BEDROHUNGS-BIBLIOTHEK

JULITH GmbH
Awareness-as-a-Service

Quishing — wenn der QR-Code lügt

QR-Codes umgehen klassische E-Mail-Filter und Link-Vorschauen. Quishing-Angriffe nutzen das gezielt aus — in Briefen, Aufklebern auf Parkautomaten, gefälschten Speisekarten.

min Lesezeit: 6 min **Aktualisiert:** 14. März 2026 **Risiko:** Hohes Risiko
Quelle: awareness-as-a-service.com/de/resources/threats/quishing

Was ist Quishing?

Quishing (QR-Code + Phishing) ist der Einsatz manipulierter QR-Codes, um Opfer auf gefälschte Websites zu lotsen. Der Begriff ist vergleichsweise jung, das Phänomen hat seit 2023 erheblich zugenommen — parallel zur allgemeinen Verbreitung von QR-Codes im Alltag.

Das Tückische an Quishing ist das Zusammenspiel zweier Schwachstellen: E-Mail-Gateways können den Inhalt eines Bildes nicht als Link analysieren; Nutzer können den Zielort eines QR-Codes vor dem Scannen nicht sehen. Beide Schwächen werden gezielt ausgenutzt.

Angriffsvektoren sind vielfältig: QR-Codes in E-Mails ("Bitte verifizieren Sie Ihr Konto"), physische Aufkleber auf öffentlichen Ladestationen oder Parkautomaten sowie gedruckte Materialien, die in Wartezimmern, auf Konferenzen oder in Büroküchen auliegen.

Auf einen Blick

01

Unsichtbar für E-Mail-Filter

QR-Codes sind Bilder. Kein Link-Scanner im Gateway sieht, wohin sie führen — der Angriff passiert den Perimeter ungeprüft.

02

Auch physisch möglich

Aufkleber auf Parkautomaten, Ladesäulen oder Restaurantmenüs sind real dokumentierte Angriffsvektoren.

03

Scan erfolgt oft mit privatem Handy

Wer einen QR-Code mit dem Privatgerät scannt, umgeht MDM, VPN und andere Unternehmenskontrollen.

Woran erkennen Sie Quishing?

QR-Code im Brief oder Aushang
Behörden, Banken und Versorger kommunizieren selten per QR-Code in Briefen. Prüfen Sie den Brief-Absender sorgfältig.

Kein Klartext-Ziel sichtbar
Wenn weder Brief noch E-Mail-Text erklärt, wohin der QR-Code führt, ist Vorsicht angebracht.

Aufforderung zur Anmeldung nach dem Scannen
"Bitte melden Sie sich erneut an" oder "Bestätigen Sie Ihre Identität" direkt nach dem Scan sind klassische Phishing-Muster.

Angeblich neue Sicherheitsmaßnahme
"Aus Sicherheitsgründen bitten wir Sie, Ihr Konto per QR-Code zu verifizieren" — echte Sicherheits-Updates werden nicht per QR verteilt.

Aufkleber über bestehenden QR-Codes
An öffentlichen Stellen (Ladesäule, Parkscheinautomat) können Angreifer eigene Aufkleber über den echten QR-Code kleben. Prüfen Sie, ob der Code aufgeklebt wirkt.

So schützen Sie sich

Für Mitarbeitende

- **QR-Code-Scanner mit URL-Vorschau verwenden:** Die meisten modernen Smartphones zeigen vor dem Öffnen die Ziel-URL an. Diese prüfen, bevor die Seite geladen wird.
- **Im Zweifel URL manuell eintippen:** Wenn ein Brief Sie zu einer Unternehmenswebsite führen soll, tippen Sie die bekannte URL direkt ein — statt den QR-Code zu scannen.
- **Keine Zugangsdaten nach QR-Scan eingeben,** ohne die URL im Browser zu verifizieren.
- **Physische QR-Codes im Büro hinterfragen:** Unbekannte Aushänge oder aufgeklebte QR-Codes an Druckern, Türen oder Konferenzräumen dem Facility-Management melden.

