THREATS LIBRARY

JULITH GmbH
Awareness-as-a-Service

Quishing — when the QR code lies

QR codes bypass classic email filters and link previews. Quishing attacks exploit this deliberately — in letters, stickers on parking meters, fake menus.

min read: 6 min **Updated:** 14 March 2026 **Risk:** High risk
Source: awareness-as-a-service.com/en/resources/threats/quishing

What is quishing?

Quishing (QR code + phishing) is the use of manipulated QR codes to lead victims to fraudulent websites. The term is relatively new, but the phenomenon has grown considerably since 2023 — in parallel with the general spread of QR codes in everyday life.

The insidious aspect of quishing is how two weaknesses combine: email gateways cannot analyse the content of an image as a link; users cannot see where a QR code leads before scanning it. Both weaknesses are deliberately exploited.

Attack vectors are varied: QR codes in emails ("please verify your account"), physical stickers on public charging points or parking meters, and printed materials left in waiting rooms, at conferences, or in office kitchens.

At a glance

01
Invisible to email filters
QR codes are images. No link scanner in a gateway can see where they point — the attack passes the perimeter uninspected.

02
Physical attacks are documented
Stickers on parking meters, EV charging stations, and restaurant menus are real, documented attack vectors — not theoretical.

03
Scanned on a personal phone
When someone scans a QR code with their personal device, they bypass MDM, VPN, and other corporate controls entirely.

How to recognise quishing

! **QR code in a letter or notice**
Authorities, banks, and utilities rarely communicate via QR codes in letters. Scrutinise the sender carefully before scanning.

No visible destination
If neither the letter nor the email text explains where the QR code leads, treat it with suspicion.

Login prompt after scanning
"Please sign in again" or "confirm your identity" immediately after a scan are classic phishing patterns.

Claimed new security measure
"For security reasons, please verify your account via QR code" — genuine security updates are not distributed by QR code.

Sticker over an existing QR code
At public locations (charging station, parking machine), attackers can place their own sticker over the legitimate QR code. Check whether the code looks pasted on.

How to protect yourself

For employees

- **Use a QR code scanner with URL preview:** Most modern smartphones show the destination URL before opening the page. Check it before the site loads.
- **When in doubt, type the URL manually:** If a letter is supposed to direct you to a company website, type the known URL directly instead of scanning the code.
- **Do not enter credentials after a QR scan** without verifying the URL in the browser address bar.
- **Question unfamiliar QR codes in the office:** Unknown notices or codes stuck to printers, doors, or meeting rooms should be reported to facilities management.

For administrators

- **Extend training explicitly to quishing** — many awareness programmes still focus only on email links.
- **Email gateway rules for QR code images:** Some next-generation gateways now analyse QR content in email attachments and inline images.
- **Policy for physical notices:** QR codes in office buildings only with approval and clear source labelling (logo, date, responsible team).
- **Mobile Threat Defence (MTD):** Evaluate solutions that check QR scan destinations against reputation databases.

Real cases

CASE 01 · INSURANCE COMPANY · DE · Q3/2025

A letter purportedly from the "Financial Supervisory Authority" asked employees to complete a new identification process via QR code. Five employees scanned the code and entered their Office 365 credentials. Two mailboxes were compromised within the hour.

Damage: two compromised mailboxes, internal pricing lists exfiltrated · **Detection:** SOC alert on unusual login geography · **Lesson:** Regulatory procedures are not conducted via QR codes in letters.

CASE 02 · MUNICIPAL ADMINISTRATION · CH · Q1/2026

Attackers placed QR stickers over the official payment codes on the council's EV charging stations in the underground car park. Users — including staff — paid on a spoofed site and had their credit card details stolen.

Damage: approximately CHF 8,000 across multiple victims · **Detection:** user complaint to the admin hotline · **Lesson:** Physical QR codes at public locations should be checked regularly for tampering.

What to do if it happens?

THE FIRST 15 MINUTES

1. **Close the page immediately** — no further interaction, do not enter any data.
2. **Screenshot the URL** in the browser address bar — as evidence.
3. **Inform IT helpdesk** if credentials were entered on the page.
4. **Invalidate password and sessions** for the affected account — from a different device.
5. **Preserve the physical QR code** (do not remove it) and notify IT or facilities management if it is a sticker in the office building.
6. **Warn colleagues** if the QR code was in a publicly accessible location.

Frequently asked questions

Can my email gateway detect quishing?

Older gateways cannot — they see only an image. Newer AI-powered solutions can extract QR content and assess the embedded URL. It is worth checking whether your solution supports this.

Are QR codes in legitimate emails always suspicious?

Not inherently. But legitimate companies typically use text links in emails, not QR codes. QR codes in email are an unusual pattern — and the unusual deserves more attention.

How can I tell a genuine QR sticker from a fake one?

Visually, it is very difficult. Check whether the sticker sits loosely, has air bubbles, or appears to cover printed material underneath. When in doubt: do not scan, but visit the known website directly or contact the operator.

Related topics

Quishing is often embedded in broader phishing campaigns. Understanding quishing is best paired with knowledge of smishing, vishing, and classic email phishing.