Wie Sie Erkennen, ob ein QR-Code Sicher Ist, Bevor Sie Ihn Öffnen (Quishing-Guide)

Quishing ist QR-Code-Phishing. Lernen Sie die Warnsignale vor dem Scannen und was Sie nach dem Scannen prüfen sollten, bevor Sie auf 'Öffnen' tippen.

Autor: Lubor Šimůnek · Veröffentlicht: August 23, 2026 · Sicherheit

Online-Version: https://appstoryo.com/de/blog/qr-code-safe-quishing-guide



Was ist Quishing?

Quishing ist Phishing über QR-Codes. Angreifer erstellen einen Code, der nach dem Scannen auf eine betrügerische Website führt — zum Stehlen von Zugangsdaten, Installieren von Malware oder Simulieren einer Zahlungsseite. Der Begriff setzt sich aus 'QR' und 'Phishing' zusammen, und die Bedrohung wächst, weil Menschen QR-Codes fast instinktiv vertrauen.

Warum QR-Codes ein besonderes Risiko darstellen

Bei einem normalen Link können Sie die Maus darüber bewegen und die URL lesen, bevor Sie klicken. Bei einem QR-Code sehen Sie das Ziel erst, wenn Ihr Scanner ihn decodiert hat — und viele Kamera-Apps öffnen den Browser sofort, ohne die Adresse anzuzeigen. Dieser Moment reicht für eine schädliche Website aus, um Ihr Gerät zu verfolgen.

QR-Codes umgehen auch Spam-Filter vollständig: Ein Filter sucht nach verdächtigem Text oder bekannten schädlichen URLs, aber ein QR-Code-Bild wirkt völlig harmlos. Deshalb ersetzen Phishing-E-Mails ihre alten Links zunehmend durch QR-Codes, besonders bei Angriffen auf Unternehmen.

Im Alltag begegnet Quishing als Aufkleber über echten Codes an Parkautomaten, gefälschten

Speisekarten, Paketbenachrichtigungen im Briefkasten und falschen öffentlichen Ladestationen mit der Aufforderung, 'zum Bezahlen zu scannen'.

Warnsignale VOR dem Scannen

- **Aufkleber über einem Original-Code.** Ein QR-Aufkleber, der über einem anderen klebt, ist ein klassischer Austausch. Heben Sie die Ecke leicht an — wenn er sich ablöst, nicht scannen.
- **Dringlichkeitssprache auf einem unbekannten Flyer.** 'Jetzt scannen und Preis gewinnen' oder 'Ihr Paket liegt bereit — scannen Sie zum Umplanen' sind Drucktaktiken.
- **Unverlangte E-Mail oder Post.** Eine unerwartete Mitteilung einer Bank, eines Paketzustellers oder einer Behörde, bei der ein QR-Code der zentrale Aufruf zum Handeln ist, ist ein starkes Warnsignal.

Was Sie NACH dem Scannen und VOR dem Öffnen prüfen sollten

- **Stimmt die Domain mit Ihren Erwartungen überein?** Wenn Sie einen QR bei einer Bank gescannt haben, muss die URL auf der offiziellen Domain liegen.
- **Ist es ein URL-Kürzer?** Dienste wie bit.ly oder tinyurl.com verbergen das eigentliche Ziel. Nutzen Sie einen URL-Expander, um die echte Adresse zu ermitteln.
- **Falsch geschriebene Domains.** Achten Sie auf paypa1.com oder g00gle.com — lesen Sie jeden Buchstaben sorgfältig.
- **Verdächtige Subdomains.** login.sicher.amazon-pakete-de.com wirkt legitim, aber die eigentliche Domain ist amazon-pakete-de.com, nicht amazon.com.

Wie QR Code Reader Without Ads hilft

QR Code Reader Without Ads zeigt die vollständige URL an, bevor irgendetwas geöffnet wird. Sie haben einen Moment, um den Link zu prüfen. Sieht die Adresse verdächtig aus, tippen Sie einfach nicht auf 'Öffnen'. Die App speichert einen lokalen Scan-Verlauf auf Ihrem Gerät, sammelt keine Daten und zeigt keine Werbung. Verfügbar im App Store und bei Google Play — suchen Sie nach 'QR Code Reader Without Ads'.

Laden Sie QR Code Reader Without Ads kostenlos für iOS oder Android herunter — ohne Werbung, ohne Tracking und komplett offline nutzbar.

Zitieren als: Lubor Šimůnek (2026). *Wie Sie Erkennen, ob ein QR-Code Sicher Ist, Bevor Sie Ihn Öffnen (Quishing-Guide)*. AppStoryo, lapnito.cz s.r.o.. https://appstoryo.com/de/blog/qr-code-safe-quishing-guide
© 2026 lapnito.cz s.r.o.