Für Administratoren

- **Schulung explizit auf Quishing ausweiten** — viele Awareness-Programme fokussieren noch auf E-Mail-Links.
- **E-Mail-Gateway-Regeln für QR-Code-Bilder** konfigurieren: Einige Next-Gen-Gateways analysieren QR-Inhalte in E-Mail-Anhängen und Inline-Bildern.
- **Richtlinie für physische Aushänge:** QR-Codes im Bürogebäude nur mit Genehmigung und visueller Herkunfts-Kennzeichnung (Logo, Datum).
- **Mobile-Threat-Defence** (MTD) prüfen, die QR-Scan-Ziele auf Reputation analysiert.

Echte Beispiele

FALL 01 · VERSICHERUNGSGESELLSCHAFT · DE · Q3/2025

Ein vermeintlicher Brief der "Finanzmarktaufsicht" forderte Mitarbeitende auf, per QR-Code ein neues Identifikationsverfahren zu durchlaufen. Fünf Mitarbeitende scannten den Code und gaben ihre Office-365-Zugangsdaten ein. Zwei Postfächer wurden innerhalb einer Stunde kompromittiert.

Schaden: zwei kompromittierte Postfächer, interne Preislisten abgeflossen · **Erkennung:** SOC-Alert auf ungewöhnliche Login-Geografie · **Lehre:** Behördliche Verfahren werden nicht per QR-Code im Brief abgewickelt.

FALL 02 · STADTVERWALTUNG · CH · Q1/2026

Auf den stadteigenen E-Ladestationen im Tiefgaragen-Parkhaus klebten Angreifer QR-Aufkleber über die offiziellen Payment-Codes. Nutzende (darunter Mitarbeitende) bezahlten auf einer gefälschten Site — Kreditkartendaten wurden abgegriffen.

Schaden: rund CHF 8.000 in Summe über mehrere Betroffene · **Erkennung:** Nutzerbeschwerde an Verwaltungshotline · **Lehre:** Physische QR-Codes an öffentlichen Stellen regelmäßig auf Manipulation prüfen.

Was tun, wenn es passiert ist?

DIE ERSTEN 15 MINUTEN

1. **Seite sofort schließen** — kein weiteres Interagieren, kein Eingeben von Daten.
2. **Screenshot der URL** im Browser-Adressfeld machen — als Beweismittel.
3. **IT-Helpdesk informieren,** wenn Zugangsdaten auf der Seite eingegeben wurden.
4. **Passwort und Sessions invalidieren** für das betroffene Konto (von einem anderen Gerät aus).
5. **Physischen QR-Code sichern** (nicht entfernen) und IT oder Facility-Management benachrichtigen, wenn es sich um einen Aufkleber im Bürogebäude handelt.
6. **Kollegen warnen,** wenn der QR-Code an einem öffentlich zugänglichen Ort angebracht war.

Häufige Fragen

Kann mein E-Mail-Gateway Quishing erkennen?

Ältere Gateways nicht — sie sehen nur ein Bild. Neuere Lösungen mit KI-basierter Bildanalyse können QR-Inhalte extrahieren und die enthaltene URL bewerten. Ob Ihre Lösung das unterstützt, lohnt sich zu prüfen.

Sind QR-Codes in legitimen E-Mails generell verdächtig?

Nicht grundsätzlich. Aber legitime Unternehmen verlinken in E-Mails üblicherweise mit Text-Links, nicht mit QR-Codes. QR-Codes in E-Mails sind ein ungewöhnliches Muster — und Ungewöhnliches verdient mehr Aufmerksamkeit.

Wie unterscheide ich einen echten von einem gefälschten QR-Code-Aufkleber?

Optisch kaum. Prüfen Sie, ob der Aufkleber locker sitzt, Blasen wirft oder über einem anderen Druck klebt. Im Zweifel: Nicht scannen, sondern die bekannte Website manuell aufrufen oder den Betreiber kontaktieren.

Weitere Themen

Quishing ist häufig eingebettet in breitere Phishing-Kampagnen. Wer Quishing versteht, sollte auch die verwandten Angriffswege Smishing, Vishing und klassisches Phishing kennen.