

QR Code Betrugsmasche

Genannt Quishing

Quishing ist eine Betrugsmasche, bei der Kriminelle gefälschte QR-Codes verwenden, um an sensible Daten zu gelangen oder Geld zu stehlen.



Was ist Quishing?

Quishing ist ein Kofferwort aus "QR-Code" und "Phishing". Dabei nutzen Betrüger QR-Codes, um ahnungslose Nutzer auf gefälschte Webseiten zu locken, wo sie persönliche Informationen wie Kreditkartendaten oder Passwörter eingeben sollen. Diese Betrugsmasche kann in verschiedenen Kontexten auftreten, z.B. in gefälschten Bankbriefen, an Ladesäulen für Elektroautos oder auf Parkautomaten.

Wie funktioniert Quishing?

- **Manipulation von QR-Codes:** Kriminelle überkleben echte QR-Codes mit gefälschten, die auf betrügerische Webseiten führen. Diese Seiten sehen oft täuschend echt aus und fordern die Nutzer auf, sensible Daten einzugeben.
- **Verbreitung:** Quishing kann über verschiedene Kanäle erfolgen, einschließlich Briefpost, E-Mails, und sogar in öffentlichen Verkehrsmitteln. Oft werden QR-Codes in gefälschten Straßzetteln oder Werbeplakaten platziert.

Schutzmaßnahmen

- **Überprüfen Sie QR-Codes:** Scannen Sie QR-Codes nur, wenn Sie sich über deren Echtheit sicher sind. Nutzen Sie, wenn möglich, QR-Code-Scanner, die den Link vor dem Öffnen anzeigen.

-

- **Seien Sie vorsichtig bei unerwarteten QR-Codes:** Wenn Sie einen QR-Code in einem Brief oder auf einem Plakat sehen, das Sie nicht erwartet haben, seien Sie vorsichtig. Kontaktieren Sie im Zweifelsfall die angebliche Quelle, um die Echtheit zu überprüfen.
- **Aktivieren Sie Sicherheitsfunktionen:** Einige Smartphones bieten die Möglichkeit, das sofortige Öffnen von Links zu deaktivieren, was zusätzlichen Schutz bieten kann.

Fazit

Quishing ist eine ernstzunehmende Betrugsmasche, die immer häufiger vorkommt. Seien Sie wachsam und schützen Sie Ihre persönlichen Daten, indem Sie QR-Codes nur von vertrauenswürdigen Quellen scannen und immer die Links überprüfen, auf die Sie weitergeleitet werden.