

WHATSAPP SCAM

WHATSAPP SCAM

WHATSAPP SCAM



WHATSAPP SCAM

WHATSAPP SCAM

WHATSAPP SCAM

7 MODUS TERBARU PENIPUAN LEWAT WHATSAPP



MODUS KURIR



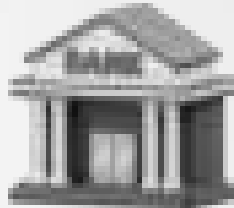
FILE UNDANGAN NIKAH



SURAT TILANG PALSU



CATUT MYTELKOMSEL



PENGUMUMAN BANK



UNDANGAN VCS



KURAS REKENING PAKAI KODE QR

More Info:

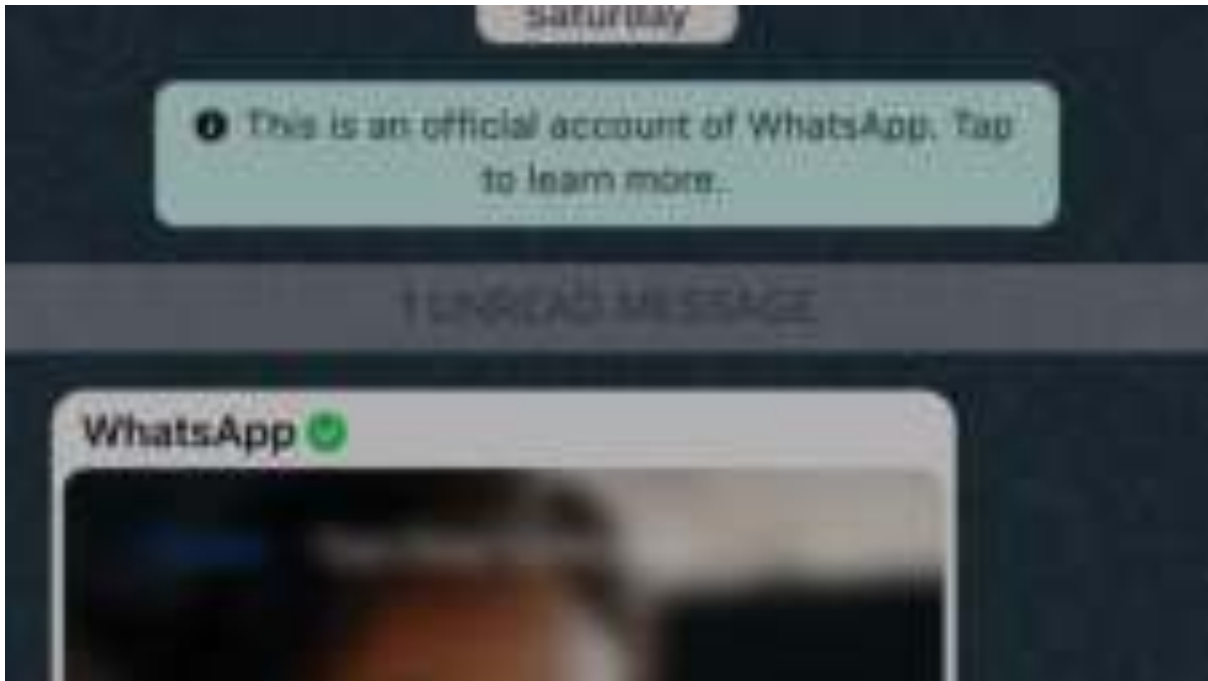


WHATSAPP SCAM

WHATSAPP SCAM

WHATSAPP SCAM

7 Modus Terbaru Penipuan Lewat WhatsApp, Korbannya Banyak Banget!



Aplikasi pesan WhatsApp hampir digunakan untuk berbagai kebutuhan khususnya di Indonesia. Namun, para pengguna aplikasi WhatsApp nampaknya masih perlu berhati-hati lantaran banyak modus penipuan yang memakan korban melalui aplikasi pesan tersebut.

Kebanyakan penipuan lewat WhatsApp memanfaatkan file APK yang dikirim acak ke nomor HP orang lain. Tujuannya agar penerima chat mengklik dan mendownload file kemudian tanpa sadar menginstal aplikasi jahat di HP-nya.

Cara pembobolan yang disebut sebagai phising ini serupa dengan kejahatan mengirim link lewat email. Penipu online berharap agar penerima email atau WhatsApp memberikan akses secara tak sadar sehingga HP atau akun finansial bisa diambil alih atau dibajak.

Berikut 7 jenis modus penipuan online di WhatsApp tahun ini:

Modus Kurir

Penipuan ini dilaporkan akun Instagram yakni mengungkapkan chat Telegram dengan seseorang yang mengaku berasal dari J&T. Penipu mengirimkan lampiran dengan nama file berbentuk apk dengan tulisan LIHAT Foto Paket'.

