Nama : Atiqah Shafa Muthmainnah Jaddu

NIM : 20230140197

1. Serangan Rekayasa Sosial terhadap Wartawan (2023)

Pada tahun 2023, Southeast Asia Freedom of Expression Network (SAFEnet) mencatat bahwa serangan rekayasa sosial terhadap wartawan dan aktivis digital meningkat tajam di Indonesia. Dari laporan yang diterima, terdapat 323 kasus yang diduga merupakan bagian dari upaya untuk mengakses informasi atau akun pribadi para wartawan.

Modus operasi yang digunakan meliputi pengiriman tautan phishing, penggunaan akun palsu yang berpura-pura sebagai teman atau rekan kerja, hingga penyusupan ke dalam grup percakapan internal. Tujuan utama dari serangan ini adalah mengakses informasi pribadi, komunikasi internal, atau data sensitif lainnya yang bisa dimanfaatkan untuk intimidasi atau penyebaran disinformasi. Serangan semacam ini menjadi ancaman serius bagi kebebasan pers dan keamanan digital di Indonesia.

2. Modus Penipuan Mengaku Sebagai Staf IT atau Teknis

Modus ini sangat umum ditemukan dalam berbagai laporan kasus rekayasa sosial di Indonesia. Pelaku biasanya berpura-pura menjadi staf teknis atau tim keamanan dari suatu institusi atau perusahaan digital, termasuk bank, penyedia layanan internet, atau aplikasi dompet digital. Mereka menghubungi korban melalui telepon, pesan teks, atau email, mengklaim bahwa ada aktivitas mencurigakan pada akun korban.

Dengan memanfaatkan rasa panik atau ketidaktahuan korban, pelaku kemudian meminta data pribadi seperti username, password, kode OTP (One-Time Password), atau bahkan mengarahkan korban untuk menginstal aplikasi pengendali jarak jauh. Ketika korban terjebak, pelaku bisa langsung mengakses akun digital korban dan melakukan tindakan yang merugikan seperti menguras saldo atau mengakses data sensitif perusahaan. Modus ini sering terjadi saat akhir pekan atau malam hari, waktu di mana pengguna lebih lengah dan layanan dukungan resmi sulit dihubungi.

3. Penipuan Menggunakan Rekayasa Sosial di Sektor Dompet Digital dan Fintech

Laporan riset dari Universitas Gadjah Mada (UGM) bersama GoPay menunjukkan bahwa sektor dompet digital dan fintech menjadi target utama para pelaku rekayasa sosial, terutama sejak pandemi COVID-19 yang mendorong lonjakan transaksi digital. Modus yang digunakan mencakup pendekatan personal melalui media sosial, percakapan pribadi, dan bahkan penyamaran sebagai layanan pelanggan resmi.

Pelaku membangun kepercayaan dengan calon korban terlebih dahulu, lalu memancing korban untuk mengungkapkan informasi penting seperti PIN, kode OTP, atau mentransfer sejumlah uang dengan dalih memenangkan hadiah atau menghindari pemblokiran akun. Karena pelaku sangat meyakinkan dan seringkali memiliki informasi yang tampak valid, banyak korban yang tertipu, terutama mereka yang kurang memahami keamanan digital.