SPEAR PHISHING

PENIPUAN DIGITAL YANG MENGINCAR TARGET SECARA SPESIFIK

Spear phishing adalah serangan siber yang menargetkan seseorang atau organisasi secara spesifik dengan pesan yang terlihat sangat meyakinkan. Berbeda dengan phishing biasa yang dikirim massal ke banyak orang, spear phishing dilakukan dengan riset mendalam tentang korban, seperti nama, jabatan, alamat email, hingga kebiasaan kerja untuk membuat korban percaya bahwa pesan tersebut benar-benar berasal dari pihak yang dikenal, lalu mengelabui agar korban membuka tautan, mengunduh lampiran, atau membocorkan data rahasia Perusahaan.

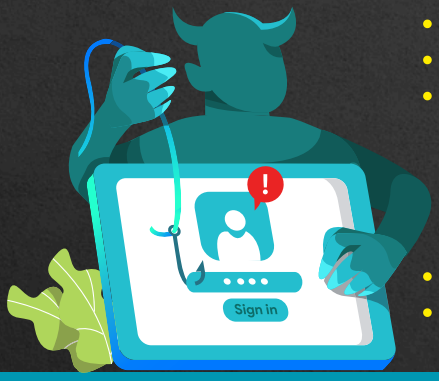
Modus Umum Spear Phishing

1. Penyamaran sebagai Atasan/rekan kerja: seringkali meminta bantuan transfer dana untuk keperluan mendesak atau meminta dikirimkan data sensitif Perusahaan.
2. Penyamaran Tim IT atau bagian Kepegawaian: Mengirimkan form untuk diunduh dan diminta memasukkan data pribadi untuk verifikasi data dengan alasan upgrade sistem
3. Penyamaran Rekanan/Vendor: Mengirimkan invoice (tagihan), lampiran invoice tersebut berisi malwareatau ransomware.
4. Undangan atau Agenda Palsu: Mengirimkan file .zip atau .pdf dengan judul Undangan Rapat yang disisipi virus.

Ciri Pesan Spear Phishing

1. Terdapat permintaan mendesak seperti: segera kirim, rahasia, atau jangan dibagikan ke siapa pun.
2. Meminta data pribadi atau akses sistem, seperti NIK, password, OTP, atau file penting.
3. Alamat pengirim mirip tapi tidak sama, misalnya @go.id diganti menjadi @go-id.com.
4. Mengandung tautan atau lampiran mencurigakan, seperti file ZIP, Excel, atau link login palsu.
5. Bahasa dan gaya penulisan mirip asli/dibuat menyerupai gaya komunikasi orang yang mereka tiru.

Yang Harus Dilakukan Jika Terlanjur Menjadi Korban



- Putus koneksi internet dan ganti password.
- Aktifkan verifikasi dua langkah agar akun tidak disalahgunakan.
- Laporkan ke pihak terkait:
  - Unit Keamanan Siber Instansi (IT Support, CSIRT Instansi)
  - Pihak Bank atau penyedia layanan (jika terjadi transaksi)
  - BSSN (Badan Siber dan Sandi Negara) atau Kepolisian (Cyber Crime Unit) jika membutuhkan eskalasi mitigasi insiden dan mengalami kerugian.
- Lakukan scanning malware.
- Pastikan simpan bukti seperti email atau tangkapan layar sebagai data dukugn dalam proses pelaporan.

DISKOMINFOS PROVINSI BALI
PROGRAM LITERASI KESADARAN KEAMANAN SIBER
Ingin mendapatkan informasi terbaru dan konten literasi keamanan siber ?
Ayo berlangganan KABAR LENTERA (GRATIS !) di https://balikom.info/kabarlentera

SECURITY IS INCOMPLETE WITHOUT U
#JagaRuangSiber
LENTERA SIBER
SAYA NETIZEN CERDAS

DISKOMINFOS.BALIPROV.GO.ID | diskominfosbali | diskominfos_bali | lenterasiber | balikom.info/link/lenterasiber
TLP: CLEAR

Balai Besar Sertifikasi Elektronik
Dokumen ini telah ditandatangani secara elektronik (TTE).
Scan/Klik QR Code untuk informasi TTE.
Upload file pada https://tte.komdigi.go.id/verifyPDF untuk cek keaslian file.
BANGGA BUATAN INDONESIA
BANGGA BERWISATA DI INDONESIA