MEIN HESSEN NACHRICHTEN AG

27. Juni 2025

Achtung in Kassel: Gefälschte QR-Codes an Parkscheinautomaten entdeckt!

In Kassel gibt es Betrugswarnungen zu gefälschten QR-Codes an Parkscheinautomaten. Experten raten zur Vorsicht und bieten Schutzmaßnahmen an.

Kassel, Deutschland - In Kassel sind derzeit zahlreiche Parkscheinautomaten ins Visier von Betrügern geraten. Unbekannte haben diese Automaten mit gefälschten QR-Codes überklebt, die ahnungslose Nutzer in die Falle locken sollen. Diese Betrugsmasche, bekannt als ȣQuishingȣ, führt dazu, dass beim Scannen der QR-Codes die Bediener auf angeblich vertrauenswürdige Webseiten geleitet werden, deren einziger Zweck jedoch der Diebstahl persönlicher Daten ist. Die Polizei in Nordhessen ist über das Vorgehen informiert und empfiehlt dringend, die QR-Codes vor dem Scannen genau zu überprüfen. Hessenschau berichtet, dass das Landeskriminalamt Hessen konkrete Warnhinweise gegen Quishing herausgegeben hat.

ȣQuishingȣ setzt sich aus den Begriffen ȣQR-Codeȣ und ȣPhishingȣ zusammen. Dabei nutzen Betrüger die Schwächen der QR-Code-Technologie aus. Scannt ein Nutzer einen gefälschten QR-Code, der auf einen externen Server umleitet, kann er dennoch auf die offizielle Seite des Anbieters geleitet werden, aber unter falschen Vorzeichen. Insgesamt werden so Kontakt- und Bankdaten ohne das Wissen des Nutzers gestohlen. Das Verfahren ist besonders riskant, da viele Smartphones den Inhalt eines QR-Codes erst beim Öffnen der Webseite anzeigen, wodurch es für die Betrüger einfacher ist, sensible Daten abzufangen Geldundverbraucher.

Das Risiko im Fokus

Betroffen sind insbesondere Nutzer des Zahlungsdienstleisters Pay by Phone. Die Stadt Kassel hat bereits Maßnahmen ergriffen, um die gefälschten QR-Codes zu entfernen, denkt aber auch darüber nach, Strafanzeige gegen die unbekannten Täter zu stellen. In einer Stadt mit über 300 Parkscheinautomaten ist das jedoch keine einfache Aufgabe. Christopher Kunz von Heise Security weist darauf hin, dass die Täter gezielt schwächere Smartphones und veraltete Software ausnutzen. Diese Risikofaktoren können dazu führen, dass wichtige Sicherheitsvorkehrungen im wahrsten Sinne des Wortes umgangen werden.

ȣEs ist erschreckend, wie kreativ die Betrüger bei der Täuschung ihrer Opfer sindȣ, sagt ein Mitarbeiter des Verbraucherschutzes. Die Verbraucherzentrale Niedersachsen rät, QR-Codes nur aus vertrauenswürdigen Quellen zu scannen und vor dem Öffnen einer Webseite immer die URL zu überprüfen. Dies könne vor unangenehmen Überraschungen bewahren Verbraucherzentrale Niedersachsen.

Tipps zur Prävention

Um sich vor Quishing zu schützen, sollten Nutzer folgende Hinweise beachten:

- QR-Codes nur scannen, wenn deren Herkunft bekannt und vertrauenswürdig ist.
- Eine Smartphone-Kamera-App verwenden, die die gescannte Internetadresse vor dem Öffnen anzeigt.
- Bei verdächtigen Nachrichten den Absender recherchieren und direkt über offizielle Kontaktwege bestätigen.
- An E-Ladesäulen oder ähnlichen Standorten darauf achten, ob QR-Codes überklebt wurden.
- Bei Verdacht auf Betrug schnell handeln und die Polizei informieren; bei Geldüberweisungen die Bank sofort kontaktieren.

Das Thema Quishing zeigt einmal mehr, wie wichtig eine kritische Auseinandersetzung mit digitalen Zahlungsmethoden ist. Es bleibt zu hoffen, dass durch Aufklärung und präventive Maßnahmen der Schaden begrenzt werden kann und die Nutzer sicherer unterwegs sind. Denken Sie daran: Ein gutes Händchen bei digitalen Zahlungen ist gefragt!

Details	
Ort	Kassel, Deutschland
Quellen	• www.hessenschau.de • www.geldundverbraucher.de • www.verbraucherzentrale-niedersachsen.de

Besuchen Sie uns auf: nag-hessen.de