

APA ITU SOCIAL ENGINEERING?

Social engineering adalah teknik memanipulasi manusia untuk memperoleh informasi atau akses yang diinginkan pelaku.

1. PANGGILAN TELEPON

SELAMAT PAGI... YA BETUL INI DENGAN DIVISI FINANCE...

...BETUL PAK, KAMI ADA AKUN DI BANK ABC

2. INFORMASI DIKUMPULKAN

UNTUK PIC DI BANK APAKAH MASIH DENGAN IBU RINA SEBAGAI HEAD OF FINANCE?

3. MEMINTA INFORMASI

BUKAN PAK, PIC YANG TERDAFTAR DI BANK ADALAH PAK RUDI

... IYA BETUL. DENGAN PAK RUDI PURWA SELAKU DIREKTUR OPERASIONAL

4. MEMINTA LAGI

BAIK BU. DI SINI SAYA MAU MELAKUKAN VERIFIKASI DATA SAJA IBU, AGAR TRANSAKSI PERUSAHAAN TIDAK MENGALAMI KENDALA.

SEMOGA IBU INI BISA MEMBANTU MEMBERIKAN INFORMASI YANG SAYA BUTUH

5. MEMBERIKAN INFORMASI LAGI

OH BAIK PAK JIKA BEGITU. UNTUK EMAIL YANG TERDAFTAR DI BANK ADALAH RUDI@COMPANY.COM

BUKAN PAK. KAMI MEMPUNYAI TOTAL 3 REKENING DI BANK ABC, BUKAN 2 REKENING.

? APA YANG AKAN ANDA LAKUKAN?

Seseorang dari Bank menelepon untuk meminta email Head of Finance untuk keperluan pembaruan data.

- A** Tetap memberikan informasi karena alamat email bukan informasi yang berbahaya.
- B** Memberikan data tersebut karena penelepon terdengar profesional.
- C** Verifikasi melalui kontak resmi dari Bank
- D** Menyambungkan telepon langsung ke bagian Finance tanpa melakukan verifikasi lebih lanjut.

YANG SEHARUSNYA DILAKUKAN

-  **Verifikasi identitas penelpon**
Sebelum memberikan data apapun, verifikasi kembali siapa yang menghubungi Anda.
-  **Lindungi informasi perusahaan**
Informasi sekecil apapun dapat dimanfaatkan untuk serangan yang lebih besar.
-  **Waspada permintaan mendesak**
Pelaku sering menciptakan urgensi fiktif agar kita tidak sempat berpikir dan verifikasi.
-  **Laporkan jika ragu**
Laporkan ke Tim Security jika ada permintaan mencurigakan untuk mencegah penyebaran.