Mereka yang mengunduh file itu akan kehilangan uang yang disimpan di bank. Berbagai data termasuk keuangan yang bakal diambil oleh para pelaku.

File Undangan Nikah

Penipuan ini sempat jadi banyak perbincangan karena banyaknya pengguna WhatsApp yang mendapatkan. Mereka dikirim file apk oleh orang yang tidak dikenal yakni sebuah undangan pernikahan.

File atau aplikasi dengan judul Surat Undangan Pernikahan Digital berukuran 6,6 mb. Para penipu mengajak korbannya membuka file untuk mengecek kebenaran file di dalamnya.

Surat Tilang Palsu

Sejumlah warganet juga mendapatkan dirinya dikirim surat tilang palsu. Terdapat file apk berjudul 'Surat Tilang-1.0 apk' dalam chat tersebut.

"AWAS! Hati-hati terhadap penipuan menggunakan modus kirim surat tilang lewat WhatsApp seperti ini. Jangan sekali-kali mengklik/download file dgn ekstensi ".apk" dari orang tak dikenal di gadget anda," kicau akun @MurtadhaOne1.

Catut MyTelkomsel

Penipuan di WhatsApp lainnya juga pernah ada yang menggunakan nama MyTelkomsel. Ini merupakan aplikasi milik operator Telkomsel.

Korban akan diminta klik file apk yang dikirimkan. Berikutnya mereka akan diminta memberikan izin akses pada sejumlah aplikasi, termasuk foto, video, SMS, dan akses akun layanan perbankan digital atau fintech.

Pengumuman dari Bank

Penipuan lain adalah membuat pengumuman yang seakan berasal dari bank. Isinya mengenai perubahan tarif transaksi dan transfer yang tidak masuk akal.

Pengguna WhatsApp akan diberikan link untuk mengisi formulir. Link tersebut akan membuat data mereka dicuri para pelaku.

Undangan VCS

Modus lainnya adalah melakukan video call sex (VCS) dari nomor tidak dikenal. Mereka disebut akan memeras para korbannya.

Dihubungi beberapa waktu lalu, Pakar keamanan siber Alfons Tanujaya mengatakan modus ini memanfaatkan ketidaktahuan seseorang soal teknologi dan menjadikannya ancamannya. "Ini pada prinsipnya adalah pemerasan yang memanfaatkan ketidaktahuan atau keamanan seseorang tentang teknologi," kata dia.

"Kalau ragu dan diperas, hubungi teman yang mengerti dan minta bantuannya untuk menghadapi ancaman-ancaman yang tidak kita mengerti, jangan main mengikuti ancaman saja," paparnya.

Kuras rekening pakai kode QR

Metode lainnya yang sering digunakan adalah quishing, yaitu kombinasi dari kode QR dan phishing. Pelaku akan memancing korbannya agar mendapatkan informasi dan detail pribadi mereka.

Saat memindai QR Code, biasanya korban akan dibawa ke situs tertentu. Selain bisa menunjukkan pesan teks biasa, situs tersebut bisa melacak daftar aplikasi hingga alamat peta korban.

Pelaku memanfaatkan kemampuan tersebut untuk mengarahkan calon korbannya ke situs web palsu. Mereka akan membuat orang sulit mendeteksi situs yang akan dikunjungi sebelum membuka web.

Wired menyebut, pelaku quishing akan mengelabui seseorang untuk mengunduh sesuatu ke dalam perangkat. Unduhan tersebut akan membahayakan perangkat milik korban.

Langkah berikutnya, para korban akan diminta memasukkan beberapa kredensial login. Informasi itu akan didapatkan oleh pelaku quishing.

Kejahatan ini semakin masif karena kode QR bisa dibuat dengan mudah dan siapa saja. Seseorang bisa membuatnya bahkan tanpa keahlian khusus.

Cara Terhindar Quishing

Jangan khawatir, ada cara untuk menghindari kejahatan quishing. Utamanya adalah jangan percaya QR code yang dipasang di tempat umum atau diberikan pada orang yang tidak jelas dari mana asalnya.

Anda juga bisa mengenali QR code dengan tujuan kejahatan. Karena biasanya penipu akan meningkatkan rasa urgensi dan kekhawatiran calon korbannya. Misalnya dengan menyertakan pernyataan, "Pindai kode QR ini untuk memverifikasi identitas Anda atau mencegah penghapusan akun Anda".

Terakhir, jangan lupa mengaktifkan autentikasi dua faktor pada tiap akun. Selain itu, jangan lupa untuk keluar dari perangkat yang tidak digunakan lagi.



[Avian Brands](#) © 2024