NACHRICHTEN
Österreich

26. März 2025

Achtung, QR-Code-Falle! Polizei warnt vor fieser Betrugsmasche

Polizei warnt vor gefälschten QR-Codes in Österreich: Neue Betrugsmasche zielt auf persönliche Daten von Autofahrern und Bankkunden ab.

Salzburg, Österreich - QR-Codes erfreuen sich in Österreich großer Beliebtheit und bieten zahlreiche praktische Anwendungen, doch die Polizei warnt eindringlich vor einer neuen Betrugsmasche. Verbrecher nutzen gefälschte QR-Codes, um persönliche Daten und finanzielle Informationen von ahnungslosen Bürgern zu stehlen. Diese Betrugsform, auch als „Quishing“ bekannt, zielt insbesondere auf Autofahrer ab, die Parkscheine per Smartphone bezahlen, sowie auf Bank- und Paketdienstkunden. Betrüger überkleben Originalcodes an Parkautomaten, Abholscheinen der Post und Bankunterlagen mit täuschend echten Fälschungen.

Nutzer, die versehentlich einen dieser gefälschten QR-Codes scannen, werden auf betrügerische Webseiten geleitet und aufgefordert, vertrauliche Informationen einzugeben. Berichten zufolge wurden im Februar 2023 in Salzburg etwa 40 Parkautomaten mit solchen Manipulationen entdeckt, und Gefahr besteht ebenso in Städten wie Linz und in der Steiermark. Autofahrer sind besonders gefährdet, da digitale Sicherheitssoftware oft nicht in der Lage ist, diese Angriffe zu erkennen.

Warnungen und Prävention

Die Arbeiterkammer hat die Problematik als landesweites

Phänomen erkannt und warnt eindringlich vor der Verwendung aufgeklebter QR-Codes. Ein AK-Experte rät dazu, diese nicht zu scannen und stattdessen offizielle Apps für Zahlungen zu nutzen. In Wien wurde zudem von gefälschten Strafzetteln berichtet, die wie offizielle Zahlungsaufforderungen der Polizei aussahen. Diese Betrügermethoden beschränken sich nicht nur auf Parkautomaten, sondern sind auch in E-Mails und Briefen von Banken oder der Österreichischen Gesundheitskasse (ÖGK) zu finden.

Im Kontext der Cybersicherheit ist es wichtig zu betonen, dass Quishing nicht auf Österreich beschränkt ist. Vor großen Veranstaltungen, wie den Olympischen Spielen 2024 in Paris, haben Cyberkriminelle ähnliche gefälschte QR-Codes und Domains registriert, um persönliche Daten zu stehlen. Sicherheitsmaßnahmen gegen Quishing umfassen die Überprüfung der URL nach dem Scannen und die manuelle Eingabe der URL in den Browser, um Risiken zu minimieren. Nutzer sollten stets kritisch die Herkunft von Domains prüfen und darauf achten, dass Webseiten durch „https“ und ein Schloss-Symbol gesichert sind.

Vorsichtsmaßnahmen für die Nutzer

- Überprüfen Sie die URL nach dem Scannen mit speziellen Tools.
- Eingabe der URL manuell, anstatt den QR-Code zu scannen, wenn möglich.
- Prüfen Sie auf SSL-Zertifikate, die sichere Seiten auszeichnen.
- Nutzung von Link-Checkern zur Identifizierung potenziell gefährlicher Links.
- Überprüfen Sie die Bewertungen und die Reputation unbekannter Online-Shops.

Die fortschreitende Digitaliserung bringt nicht nur Vorteile, sondern auch neue Risiken mit sich. Es ist unerlässlich, dass Bürger wachsam bleiben und sich über die aktuellsten

Betrugsmethoden informieren, um nicht Opfer von Cyberkriminalität zu werden. Die Polizei, sowie andere Institutionen, bleiben wachsam und informieren weiterhin über diese besorgniserregende Entwicklung in der digitalen Welt.

Kosmo berichtet, dass ... **Kleine Zeitung** informiert über ... und **Security Insider** bietet wertvolle Tipps für den Schutz vor QR-Code-Betrug.

Details	
Vorfall	Betrug
Ursache	QR-Codes
Ort	Salzburg, Österreich
Quellen	• **www.kosmo.at** • **www.kleinezeitung.at** • **www.security-insider.de**

Besuchen Sie uns auf: die-nachrichten.at