CyberGuardLab

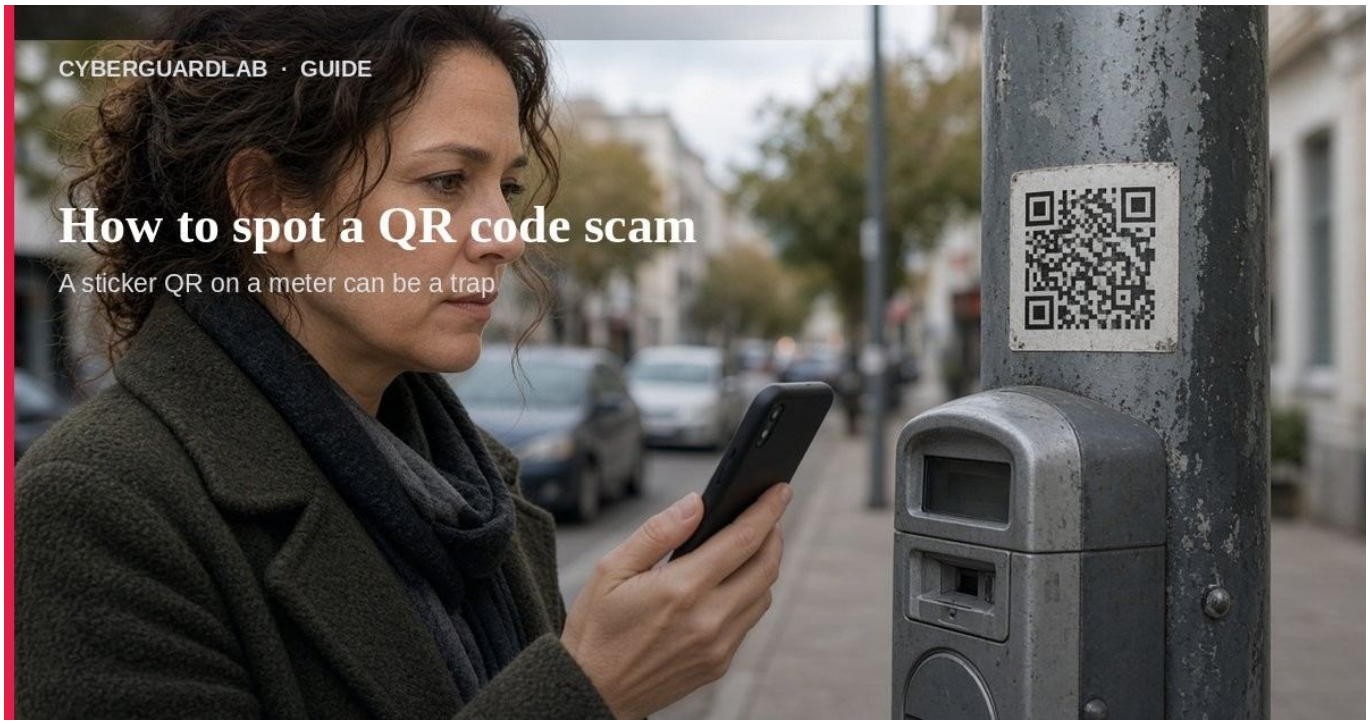
Household antivirus, explained

cyberguardlab.com

# How to spot a QR code scam

https://cyberguardlab.com/blog/qr-code-scam

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.




A QR code scam (sometimes called "quishing") is when a code sends your phone to a fake site or harmful link so someone can steal money or personal information. Per FTC consumer alerts, scammers stick their own codes over real parking-meter codes, and they also send unexpected QR codes by text or email with urgent stories. This guide is about QR codes you scan in the real world or in a message, not general email phishing, fake delivery texts, or spam texts (those scripts sometimes end with a QR, but the primary keyword here is the code itself). You do not need to buy antivirus to refuse a sketchy scan.

