Over 10% of QR Codes Are Scamsâ€”Hereâ€™s How to Stay Safe

March 13, 2025 - QR codes are everywhereâ€”on restaurant tables, parking meters, online orders, and even surprise packages that arrive at your doorstep. But experts warn that at least 10% of these codes are fraudulent, part of an alarming wave of scams that could drain your bank account before you even realize what happened.

The problem has exploded since 2022, with scammers using QR codes to steal an estimated $75 billion annually. Many of these schemes are driven by international cybercriminals, including state-sponsored hackers from China, who are now targeting financial data stored on smartphones.

Hereâ€™s how it works: You scan a fake QR code thinking youâ€™re paying for a meal or returning an online order. Instead, th code redirects you to a fraudulent website that looks legitimate but is designed to capture your financial details. In some cases, these codes install malware that locks your phone, giving thieves access to everything from bank accounts to private emails.

Unlike credit card fraud, where banks can often reverse unauthorized transactions, QR code scams can be much harder to recover fromâ€”especially if thieves access your debit card or digital payment accounts.

Scammers are getting creative in where they place these codes. Some common places include:

- Restaurant tabletops: Fake QR codes are placed over legitimate payment codes.
- Parking meters and kiosks: You think youâ€™re paying for parking, but youâ€™re actually sending money to a scamme
- Bulletin boards and drive-thru windows: Fraudsters stick fake QR codes over legitimate ones at businesses.
- Unsolicited packages: You receive a package you never ordered, often with a note instructing you to scan a QR code to find out who sent it.

This last scheme, known as a â€œbrushing scam,â€• is growing rapidly. Consumers report receiving lightweight items like ping-pong balls, face masks, or even baby burp clothsâ€”along with a QR code that leads to phishing sites or malware. Fraudsters use this trick to create fake product reviews under the victimâ€™s name or to gain access to personal data.

Authorities in several states, along with the U.S. Postal Inspection Service, have flagged an uptick in these scams. Some fraudsters use QR codes simply to flood your phone with spam, while others aim for full financial takeover.

While QR codes are a convenient way to access information and make payments, here are some simple steps to keep yourself safe:

- Avoid scanning QR codes from unknown sources. If a QR code is on a public sign or an unsolicited package, assume it could be fraudulent.
- Manually enter web addresses. If a QR code directs you to a website, type the URL yourself rather than scanning.
- Check for tampering. If a QR code looks like it has been placed over another one, donâ€™t scan it.
- Use your phoneâ€™s security features. Keep your phoneâ€™s operating system updated and enable security settings that flag suspicious links.
- Report suspicious activity. If you receive a questionable QR code, report it to the Federal Trade Commission, the Better Business Bureau, or the retailer it claims to be from.

- Monitor your financial accounts. Regularly check bank and credit card statements for any unauthorized transactions.

With digital scams evolving rapidly, staying informed is the best defense. A little skepticism can go a long way in keeping your personal and financial information safe from fraudsters. So next time you see a QR codeâ€”pause, think, and ask yourself: Is this really worth the risk?
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