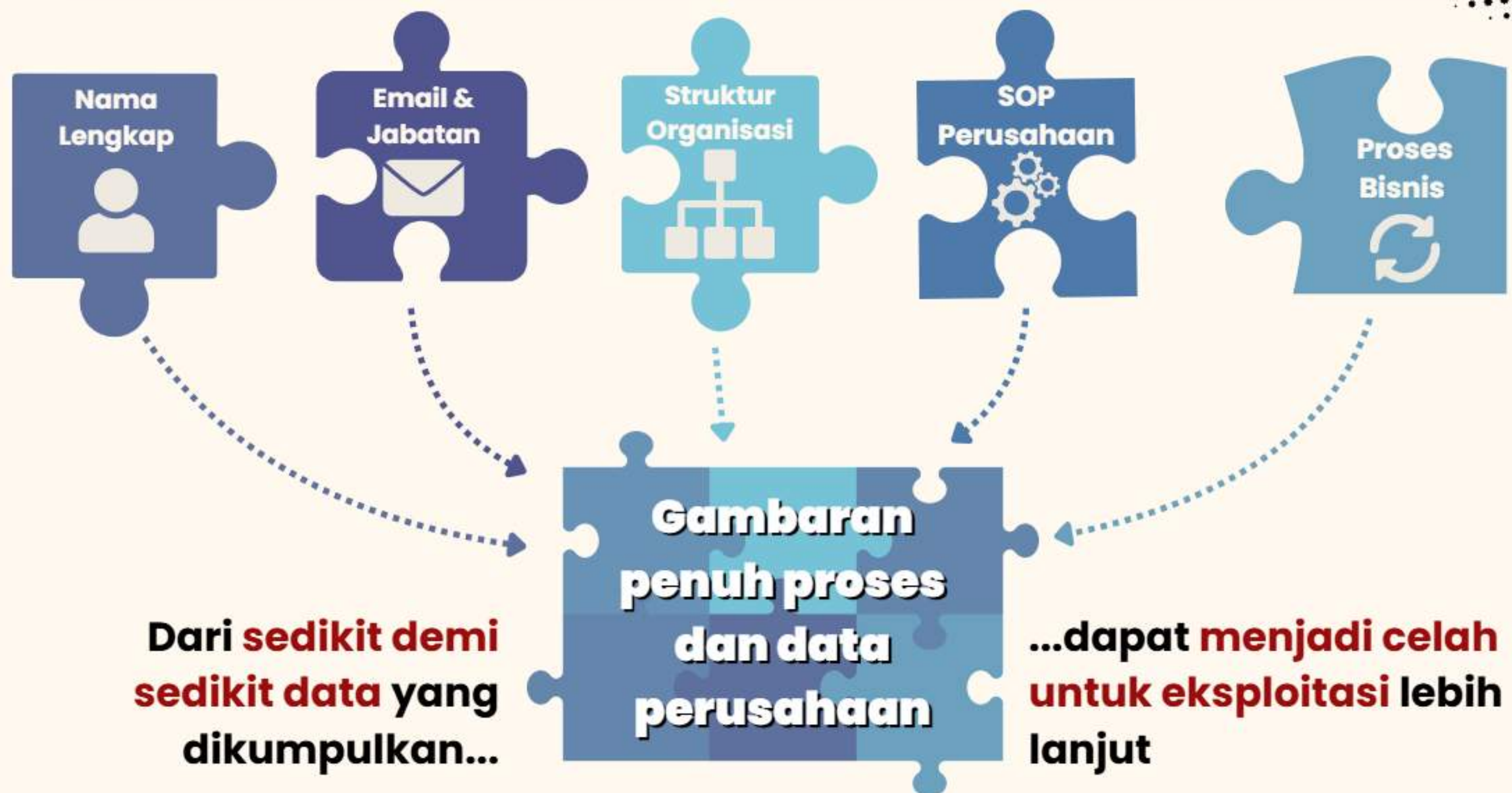


RINGKASAN

Serangan Social Engineering tidak selalu terlihat berbahaya. Pelaku akan mengumpulkan informasi sedikit demi sedikit dari banyak orang. Dalam komik diatas, informasi seperti email dan bank account dapat digunakan kembali untuk serangan berikutnya yang lebih meyakinkan.

SATU INFORMASI MUNGKIN TIDAK BERBAHAYA...

...namun jika dikumpulkan sedikit demi sedikit,
pelaku dapat memahami perusahaan Anda



INGAT

Pelaku jarang meminta password atau data sensitif pada percakapan pertama.

Mengumpulkan informasi

Memahami proses bisnis

Mencari celah perusahaan

Melakukan penipuan

Apa yang dapat Anda lakukan?



01 STOP

Jangan terburu-buru mengambil tindakan. Pelaku social engineering sering menciptakan rasa mendesak agar Anda bertindak tanpa sempat berpikir atau melakukan verifikasi.



02 THINK

Pikirkan apakah permintaan tersebut masuk akal. Apakah sesuai dengan proses kerja yang biasa? Apakah ada hal yang terasa tidak wajar atau berbeda dari biasanya?



03 VERIFY

Sebelum memberikan informasi, membuka lampiran, atau klik tautan, verifikasi terlebih dahulu melalui jalur komunikasi resmi yang sudah Anda kenal sebelumnya.