## 1. How QR scams usually work

From FTC QR-code alerts:

**Paid link**

* Sticker-over parking meters - People report scammers covering a legit pay-to-park QR with their own sticker. The fake code opens a lookalike payment site.
* Unexpected text or email QR - The story creates urgency: package problem, account issue, "suspicious activity," password change.
* Spoofed login or payment page - After you scan, the page looks real. If you type a password or card number, the scammer gets it.
* Malware risk - FTC notes a bad QR can also try to install malware that steals information.
* Rush is the tell - They want you to open the URL without reading the preview.

## 2. Check before you scan (or before you open the link)

* Look at the physical code - Raised edges, crooked placement, different paper, or a sticker taped over another code are red flags. Prefer the official app or a card reader when something looks off.
* Read the URL preview - Many phone cameras show the link before opening. Look for misspellings, switched letters, odd domains, or shortened links you cannot verify.
* Skip unexpected message QRs - FTC: don't scan a QR in an email or text you weren't expecting, especially if it urges you to act immediately. Contact the company with a number or site you already trust.
* Type the site yourself when unsure - For banks, carriers, or retailers, open the real app or type the known URL instead of trusting the code.
* Keep the phone updated - Update the OS and apps so malicious links are harder to exploit.

## 3. What to do in the first 15 minutes if you already scanned

* Stop interacting - Do not message "support" on the page you reached.
* Change passwords - If you entered a username or password, change it everywhere you reused that password.
* Turn on MFA - Add multifactor authentication on email, banking, and the account involved (see CISA MFA guidance). See also turn on 2FA.

* Review transactions - Check bank and card statements for charges you did not make; follow credit card fraud first-hour if needed.
* Report - File at ReportFraud.ftc.gov.
* Optional device check - Only if you installed an app or saw strange behavior: run Windows Security / Microsoft Defender on a PC, or review phone apps. Buying a suite is not required first - see Is Microsoft Defender enough?.

## 4. Safer QR habits (without buying software)

* Treat parking and public stickers with extra care; inspect before you scan.
* Prefer official apps for parking, restaurants, and tickets when available.
* Never enter a password or card on a page you reached only through an unverified code.
* Use strong unique passwords and MFA on money and email accounts.
* Teach kids and grandparents the same "preview the URL" pause.

## FAQ

### How do I spot a QR code scam?

A code that looks stickied over another, arrives in an unexpected message, or opens a misspelled / rushed login or payment page is a classic QR scam pattern per FTC alerts.

### Is every QR code dangerous?

No. Menus, tickets, and boarding passes are common and often fine. The risk is unexpected or tampered codes and the sites they open.

### What if I already entered my card?

Call the card issuer, watch for unauthorized charges, and report at ReportFraud.ftc.gov.

### Do I need antivirus to handle a QR scam?

No. Refuse the login/payment, change passwords, enable MFA, and report. Defender or good habits are enough unless you also installed malware.

### How is this different from phishing email?

Same goal (steal credentials or money), different delivery: the harmful link is inside a scannable code instead of a clickable email URL.

## If you still want a paid suite

Avoiding a bad QR scan does not require paid antivirus. Microsoft Defender is a valid buy-nothing choice for many Windows households. What actually helps is previewing URLs, refusing unexpected codes, and MFA. If the household later wants multi-device paid protection, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

## Sources

* See a QR code parked somewhere? Don't scan it...yet! (FTC, Sep 2026)
* Scammers hide harmful links in QR codes to steal your information (FTC)
* How To Avoid a Scam (FTC)
* ReportFraud.ftc.gov (FTC)
* Turn On MFA (CISA)
* Recognize and Report Phishing (CISA)
* Windows security overview (Microsoft)

## Also read

* How to spot a phishing email
* How to spot a fake delivery text scam
* How to recognize and report spam text messages

* Credit card fraud: first hour
* Turn on 2FA for Gmail, Apple, and bank