

QR code scams

Easy · 2 min · Free

A QR code is just a link you can't read. Scammers stick fake ones on parking meters and send them in texts and emails. Before you open one, read the web address your camera shows, and pay parking through the city's real app or the meter itself.

YOU'LL NEED

- ☐ Your phone's camera
- ☐ The real app or website for whatever you're paying, found yourself

WHAT TO KNOW

- 1 Know where the fake ones show up.** There are reports of scammers covering QR codes on parking meters with their own, and of QR codes sent by text or email with a made-up reason to scan.
- 2 Look before you open.** Most phone cameras show the web address before you tap it. If you see a QR code in an unexpected place, inspect the address first.
- 3 Check the spelling.** If it looks like an address you know, make sure it isn't faked with a misspelling or one switched letter.
- 4 Skip codes you weren't expecting.** Don't scan a QR code in an email or text you weren't expecting, especially one that says to act now.
- 5 Pay parking another way when you can.** Use the coin or card slot on the meter, or type the city's parking app name into your app store yourself. On a meter, look at the sticker: a code stuck on top of another sticker is a reason to walk away.
- 6 Keep your phone updated.** Updating your phone's software helps protect it, and strong passwords with two-step sign-in protect your accounts.

Watch out A fake code can take you to a look-alike site that asks for your card, or install malware that steals your information. If a page asks you to log in or pay right after a scan, stop and go to the real site yourself. Real companies won't text or email you a link to update your payment information.

DAD NOTE *Treat a QR code like a link from a stranger. Half a second to read the address beats a month of fighting a charge.*

Full lesson: aptkeys.com/tools/spotting-scams/qr-code-scams/

Checked October 3, 2026. Sources: Federal Trade Commission.