What is Quishing (QR Phishing)?

QR codes are quick and convenient, but they can also be hijacked by attackers. Fake codes often lead to malicious websites designed to steal data, install malware, or trick you into entering login credentials. Because scanning feels safe and effortless, many users don't stop to double-check.

How It Works

Planted in the Real World

Attackers can print fake QR codes and place them on posters, flyers, or even over legitimate codes on restaurant menus or delivery labels. Scanning takes you somewhere unexpected.

Tip: *Look closely for signs of tampering before scanning physical QR codes.*

Hidden in Digital Messages

Phishing emails or invoices may contain QR codes that appear to link to a payment site, login portal, or tracking page. Once scanned, they redirect to malicious websites.

Tip: *Preview the link before opening it, and avoid logging in to sensitive accounts through QR scans unless you fully trust the source.*

The Illusion of Safety

Scanning feels casual, like snapping a picture. Attackers exploit this false sense of security to get people to act without caution.

Tip: *Whenever possible, use official apps or type web addresses directly instead of relying on QR scans.*