Vorsicht vor Quishing: Tipps zum Schutz vor betrügerischen QR-Codes

Die Verbraucherzentrale NRW warnt vor „Quishing“: Gefälschte QR-Codes sind eine neue Betrugsmasche. Informieren Sie sich jetzt!

Die Verbraucherzentrale NRW hat eine dringende Warnung herausgegeben, um die Öffentlichkeit über neue Betrugsmethoden zu informieren, die sich zunehmend verbreiten.

Im Rhein-Erft-Kreis ist das Scannen von QR-Codes zur normalen Praxis geworden, sei es um die neuesten Speisekarten zu lesen oder um auf die Bankkonten zuzugreifen. Doch eine neue Betrugsmasche, bekannt als „Quishing“, zieht dunkle Schatten über diese vermeintlich harmlose Technologie.

Quishing ist ein Begriff, der sich aus den Wörtern QR-Code und Phishing zusammensetzt. Phishing bezieht sich auf den Versuch, persönliche Informationen wie Passwörter zu stehlen. Dabei bedienen sich die Betrüger nicht nur digitaler Mittel, sondern kombinieren diese mit traditionellen Methoden, um Opfer zu täuschen.

Ein Beispiel: Kriminelle manipulieren QR-Codes an öffentlichen Orten, indem sie sie überkleben, oder sie verschicken gefälschte Briefe von Banken. Hierbei können ahnungslose Personen leicht auf eine gefälschte Internetseite geleitet werden, die böswillige Absichten verfolgt.

Gefahren bei QR-Codes

Wenn man einen QR-Code scannt, öffnet sich oft sofort eine damit verbundene Webseite. Obwohl dies sehr praktisch ist, birgt es auch erhebliche Risiken. Die Verbraucherzentrale empfiehlt, QR-Codes nur zu scannen, wenn man sicher ist, wohin sie führen. Es sollte vermieden werden, dass das Smartphone automatisch auf Links zugreift, die möglicherweise gefährlich sind.

Mit einer speziellen App kann man den Link vor dem Öffnen anzeigen lassen. So kann geprüft werden, ob der Link legitim ist. Wenn Unsicherheiten bestehen, sollte die Webseite niemals geöffnet werden, da diese Schritte entscheidend sein können, um persönliche Daten zu schützen.

Besondere Vorsicht ist auch bei den QR-Codes in Briefen geboten. Bankmitteilungen, die auf den ersten Blick seriös erscheinen, können ebenfalls gefälscht sein. Bei einem solchen Schreiben ist es ratsam, die Authentizität durch Kontaktaufnahme mit der Bank zu überprüfen. Die Kontakten sollten dabei über offizielle Kanäle, wie die Webseite der Bank, erfolgen, um sicherzustellen, dass keine weiteren Daten in die falschen Hände geraten.

Schutzmaßnahmen für Autofahrer

Auch Autofahrer müssen beim Scannen von QR-Codes genau aufpassen, insbesondere an E-Ladesäulen oder bei angeblichen Strafzetteln. Cyberkriminelle nutzen häufig diese Gelegenheiten, um mithilfe gefälschter Codes Geld zu stehlen. Sie überkleben die echten QR-Codes oder hinterlassen falsche Strafzettel, um Überweisungen zu erzielen.

Hier ist es wichtig zu prüfen, ob ein QR-Code nicht manipuliert wurde. Im Zweifelsfall sollte auch die Polizei kontaktiert werden, um sicherzustellen, dass keine falschen Sanktionen ausgesprochen wurden und dass die finanziellen Transaktionen sicher sind.

Wer dennoch auf eine Betrugsmasche hereingefallen ist, sollte sofort die Polizei einschalten und gegebenenfalls seine Bank informieren. Die Verbraucherzentrale gibt Hinweise darauf, dass oft bestimmte Indikatoren auf einen Betrugsversuch hinweisen, wie etwa eine fehlende persönliche Anrede oder der Druck, sofort handeln zu müssen.

Für weitere Informationen zu spezifischen Betrugsfällen und wie man sich davor schützen kann, bietet die Verbraucherzentrale NRW online Hilfestellungen an. Es ist essenziell, über aktuelle Betrugsmaschen informiert zu sein und sich nicht von vermeintlich sicheren Angeboten blenden zu lassen.

Details