Penipuan update Whatsapp Palsu: penipuan atau cuma viral?

Tidak lama ini Sebuah peringatan tentang modus penipuan baru yang berkedok pembaruan (update) aplikasi whatsapp beredar luas akhir-akhir ini , namun apakah ini ancaman siber atau hanya konten viral yang di besar-besarkan. Artikel ini akan mengupas berdasarkan analisis pakar dan fakta yang ada.

Beredar video dari sebuah akun tiktok yang memperingatkan masyarakat tentang modus penipuan terbaru. Pelaku diduga mengirimkan notifikasi palsu yang tampak sangat resmi ke ponsel korban. notifikasi itu berisi pesan seperti, "This version of WhatsApp has expired. Please go to the App Store to update", namun mengarahkan pengguna ke situs web atau tautan mencurigakan yang bertujuan mencuri data pribadi.
Pengunggah video menekankan bahwa tampilan “notifikasi ini dibuat sangat mirip dengan aslinya”, sehingga berpotensi mengecoh pengguna awam.

Benarkah Ancaman Nyata?
Menganggapi peringatan ini, pakar keamanan siber, Alfons Tanuwijaya memberikan persepektif kritis yang penting di simak, berikut poin-poinnya yang dilansir dari kompas.com:

1. Minim Bukti, Alfons menilai klaim dari video tersebut tidak disertai bukti pendukung yang memadai, hanya menampilkan tangkapan layar tanpa informasi lebih lanjut tentang situs phishing aktif atau mekanisme pencurian data.
2. Proteksi Sistem Operasi yang Modern, Secara teknis Alfons menjelaskan bahwa perangkat modern memiliki pertahanan yang baik, seperti Iphone akan memblokir instalasi aplikasi dari luar App Store, dan Android (versi 11 ke atas) secara default juga melarang instalasi dari luar Play Store
3. Kemungkinan Bukan kasus nyata, berdasarkan analisisnya, Alfons menyimpulkan bahwa kemungkinan besar ini bukan kejadian penipuan yang nyata

Tips Menghadapi Potensi Ancaman Serupa
pertama, Update dari sumber yang resmi dengan selalu lakukan pembaruan aplikasi hanya melalui toko aplikasi resmi seperti Google Play Store (Android) atau App Store (iOS). Jangan pernah mengikuti tautan untuk mengupdate dari pesan, email, atau situs web yang tidak dikenal. Praktik ini termasuk dalam Panduan Keamanan Digital untuk Masyarakat dari Kementerian Komunikasi dan Informatika (Kominfo) Republik Indonesia.

Kedua, verifikasi informasi viral, sebelum percaya atau menyebarkan informasi keamanan yang viral, periksa kebenarannya terlebih dahulu. Anda dapat mengecek di cekfakta.com yang dijalankan oleh Masyarakat Anti Fitnah Indonesia (Mafindo), atau memanfaatkan layanan Turnbackhoax.id. Situs-situs ini secara aktif melacak dan memverifikasi berbagai klaim yang beredar di internet.

Ketiga, aktifkan lapisan keamanan tambahan, guna untuk perlindungan extra pada akun yang dijalankan oleh Masyarakat Anti Fitnah Indonesia (Mafindo), atau memanfaatkan layanan Turnbackhoax.id. Situs-situs ini secara aktif melacak dan memverifikasi berbagai klaim yang beredar di internet.

Keempat, Waspada terhadap social engineering, modus ini mengandalkan rekayasa sosial (social engineering)—yakni memanfaatkan rasa urgensi ("aplikasi kedaluwarsa") dan kepercayaan terhadap merek (logo WhatsApp) untuk memicu korban bertindak ceroboh.

Sumber Referensi:

1. Kompas.com. (2025, 29 Oktober). Beredar Peringatan Penipuan Modus Update WhatsApp, Pakar Siber Beberkan Faktanya. Diakses dari https://www.kompas.com/tren/read/2025/10/29/143000865/beredar-peringatan-penipuan-modus-update-whatsapp-pakar-siber-beberkan
2. Kementerian Komunikasi dan Informatika (Kominfo) Republik Indonesia. Panduan Keamanan Digital untuk Masyarakat.
3. Masyarakat Anti Fitnah Indonesia (Mafindo). CekFakta. Diakses dari https://cekfakta.com
4. WhatsApp. Tentang Verifikasi Dua Langkah. Diakses dari Pusat Bantuan WhatsApp.
5. Lembaga Sertifikasi Profesi Keamanan Siber Indonesia (LSP-CSI). Materi Edukasi Keamanan Siber.