Quishing is the Scam Artists New Friend

July 29, 2025 - Quishing is the sneaky new scam you didnâ€™t see coming-until it hit your phone. The term blends, "QR code" with "phishing," referring to fraud where attackers trick people into scanning bogus QR codes that lead to malicious websites or malware. Once scanned, victims may unknowingly give up passwords, payment details, or other personal data-and those details fuel fraud and identity theft.

According to Egressâ€™s recent Phishing Threat Trends report, QR code phishing has skyrocketed: QR codes were involved in just 0.8â€¯% of phishing attacks in 2021 but jumped to 12.4â€¯% in 2023 and remained at 10.8â€¯% in early 2024. Thatâ€™s more than a tenfold rise since 2021.

Keepnet Labs tracked thousands of actual quishing incidents in mid 2023 - nearly 9,000 cases between June and August alone-marking a major shift in criminal tactics. Another source noted that around 26â€¯% of malicious links in phishing attacks are now hiding behind QR codes, making traditional filters less effective.

Real world harm is piling up. In the U.K., drivers fell victim to quishing via fake parking-payment QR codes. Action Fraud received more than 1,386 reports in 2024, more than double the prior year; in the first quarter of 2025 they logged 502 reports. One woman in the UK alone suffered Â£13,000 in fraud and debt when scammers duplicated legitimate parking codes. In Singapore, victims lost over $445,000 in total, including one person who was drained of about $20,000 after scanning a malicious QR code at a bubble tea shop and installing malware.

Quishing is dangerous for your money-and your identity. Scammers may harvest login credentials, Social Security numbers, or financial data. That info can be used to open bank accounts in your name, file fake tax returns, seek medical services under your identity, or ruin your credit. While thereâ€™s no single public stat tying identity theft directly to quishing, the rise of phishing generally correlates with identity-theft losses-and there are millions of such victims annually.

Experts expect quishing to keep growing as QR codes spread-from payments at parking lots and EV chargers to delivery stickers and restaurant menus. Physical placement of fake codes over real ones makes detection even harder. In corporate environments, Egress also found that 77â€¯% of quishing payloads impersonate well known services like Microsoft or DocuSign to trick users into trusting the code. In simulated phishing campaigns at real organizations, quishing proved just as effective as traditional clickable links, but much harder to detect or block.
So what can you do to stay safe?

Never scan QR codes on unexpected flyers, stickers, or parking meters-especially if they appear hastily posted. If possible, use the official app or website instead. Always check the previewed URL your phone shows after scanning-misspellings, strange domains, or no "https" are red flags. Avoid scanning QR codes in unsolicited emails or texts urging urgent action. Instead, close the message and navigate directly to the companyâ€™s verified site or call them.

Use scanner apps that preview and check link safety before loading. Keep your device updated with the latest system patches. Enable multi factor authentication (MFA) on email, banking, and other critical accounts-so stolen credentials alone wonâ€™t let attackers in.

In short: quishing is a low effort yet highly effective scam for criminals and a growing path to fraud and identity theft for the rest of us. Be cautious, donâ€™t scan blindly, verify what youâ€™re scanning-and keep your personal data safe.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS