MEIN Norddeutschland
NACHRICHTEN AG
30. Juni 2025

Polizei warnt: Gefälschte QR-Codes an Parkautomaten meiden!

Goslar informiert über aktuelle Risiken von gefälschten QR-Codes und Cyberkriminalität, insbesondere vor den Olympischen Spielen 2024.

Goslar, Deutschland - In den letzten Tagen macht ein neuer Betrugsfall von sich reden, der insbesondere in Norddeutschland für Unruhe sorgt. Die Polizei warnt vor gefälschten QR-Codes, die an Parkautomaten angebracht worden sind. Diese Masche, die als ȣQuishingȣ bezeichnet wird, nutzt die unbedachte Nutzung von QR-Codes aus, um ahnungslose Nutzer zu finanziellen Verlusten zu führen. Datenschützer und IT-Experten empfehlen, ganz besonders aufmerksam zu sein, wenn QR-Codes gescannt werden, da diese in verschiedenen öffentlichen Bereichen als verlockende Möglichkeit präsentiert werden.

Wie die Golem.de berichtet, ist Quishing eine Cyberkriminalitätsform, bei der gefälschte QR-Codes von

Betrügern genutzt werden, um sensible persönliche Daten und Zahlungsinformationen zu stehlen. Besonders an stark frequentierten Orten wie Parkplätzen kann dies für Ungeübte zum finanziellen Stolperstein werden. Dabei werden oft QR-Codes verwendet, die legitime Dienstleistungen imitieren, um ahnungslose Nutzer auf Phishing-Webseiten zu locken.

Wie funktioniert Quishing?

Betrüger platzieren gefälschte QR-Codes einfach neben den originalen, und wenn jemand diesen scannt, landet er auf einer gefälschten Webseite. Diese könnte beispielsweise eine gefälschte Zahlungsmöglichkeit bieten, wo die eingegebenen Kreditkartendaten abgegriffen werden. Die Gefahren dieser Masche nehmen zu, je höher die Frequenz von Besucherströmen ist.

Sicherheitsmaßnahmen, die gegen Quishing helfen können, sind unter anderem:

- Die URL vor dem Scannen des QR-Codes genau prüfen.
- QR-Code-Scanner zu verwenden, die eine URL-Vorschau anzeigen.
- Immer die URL manuell in den Browser einzugeben, anstatt den QR-Code zu scannen.
- Auf SSL-Zertifikate zu achten (d.h. sichere Seiten beginnen mit ȝhttpsȝ und zeigen ein Schloss-Symbol).
- Über Links und Domains mit Tools wie dem F-Secure Link Checker zu überprüfen.
- Bewertungen von Online-Shops in vertrauenswürdigen Bewertungsportalen zu prüfen.
- Sicherheits-Apps zu nutzen, um potenzielle Bedrohungen zu erkennen und zu blockieren.

Gefahren bei Großveranstaltungen

Die Bedrohung durch gefälschte QR-Codes ist nicht nur lokal zu finden. Anlässlich der bevorstehenden Olympischen Spiele 2024

in Paris wurde bereits eine Vielzahl von gefälschten Domains registriert. Fast 200 dieser ȝFake-Webseitenȝ haben mit Namen wie ȝparisolympics2024.storeȝ oder ȝshop-olympics.shopȝ legitime Konkurrenz in den Suchergebnissen nachgeahmt. Nutzer, die dort Souvenirs oder Tickets kaufen wollten, gaben unwissentlich auch ihre Kreditkartendaten preis, was für viele in einem bösen Erwachen endete. Security-Insider beschreibt die gestiegene Gefahr insbesondere während solcher Großveranstaltungen, wo das Interesse zu groß und die Vorsicht oftmals nicht gegeben ist.

Umso wichtiger ist es, die eigene Online-Sicherheit im Blick zu haben. Wer QR-Codes scannt, sollte dies immer mit einem gesunden Misstrauen tun und sicherstellen, dass die dargestellte URL vertrauenswürdig ist.

Es liegt an uns, aufmerksam und informiert zu bleiben ج gerade in einer Zeit, in der die digitale Welt voller Risiken steckt. Die Polizei und Cybersecurity-Expert:innen raten unbedingt dazu, sich vor der Nutzung von QR-Codes genau zu informieren und im Zweifelsfall besser auf die gute alte manuelle Eingabe zu setzen.

Details	
Ort	Goslar, Deutschland
Quellen	• www.golem.de • der-markt.net • www.security-insider.de

Besuchen Sie uns auf: die-nachrichten.com