



SERI EDUKASI KESADARAN KEAMANAN



PHANTOM HACKER SCAM

PUSAT DATA DAN TEKNOLOGI INFORMASI KOMUNIKASI

2025

Materi Edukasi #6



Halo, kami dari Bank TIPUTIPU. Rekening anda diretas. Segera hubungi tim keamanan kami di nomor ini 08xx-xxxx-xxxx

rekening saya kenapa? oke saya hubungi sekarang



Halo, kami dari tim keamanan Bank TIPUTIPU. Kami deteksi akun Anda sedang diakses hacker luar negeri. Untuk melindungi dana Anda, kami bantu pindahkan sementara ke rekening aman atas nama Bapak sendiri. Mohon login ke aplikasi dan ikuti instruksi kami.



Nah kasus diatas merupakan contoh nyata dari Phantom Hacker Scam, yaitu modus penipuan berlapis yang memanfaatkan kepanikan dan kepercayaan korban.

Materi Edukasi #6

PHANTOM HACKER SCAM?



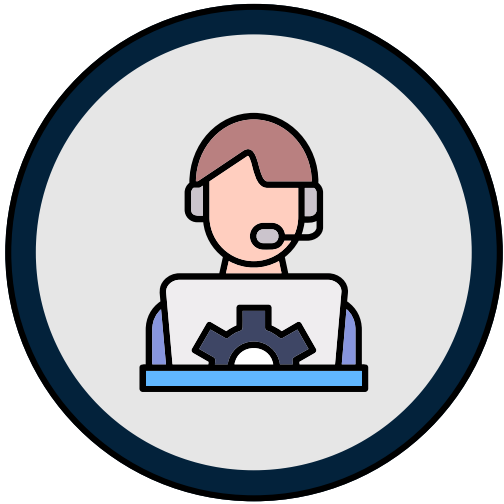
FBI memperingatkan kepada masyarakat terkait “PHANTOM HACKER SCAM”, penipuan dimana pelaku berpura pura sebagai pihak bank dan menipu korban agar mentrasfer uang ke rekening yang dikatakan “aman” untuk menghindari hacker palsu. Penipu menggunakan nomor telepon palsu agar terlihat resmi dan membuat korban panik. FBI menegaskan bank tidak akan pernah meminta nasabah untuk memindahkan uang, sehingga panggilan semaca ini harus dianggap sebagai salah satu penipuan.

PHANTOM HACKER SCAM merupakan modus penipuan lanjutan dari tech support scam. Dimana pelaku berpura-pura sebagai teknisi, pegawai bank, atau pejabat pemerintah untuk meyakinkan korban bahwa akunnya diretas. Dengan dalih melindungi aset, korban dibujuk untuk memindahkan uang mereka ke “rekening aman” milik penipu.

Jadi, istilah “hacker” dalam kasus ini sebenarnya tidak menggambarkan peretas yang sesungguhnya, karena tidak ada serangan nyata yang terjadi. Semua hanyalah social engineering untuk memanipulasi korban. Modus ini paling sering menargetkan seseorang yang sudah dapat dikatakan lanjut usia, lebih mudah panik, takut dan kurang paham teknologi, sehingga pelaku mudah menipu korban.



THE SCAM !



FASE 01. TECH SUPPORT IMPOSTER

- Mengaku sebagai teknisi dukungan (**technical support**) dari perusahaan ternama.
- Meminta korban untuk **menginstall software** tertentu supaya pelaku dapat mengakses komputer dari **jarak jauh**.
- Setelah mendapatkan akses, pelaku dapat melihat **kondisi keuangan korban** dan menyiapkan **target rekening** yang paling bernilai

FASE 02. FINANCIAL INSTITUTION IMPOSTER

- Mengaku sebagai **pegawai lembaga keuangan** atau **bank**.
- Mengatakan bahwa **komputer dan rekening korban telah diretas**.
- Menyarankan korban memindahkan uang ke **rekening “aman”** milik lembaga pemerintah.



