

Don't Scan That QR Code! How to Spot Today's New Scams

Key Point: A QR code is simply a shortcut that opens a website, app, payment page, menu, coupon, or contact card on your phone. Most QR codes are safe, but scammers can use them to hide fake websites that steal passwords, payments, or personal information.

Why QR-Code Scams Work

Scammers like QR codes because the web address is hidden until after you scan. A code may lead to a fake bank login, fake Microsoft sign-in page, package delivery scam, parking payment scam, utility payment demand, or password reset page. This type of scam is often called “**quishing**”, or QR-code phishing.

Before You Scan, Ask:

- Do I know who posted this code?
- Was I expecting it?
- Does it look professionally attached, or could it be a sticker placed over another code?
- Is someone rushing me to scan, pay, or sign in?
- Would it be safer to type the company's web address myself?

Warning Signs

- A QR code appears in an unexpected email or text message.
- A sticker looks homemade, crooked, or placed over another code.
- A bill, delivery notice, or parking meter pushes you to scan immediately.
- The page asks for a password, payment, or personal information before you can verify it is real.

Safest Choices

- Type the company's web address into your browser instead of scanning.
- Use the company's official app.
- Call the phone number printed on your bill or card, not one shown after scanning.
- If unsure, ask someone you trust before continuing.

Remember: A QR code is not proof that something is legitimate. Treat it the same way you would treat a suspicious email link: **Stop. Read. Decide.**

Quick Quiz: Which is safer: scanning a QR code from an unexpected email, or typing the company's web address yourself? **Answer:** Type the address yourself.