BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis dan pembahasan yang telah dilakukan mengenai pemanfaatan OSINT untuk identifikasi serangan *phishing* pada media sosial Facebook, maka dapat ditarik beberapa kesimpulan utama sebagai berikut:

1. Efektivitas Metode OSINT dalam Deteksi Dini: Penerapan metode OSINT yang mengintegrasikan berbagai perangkat seperti VirusTotal API, Maltego, terbukti sangat efektif dalam mendeteksi dan menganalisis reputasi tautan mencurigakan secara proaktif. Metode ini mampu mengklasifikasikan ancaman secara cepat melalui analisis reputasi domain, pola URL, dan jejak infrastruktur digital sebelum korban jatuh lebih banyak.
2. Keberhasilan Atribusi Identitas Pelaku: Penelitian ini berhasil membuktikan bahwa pelaku kejahatan siber di media sosial tidak sepenuhnya anonim. Melalui kombinasi teknik *Social Media Intelligence* (SOCMINT) dan penggunaan *API Leak Checker* melalui bot Telegram, identitas asli pemilik akun penyebar *phishing* dapat diungkap secara detail. Investigasi pada lima target akun menunjukkan bahwa data kependudukan sensitif seperti nama lengkap, NIK, alamat domisili, hingga data registrasi kendaraan dapat ditemukan dan divalidasi melalui metode *cross-referencing* data digital.
3. Karakteristik Pola Serangan: Serangan *phishing* di Facebook mayoritas memanfaatkan teknik rekayasa sosial (*social engineering*) dengan iming-iming finansial untuk menjerat korban. Pelaku secara konsisten menggunakan layanan pemendek tautan (*URL shortener*) dan domain murah (seperti .top, .xyz, atau .vip) untuk menyamarkan tujuan asli situs web berbahaya guna menghindari sistem pemblokiran otomatis platform.
4. Keterbatasan dan Validasi Data: Penggunaan data dari *leak database* sangat membantu proses atribusi, namun memiliki tingkat redundansi atau kesamaan nama (*noise*) yang tinggi. Oleh karena itu, data tersebut tidak dapat berdiri sendiri dan mutlak memerlukan validasi manual dengan membandingkan jejak digital di media sosial untuk memastikan akurasi identitas dan menghindari kesalahan identifikasi (*false positive*).

5.2 Saran

Berdasarkan temuan dalam penelitian ini, penulis mengajukan beberapa saran strategis bagi pengembangan ilmu pengetahuan dan keamanan praktis:

1. Bagi Peneliti Selanjutnya

- Otomatisasi Sistem: Disarankan untuk mengembangkan sistem deteksi otomatis menggunakan bahasa pemrograman Python yang mengintegrasikan API OSINT secara *real-time*, sehingga proses pemantauan dan analisis tidak lagi bergantung pada *tools* manual.
- Perluasan Platform: Mengembangkan ruang lingkup penelitian ke platform lain seperti TikTok, Instagram, atau X (Twitter) untuk membandingkan pola penyebaran dan karakteristik pelaku di ekosistem digital yang berbeda.
- Analisis Forensik Lanjutan: Menambahkan aspek analisis forensik digital pada sisi perangkat korban untuk memahami dampak teknis dan jenis *malware* yang mungkin tertanam setelah tautan *phishing* diakses.

2. Bagi Pengguna Media Sosial

- Peningkatan Awareness: Masyarakat harus lebih waspada terhadap tawaran finansial yang tidak masuk akal dan selalu melakukan verifikasi terhadap domain tautan sebelum berinteraksi lebih jauh.
- Proteksi Data Pribadi: Pengguna disarankan untuk membatasi informasi pribadi yang dibagikan secara publik di profil media sosial guna memperkecil peluang atribusi atau penyalahgunaan data oleh pihak tidak bertanggung jawab.

3. Bagi Platform Media Sosial dan Instansi Terkait

- Penguatan Algoritma: Platform media sosial perlu meningkatkan filter keamanan terhadap penggunaan domain berisiko tinggi dan pola *URL shortener* yang sering diasosiasikan dengan *phishing kit*.
- Kolaborasi Keamanan: Diharapkan adanya kolaborasi antara penyedia layanan dan otoritas keamanan siber untuk memanfaatkan hasil investigasi OSINT sebagai basis penegakan hukum terhadap pelaku kejahatan siber.