FASE 03. GOVERNMENT IMPOSTER

- Berpura pura sebagai **pegawai pemerintah**.
- Pelaku mengirimkan surat atau **dokumen palsu** berkop surat resmi.

Semakin tinggi fasenya, semakin besar otoritas palsu yang digunakan penipu, dan semakin kuat kepercayaan serta rasa takut yang ditanamkan ke korban.

PHANTOM HACKER SCAM SAMA PENIPUAN LAIN APA BEDANYA ? 🤔



MULTI LAYERED SCAM

- Phantom Hacker menggunakan beberapa **peran penipu**: teknisi palsu, pegawai bank dan pegawai pemerintah
- Tiap perang membangun **tingkat kepercayaan baru**, membuat korban yakin.



AWAL MODUS : POP UP / PESAN PALSU

- Penipu memancing korban lewat **pop-up peringatan palsu** di perangkat korban.
- Pop-up muncul setelah korban mengklik tautan mencurigakan



SOCIAL ENGINEERING

- Pelaku meminta korban mengunduh aplikasi remote access supaya pelaku dapat mengedalikan perangkat korban.
- Kemudian pelaku dan mengetahui data finansial korban (rekening, saldo, riwayat transaksi)



PHANTOM HACKER SCAM SAMA PENIPUAN LAIN APA BEDANYA ? 🤔



PERAN BANK PALSU

- Setelah mengetahui rekening korban, pelaku mengaku dari bank korban dan mengatakan akun korban diretas
- Korban diminta memindahkan uang ke “rekening aman”



PEJABAT PEMERINTAH PALSU

- Jika korban ragu, pelaku baru akan muncul dan mengaku sebagai pejabat pemerintahan
- Tujuan: untuk meyakinkan kesan resmi supaya korban merasa harus mengikuti instruksi



Penipuan umum atau lainnya biasanya dilakukan oleh satu pihak dengan satu cerita. Sedangkan Phantom Hacker Scam melibatkan beberapa pelaku dengan narasi bertingkat yang meniru pihak resmi untuk membangun kepercayaan dan menipu korban secara psikologis

TIPS TO PROTECT YOURSELF



JANGAN KLIK Pop-Up, tautan, atau lampiran dari pesan, email, maupun SMS yang tidak dikenali



JANGAN HUBUNGI nomor telepon yang tercantum pada pop-up, pesan atau email yang mencurigakan



JANGAN UNDUH aplikasi atau software apapun atas permintaan orang tidak dikenal



JANGAN BERI AKSES jarak jauh ke komputer atau perangkat yang dimiliki kepada siapapun yang menghubungi tanpa diminta



INGAT pemerintah tidak akan pernah meminta anda untuk mengirimkan uang melalui wire transfer, cryptocurrency, gift atau prepaid card

Kalau ada yang ngaku dari bank dan minta transfer
uang demi “KEAMANAN”

percayalah, itu bukan keamanan, itu kebutuhan berlapis

Seperti biskuit tanggo...
berapa lapis?

Ratusaaaaaannn!!!





“Ingatlah **Kechilafan** **Satu Orang Sahaja** Tjukup Sudah Menjebabkan Keruntuhan Negara”

- **Dr. Roebiono Kertopati**
Bapak Persandian Republik Indonesia



REFERENSI

- <https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/the-phantom-hacker-fbi-phoenix-warns-public-of-new-financial-scam>
- <https://www.tegfcu.com/fraud-security/protect-yourself-from-phantom-hacker-scams/>
- <https://www.ic3.gov/PSA/2023/PSA230929>
- <https://www.cna.id/lifestyle/waspada-scam-share-screen-whatsapp-satu-klik-fatal-walikota-jakarta-pusat-arifin-38886>
- <https://www.americanheritagecu.org/about-us/american-heritage-and-the-community/blog/moneyblog/2025/09/11/ask-the-experts--what-is-the-phantom-hacker-scam>
- <https://www.forbes.com/sites/zakdoffman/2025/09/30/fbi-warning-all-smartphone-users-must-stop-these-calls/>