kartensicherheit.de
Aufklärung, Vernetzung, Information

EURO KARTENSYSTEME

Presseinformation

Quishing: Wie QR-Codes zur Falle werden

Frankfurt, 4. November 2026 – Mit der steigenden Verbreitung von QR-Codes nimmt eine abgewandelte Form des Phishings stetig zu: das sogenannte Quishing. Kriminelle manipulieren dabei QR-Codes, um sensible Daten abzugreifen oder Schadsoftware zu verbreiten. Die Gefahr liegt im Verborgenen: Während sich klassische Phishing-Mails teilweise an verdächtigen Webadressen erkennen lassen, verschleiern die präparierten QR-Codes das tatsächliche Ziel der Verlinkung.



Bildquelle: Imageflow/Shutterstock.com

Wo Fälschungen auftauchen können:

- In E-Mails: Als angebliche Bestätigung für Anmeldungen, Passwort-Rücksetzungen oder Rechnungen.
- Im öffentlichen Raum: Durch Überkleben von echten QR-Codes auf Parkscheinautomaten, Ladesäulen für E-Fahrzeuge, Speisekarten oder Plakaten.
- In Briefen und Flyern: Als vermeintliche Benachrichtigung von Kreditinstituten, Behörden oder Paketdiensten.

Wird ein schädlicher QR-Code gescannt, leitet er auf eine gefälschte Website, die der echten Login-Seite eines bekannten Anbieters täuschend ähnlich sieht. Gibt man dort Anmeldedaten, PINs oder Kreditkartendaten ein, landen diese bei den Kriminellen.

Schutz vor Quishing-Angriffen:

1. Vor dem Öffnen des Links im Smartphone-Browser immer die angezeigte Webadresse sorgfältig kontrollieren. Passt die Domain exakt zum angegebenen Anbieter?
2. Im öffentlichen Raum prüfen, ob ein Sticker über den ursprünglichen QR-Code geklebt wurde.
3. Sensible Daten oder Logins nicht unüberlegt nach dem Scannen eingeben. Im Zweifel die offizielle Adresse direkt im Browser aufrufen.
4. Bietet eine QR-Code-Weiterleitung den Download einer Datei oder App außerhalb offizieller Stores an, den Vorgang sofort abbrechen.
5. Wo möglich, die Zwei-Faktor-Authentifizierung aktivieren, um Zugänge zusätzlich abzusichern.

kartensicherheit.de unterstützt die bundesweite Kampagne „Machen wir Phishen Impossible!“. Unter der Schirmherrschaft der Deutschen Bundesbank und des Bundesministeriums der Finanzen warnt eine branchenübergreifende Allianz aus Finanzwirtschaft, Telekommunikation, Digitalbranche, Politik und Sicherheitsbehörden vor Cyberbetrug im Zahlungsverkehr. Ziel ist es, Verbraucherinnen und Verbraucher für typische Angriffsszenarien zu sensibilisieren und praktische Verhaltenstipps zu vermitteln.

kartensicherheit.de ist die zentrale Anlaufstelle für Aufklärung, Vernetzung und Information rund um die Sicherheit bei Kartenzahlungen, initiiert von der EURO Kartensysteme in Zusammenarbeit mit der Deutschen Kreditwirtschaft. Verbraucherinnen und Verbraucher finden dort praktische Tipps zum sicheren Umgang mit Karte und PIN, aktuelle Hinweise zu Betrugsformen wie Social Engineering sowie vielfältige Präventionsinformationen.

EURO Kartensysteme GmbH | Solmsstraße 6 | D-60486 Frankfurt am Main | **T** +49 (0) 69/9 79 45-0 | **F** +49 (0) 69/9 79 45-48 88 | **W** www.eurokartensysteme.de
Vorsitzender des Aufsichtsrats Kolja Gabriel | **Geschäftsführung** Oliver Hommel (Vorsitzender), Susanne Raupbach | **Steuernummer** 045 232 54053
Umsatzsteuer ID DE257820111 | **Handelsregister** Frankfurt am Main, HRB 80376 | **Bankdaten** Deutsche Bank AG | **IBAN** DE78 5007 0010 0092 5974 00 | **BIC** DEUTDEFFXXX

kartensicherheit.de
Aufklärung, Vernetzung, Information

EURO KARTENSYSTEME

EURO Kartensysteme GmbH
Andreas Peppler
Direktor Sicherheitsmanagement
Tel.: +49 (0) 69 979 454 558
andreas.peppler@eurokartensysteme.de

Schwarz & Sprenger - Agentur für Öffentlichkeitsarbeit GmbH
Anja Schneider
Geschäftsführerin
Tel.: +49 (0) 89 215 378 871
anja.schneider@schwarz-sprenger.de