Cara Mengetahui Apakah QR Code Aman Sebelum Membukanya (Panduan Quishing)

Quishing adalah phishing menggunakan QR code. Pelajari tanda bahaya sebelum memindai dan apa yang harus diperiksa sebelum mengetuk Buka.

Penulis: Lubor Šimůnek · Diterbitkan: August 23, 2026 · Keamanan

Versi online: https://appstoryo.com/id/blog/qr-code-safe-quishing-guide



Apa itu Quishing?

Quishing adalah phishing melalui QR code. Penyerang membuat kode yang, setelah dipindai, mengarahkan Anda ke situs berbahaya yang dirancang untuk mencuri kredensial, menginstal malware, atau menampilkan halaman pembayaran palsu. Istilah ini menggabungkan 'QR' dan 'phishing', dan ancaman ini berkembang pesat karena orang cenderung mempercayai QR code tanpa berpikir panjang.

Mengapa QR Code Memiliki Risiko Khusus

Dengan tautan biasa, Anda bisa mengarahkan kursor ke atasnya untuk melihat URL sebelum mengklik. Dengan QR code, Anda tidak dapat melihat tujuan sampai pemindai mendekodekannya — dan banyak aplikasi kamera langsung membuka browser tanpa menampilkan alamat. Momen singkat itu sudah cukup bagi situs berbahaya untuk mulai melacak perangkat Anda.

QR code juga sepenuhnya melewati filter spam: filter mencari teks mencurigakan atau URL berbahaya yang dikenal, tetapi gambar QR code tampak sepenuhnya tidak berbahaya. Itulah mengapa email phishing semakin menggantikan tautan lama mereka dengan QR code,

terutama dalam serangan yang menargetkan karyawan perusahaan.

Dalam kehidupan nyata, quishing muncul sebagai stiker yang ditempel di atas kode sah pada mesin parkir, menu restoran palsu, pemberitahuan pengiriman paket penipuan di kotak surat, dan stasiun pengisian daya publik palsu yang meminta 'pindai untuk membayar'.

Tanda Bahaya SEBELUM Memindai

- **Stiker di atas kode asli.** Stiker QR yang ditempelkan di atas QR code lain adalah penggantian klasik. Angkat sudutnya dengan hati-hati — jika terkelupas, jangan pindai.
- **Bahasa mendesak pada selebaran asing.** 'Pindai sekarang untuk klaim hadiah Anda' atau 'Paket Anda ditahan — pindai untuk menjadwalkan ulang' adalah taktik tekanan psikologis.
- **Email atau surat tidak diminta.** Komunikasi tak terduga dari bank, perusahaan pengiriman, atau lembaga pemerintah yang menggunakan QR code sebagai ajakan bertindak utama adalah tanda peringatan kuat.

Apa yang Diperiksa SETELAH Memindai dan SEBELUM Membuka

- **Apakah domain sesuai ekspektasi?** Jika Anda memindai QR di bank, URL harus berada di domain resmi.
- **Apakah menggunakan pemendek URL?** Layanan seperti bit.ly atau tinyurl.com menyembunyikan tujuan sebenarnya. Gunakan layanan URL expander untuk mengungkap alamat asli sebelum berkunjung.
- **Domain salah eja atau mirip.** Perhatikan paypa1.com (angka 1 menggantikan huruf L) atau g00gle.com (angka 0 menggantikan huruf O). Baca setiap karakter dengan cermat.
- **Subdomain mencurigakan.** login.secure.amazon-pengiriman-id.com tampak sah, tetapi domain sebenarnya adalah amazon-pengiriman-id.com, bukan amazon.com.

Bagaimana QR Code Reader Without Ads Membantu

QR Code Reader Without Ads menampilkan pratinjau URL lengkap sebelum membuka apa pun, memberi Anda waktu untuk memeriksa tautan sebelum bertindak. Jika alamatnya terlihat mencurigakan, cukup jangan ketuk 'Buka'. Aplikasi ini menyimpan riwayat pemindaian secara lokal di perangkat Anda, tidak mengumpulkan data, dan tidak menampilkan iklan. Tersedia di App Store dan Google Play dengan mencari 'QR Code Reader Without Ads'.

Unduh QR Code Reader Without Ads gratis untuk iOS atau Android — tanpa iklan, tanpa pelacakan, dan berfungsi sepenuhnya offline.

Kutip sebagai: Lubor Šimůnek (2026). *Cara Mengetahui Apakah QR Code Aman Sebelum Membukanya (Panduan Quishing)*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/id/blog/qr-code-safe-quishing-guide

© 2026 lapnito.cz s.r.o.