



HESSISCHER LANDTAG

01. 04. 2025

Kleine Anfrage

**Sandra Weegels (AfD), Pascal Schleich (AfD), Bernd Erich Vohl (AfD),
Christian Rohde (AfD), Markus Fuchs (AfD) und Karsten Bletzer (AfD)**
vom 25.02.2025

Betrug an Parkautomaten etc. durch „Quishing“

und

Antwort

Minister des Innern, für Sicherheit und Heimatschutz

Vorbemerkung Fragesteller:

Derzeit breitet sich nach Medienberichten eine Betrugsmasche aus, welche als „Quishing“ bezeichnet wird. Diese Bezeichnung setzt sich zusammen aus „QR-Code“ und „Phishing“. Betrüger bringen zum Beispiel auf Parkautomaten oder Ladesäulen täuschend echt aussehende QR-Code-Aufkleber an, durch welche die Nutzer, statt auf eine Internetseite für die Bezahlung der entsprechenden Dienstleistungen auf täuschend echt aussehende Internetseiten von Betrügern weitergeleitet werden. Dort werden den Opfern falsche Bankverbindungen angezeigt. Bei Zahlung werden die zu entrichtenden Beträge dann einem Konto des Betrügers oder eines Mittelsmannes gutgeschrieben. In Frankfurt am Main kam es bereits zu mehreren Fällen von „Quishing“ an Parkscheinautomaten.

Die Vorbemerkung der Fragesteller vorangestellt, beantworte ich die Kleine Anfrage wie folgt:

- Frage 1 Wie viele Fälle von versuchtem oder vollendeten Betrug, die unter das in der Vorbemerkung beschriebene Phänomen des „Quishings“ subsumiert werden müssen, sind bis dato in Hessen polizeilich erfasst geworden? Bitte die Fälle pro Jahr und getrennt nach versuchten und vollendeten Taten aufschlüsseln.
- Frage 2 Welche Dienstleistungsarten, welche sich im öffentlichen Raum befinden, waren bisher von solchen Betrugereien betroffen? Bitte sämtliche Dienstleistungsarten auflisten.
- Frage 3 In wie vielen dieser Fälle waren ortsgebundene Dienstleistungen im öffentlichen Raum, wie etwa die Bezahlung von Park- oder Ladegebühren, von diesen Betrugsdelikten betroffen?
- Frage 4 Welcher Schaden ist durch die entsprechenden Betrugsdelikte entstanden? Bitte die Gesamthöhe des Schadens durch alle vollendeten Betrugsdelikte im Sinne von „Quishing“ nennen.
- Frage 5 In wie vielen Fällen der unter Frage 1 abgefragten Taten konnten Tatverdächtige ermittelt werden?
- Frage 6 Welche Informationen liegen über die unter Frage 5 abgefragten Tatverdächtigen vor? Bitte insbesondere auf Alter, Staatsbürgerschaft und eventuell vorliegende Wohnsitze im Ausland eingehen.

Die Fragen 1 bis 6 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Der Begriff „Quishing“ ist ein von den Medien geprägter Begriff; Quishing oder QR-Phishing ist eine Cybersicherheitsbedrohung, bei der Angreifer QR-Codes verwenden, um Opfer auf eine schädliche Website umzuleiten oder zum Herunterladen schädlicher Inhalte aufzufordern. Diese Tatbegehungen werden in der Polizeilichen Kriminalstatistik (PKS) als Betrug erfasst. Eine gesonderte Erfassung und damit Recherche nach dem Begriff „Quishing“ ist in der PKS nicht möglich.

- Frage 7 Über welche Erkenntnisse verfügt die Landesregierung, dass es sich bei den in Hessen aufgetretenen Fällen von „Quishing“ um Erscheinungsformen der organisierten (Banden)kriminalität handelt?
- Frage 8 Liegen Erkenntnisse dahingehend vor, dass organisierte Banden aus dem Ausland für die Organisation dieser Betrugsdelikte verantwortlich zeichnen? Bitte bejahendenfalls darauf eingehen, aus welchen Ländern die Banden operieren.

Die Fragen 7 und 8 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.
Der Landesregierung liegen keine Erkenntnisse vor.

Frage 9 Welche Lösungsmöglichkeiten sieht die Landesregierung, um die Bezahlung stationär gebundener Dienstleistungen im öffentlichen Raum, wie etwa die Bezahlung von Parkgebühren, betrugssicher abwickeln zu können? Die Antwort bitte begründen.

Im Rahmen ihrer Kriminalprävention rät die hessische Polizei dazu:

- Scannen Sie keine QR-Codes aus unbekannten oder unzuverlässigen Quellen, beispielsweise auf Flyern, Schriftstücken sowie E-Mails.
- Stellen Sie sicher, dass der Absender wirklich vertrauenswürdig ist. Meist werden zur Tatbegehung die Namen bekannter Institutionen, Banken oder Sparkassen missbraucht.
- Prüfen Sie die URL auf verdächtige Zeichen oder falsche Domains.
- Vertrauen Sie nur QR-Codes die von offiziellen Quellen stammen, wie beispielsweise einer Unternehmens-Webseite.
- Nutzen Sie Sicherheitssoftware auf Ihrem Smartphone, welche schädliche Hyperlinks erkennt und blockiert. Halten Sie diese Anwendungen immer auf aktuellem Stand.
- Werden Sie skeptisch bei Zahlungsaufforderungen und scannen Sie keine Codes die auf direkte Zahlungen führen.
- Geben Sie nach dem Scannen eines QR-Codes keine sensiblen Daten, wie Passwörter oder Bankdaten ein, bevor Sie die Internetseite sorgfältig geprüft haben.

Bei Beachtung dieser Empfehlungen sinkt die Gefahr erheblich, Opfer von „Quishing“ zu werden.

Wiesbaden, 25. März 2025

Prof. Dr. Roman Poseck