WASPADA QUISHING

ANCAMAN DI BALIK KODE QR

Quishing **adalah gabungan dari kata "QR" dan "phishing". Penipuan ini menggunakan kode QR palsu untuk menjebak korban ke situs web berbahaya. Biasanya, kode QR ini ditemukan di tempat umum seperti poster, brosur, atau bahkan ditempel langsung di ATM.**

QR Code palsu disebar di tempat umum seperti ATM, jalan, papan reklame, ataupun melalui SMS, WhatsApp, dll.

Korban diminta untuk memasukkan informasi pribadi sensitif seperti data login, PIN ATM, nomor kartu kredit, dll.

Penipu membuat QR Code palsu yang menyerupai QR Code asli dari perusahaan atau lembaga terpercaya.

Ketika korban memindai QR Code palsu, mereka akan diarahkan ke situs web palsu yang dibuat semirip mungkin dengan situs web asli.

TIPS MELINDUNGI DIRI DARI QUISHING

- **Jangan sembarangan memindai QR Code yang ditemukan di tempat umum, terutama jika QR Code tersebut tidak memiliki sumber yang jelas.**
- **Jangan pernah memasukkan informasi pribadi seperti data login, pin ATM, atau nomor kartu kredit di situs web yang tidak Anda kenal atau tidak percayai.**
- **Perhatikan dengan seksama URL situs web. Pastikan URL situs web sama persis dengan situs web asli dan memiliki HTTPS di awal alamatnya.**
- **Jika Anda menemukan QR Code yang mencurigakan, laporkan kepada pihak berwenang terkait untuk ditindaklanjuti.**

DISKOMINFOS PROVINSI BALI
PROGRAM LITERASI KESADARAN KEAMANAN SIBER
Ingin mendapatkan informasi terbaru dan konten literasi keamanan siber ?
Ayo berlangganan KABAR LENTERA (GRATIS !) di https://balikom.info/kabarlentera

SECURITY IS INCOMPLETE WITHOUT U #JagaRuangSiber
LENTERA SIBER
SAYA NETIZEN CERDAS

DISKOMINFOS.BALIPROV.GO.ID | diskominfosbali | diskominfos_bali | lenterasiber | balikom.info/link/lenterasiber
TLP: CLEAR

Balai Besar Sertifikasi Elektronik
Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh BSrE

BANGGA BUATAN INDONESIA
BANGGA BERWISATA DI INDONESIA