

Vorsicht! Polizei warnt vor neuer Quishing-Betrugsmasche an Parkautomaten

Die Polizei warnt vor „Quishing“: Manipulierte QR-Codes an Parkautomaten in Österreich gefährden Daten. Tipps zum Schutz.



Vorarlberg, Österreich - In den letzten Monaten hat sich in Österreich eine besorgniserregende Betrugsmasche verbreitet, die auf die Technologie der QR-Codes abzielt. Diese Methode, bekannt als „Quishing“, ist besonders häufig an Parkautomaten anzutreffen, wo Kriminelle echte QR-Codes mit manipulierten Aufklebern überkleben. Autofahrer, die diese Codes scannen, werden auf gefälschte Bezahlssysteme geleitet, die dazu dienen, sensible persönliche Informationen auszuspionieren, wie beispielsweise Kreditkartennummern und Kennzeichen-Informationen. Laut **oe24** warnen sowohl die Polizei als auch Verbraucherschutzorganisationen vor dieser Betrugsmasche.

Der Begriff „Quishing“ setzt sich aus den Wörtern „QR-Code“ und „Phishing“ zusammen und ist nicht nur auf Parkautomaten beschränkt. Gefälschte QR-Codes treten ebenfalls in E-Mails, Briefen und auf Plakaten auf. Diese Entwicklung ist besonders alarmierend, da QR-Codes häufig als harmlos und nützlich wahrgenommen werden, jedoch von vielen Antiviren-Programmen nicht als Bedrohung erkannt werden, wie **anwal.de** beschreibt.

Risiken und Erkennung von Quishing

Manipulierte QR-Codes sind meist in Form von Aufklebern angebracht und führen nicht zu offiziellen Bezahlseiten. Bevor Nutzer ihre Daten eingeben, sollten sie unbedingt die URL der Webseite überprüfen. Die Verbraucherschutzorganisation Arbeiterkammer bietet spezifische Tipps, um sich vor Quishing zu schützen. So sollte man beispielsweise keine QR-Codes scannen, die als Aufkleber angebracht sind, und lieber die offizielle App des Anbieters nutzen, wie **vbg.arbeiterkammer.at** empfiehlt.

Ein weiteres Risiko besteht darin, dass Quishing oft unbemerkt bleibt. Aufgrund der unsichtbaren Inhalte eines QR-Codes können selbst geübte Nutzer in die Falle tappen. Typische Anzeichen für Quishing sind Aufforderungen zur Eingabe von persönlichen Informationen nach dem Scannen eines QR-Codes oder das Erhalten eines Briefes von angeblichen Instituten, in dem zur Zustimmung auf einem QR-Code gedrängt wird.

Maßnahmen zur Verhinderung und Reaktion

Die Polizei und Verbraucherschützer raten, bei Verdacht auf Quishing proaktiv zu handeln. Dazu gehört das sofortige Informieren der Bank und die Sperrung betroffener Konten. Es ist ebenfalls ratsam, alle Passwörter für Online-Konten zu ändern und Anzeige bei der Polizei zu erstatten. Um zukünftig sicherer zu agieren, sollten Nutzer skeptisch gegenüber unaufgeforderten QR-Codes sein und die Echtheit von E-Mails

oder Briefen direkt beim Absender überprüfen.

Durch die zunehmende Digitalisierung und den Einsatz von QR-Codes wird es immer wichtiger, sich über Betrugsmaschinen wie Quishing zu informieren und zu sensibilisieren. Nur so kann der finanzielle Schaden, der durch derartige Machenschaften entstehen kann, minimiert werden.

Details	
Vorfall	Betrug
Ort	Vorarlberg, Österreich
Quellen	• www.oe24.at • vbg.arbeiterkammer.at • www.anwalt.de

Besuchen Sie uns auf: die-nachrichten.at