing. Hindari memberikan informasi sensitif seperti nama lengkap, nomor telepon, alamat email, dan terutama kata sandi, kepada pihak yang tidak dikenal atau aplikasi yang tidak resmi. Selalu periksa keaslian formulir atau pesan yang meminta data pribadi.

6. Praktik Keamanan dalam Pengisian Data Pribadi

    A. Saat mengisi formulir, survei, atau berpartisipasi dalam giveaway, pastikan data pribadi yang diminta sesuai dengan tujuan yang jelas dan valid. Jangan pernah memasukkan kata sandi atau data login pada formulir yang mencurigakan. Aktifkan fitur keamanan tambahan seperti autentikasi dua faktor (2FA) untuk melindungi akun Anda.

Penguji juga ingin memberikan saran untuk pengembangan penelitian diantaranya :

1. Eksplorasi Metode dan Platform Lain

Penelitian mendatang dapat mengkaji jenis-jenis serangan lain seperti baiting atau quid pro quo, serta mengaplikasikannya pada platform game lainnya untuk memperluas cakupan analisis.

2. Penggunaan Pendekatan yang Lebih Luas

Melibatkan skenario berbasis real-life atau memanfaatkan teknologi seperti simulasi realitas virtual untuk meningkatkan efektivitas penelitian terhadap kesadaran pengguna terhadap social engineering.

3. Etika Penelitian yang Ketat

   Dalam melakukan penelitian yang melibatkan manusia, penting untuk menjaga keamanan data responden. Informasikan kepada responden bahwa data mereka akan digunakan secara anonim dan tidak disalahgunakan. Pastikan mengikuti standar etika penelitian, seperti mendapatkan persetujuan sebelum pengumpulan data.