

OJK Mengingatkan Masyarakat Waspada Penipuan M-banking.

Heriyoko - [JAKARTA.INDONESIASATU.ID](https://www.jakarta.indonesiasatu.id)

Mar 11, 2025 - 23:22



Kantor Otoritas Jasa Keuangan (OJK) Wisma Mulia Jl. Gatot Subroto, Jakarta Selatan

JAKARTA, Penggunaan digital banking sudah menjadi bagian yang tak dapat dipisahkan dalam kehidupan sehari-hari. Namun, telah menjadi sasaran empuk bagi para pelaku kejahatan untuk mencuri data sensitif, mengakses akun nasabah, atau melakukan transaksi ilegal.

Kejahatan siber melalui digital banking akhir - akhir ini semakin marak. Tidak sedikit korban yang tabungannya terkuras habis akibat ulah pelaku kriminal.

Terkait hal itu, Otoritas Jasa Keuangan (OJK) mengingatkan masyarakat untuk waspada terhadap penipuan m-banking atau mobile banking

Penipuan ini dilakukan dengan berbagai modus, seperti pencurian data pribadi, phishing, dan impersonation.

Modus penipuan m-banking

Pelaku mengirimkan SMS seolah-olah dari bank

SMS berisi informasi tentang transaksi mencurigakan, hadiah undian, atau promo menarik

SMS disertai tautan berbahaya yang dapat mencuri data pribadi dan menguras isi rekening

Pelaku berpura-pura menjadi lembaga resmi seperti perusahaan investasi agar bisa mencuri uang korbannya

Otoritas Jasa Keuangan melalui laman resminya dikutip Selasa (11/3/2025) memberikan tips untuk terhindar dari kejahatan ini :

1. Tidak memberitahukan kode akses/ nomor pribadi Personal Identification Number (PIN) kepada orang lain
2. Tidak mencatat dan menyimpan kode akses/ nomor pribadi SMS banking di tempat yang mudah diketahui orang lain
3. Periksa transaksi secara teliti sebelum melakukan konfirmasi atas transaksi tersebut untuk dijalankan
4. Setiap kali melakukan transaksi, tunggulah beberapa saat hingga menerima respon balik atas transaksi tersebut
5. Untuk setiap transaksi, nasabah akan menerima pesan notifikasi atas transaksi berupa SMS atau email yang akan tersimpan di dalam inbox. Periksa secara teliti isi notifikasi tersebut dan segera kontak ke bank apabila ada transaksi yang mencurigakan
6. Jika merasa diketahui oleh orang lain, segera lakukan penggantian PIN
7. Bilamana SIM Card GSM hilang/ dicuri/ dipindahtangankan kepada pihak lain, segera beritahukan ke cabang bank terdekat atau segera melaporkannya ke call center bank tersebut;
8. Hati-hati dengan aplikasi di internet yang merupakan spam atau malware yang mungkin dapat mencuri data-data pribadi dan menyalahgunakannya di kemudian hari
9. Tidak melakukan transaksi internet di tempat umum seperti warnet, WIFI gratis,

karena data-data kita berpotensi dicuri oleh pihak lain dalam jaringan yang sama

10. Tidak lupa melakukan proses logout setelah selesai melakukan transaksi di internet banking

11. Jika berganti ponsel, pastikan bahwa semua data-data sudah terhapus untuk menghindari penyalahgunaan oleh pihak lain yang menggunakan ponsel tersebut (hy)