

Achtung! So schützen Sie sich vor dem neuesten QR-Code-Betrug!

Die Polizei warnt vor der Betrugsmasche „Quishing“, bei der Täter QR-Codes nutzen, um persönliche Daten zu stehlen. Seien Sie vorsichtig!

Achtung, aufgepasst! Die Polizei schlägt Alarm: Mit einer brandneuen Betrugsmasche namens „Quishing“ versuchen Verbrecher, den Menschen das Geld aus der Tasche zu ziehen! Anscheinend beliebte QR-Codes werden von Kriminellen schamlos ausgenutzt, um an sensible Daten zu gelangen. Doch was steckt wirklich dahinter?

Zunächst sorgt eine Flut gefälschter Briefe für Verwirrung – geschickt inszeniert, erwecken sie den Eindruck, von renommierten Banken zu stammen. Diese Schreiben sehen professionell aus und sollen das Vertrauen der Empfänger wecken, damit sie nicht misstrauisch werden. Tragisch ist, dass viele Leute glauben, sie könnten ihren Bankdaten vertrauen. Doch Vorsicht: Wer glaubt, sich sicher zu fühlen, könnte schnell zum Opfer werden!

So funktioniert das perfide Spiel

Die Betrüger tarnen sich als ihre eigene Bank und fordern die Empfänger auf, einen QR-Code zu scannen. Doch statt der vertrauenswürdigen Bankseite landet der Unbedarfte auf einer fiesen Fake-Webseite. Kaum jemand kann auf den ersten Blick erkennen, dass hier die Falle zuschnappt! Und ehe man sich versieht, gibt das Opfer seine wertvollen Zugangsdaten preis oder veranlasst sogar Geldtransfers!

Die Polizei warnt eindringlich davor, auf solche fiesen Tricks hereinzufallen. Ihr Appell ist klar und deutlich: Seien Sie wachsam! Überprüfen Sie im Zweifelsfall den Absender und kontaktieren Sie Ihre Bank über offizielle Kommunikationswege – ganz ohne QR-Code! Wissen Sie, woher der QR-Code stammt, bevor Sie ihn scannen! Wenn Ihnen ein verdächtiges Schreiben ins Haus flattert, schieben Sie es direkt in den Papierkorb!

So schützen Sie sich!

Seien Sie sicher, dass Sie beim Umgang mit QR-Codes genauso genau sind wie bei E-Mails von unbekannten Absendern. Ihre Daten sind kostbar – wahren Sie diese mit aller Konsequenz! Nutzen Sie außerdem die Multi-Faktor-Authentifizierung, um sicherzustellen, dass selbst wenn die Betrüger Ihre Daten ergattern, sie trotzdem keinen Zugriff auf Ihre Konten haben!

Sollten Sie bereits auf einen dieser Betrugsversuche hereingefallen sein, zögern Sie nicht! Kontaktieren Sie umgehend die Polizei oder sperren Sie Ihr Konto über den Sperr-Notruf 116116. Handeln Sie rasch, denn jede Sekunde zählt!

Details

Besuchen Sie uns auf: n-ag.de