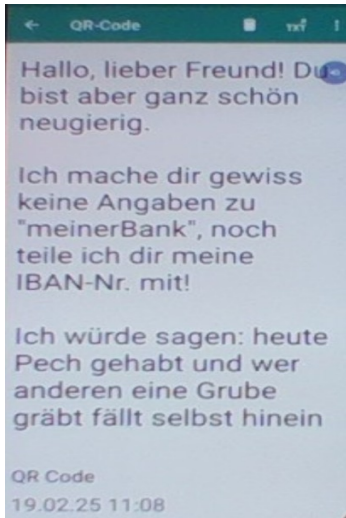


Per Post zum Betrugsversuch **niemals** QR-Code abscannen



Gefälschte Strafzettel: Polizei warnt vor falschen QR-Codes



Gefährlich wird es auch für Falschparker: Polizei/Ordnungsamt setzen immer häufiger QR-Codes auf Strafzetteln ein, um **Bürgern die Bezahlung des Bußgeldes zu erleichtern?**

Dies ist kein Ersatz für einen Bußgeldbescheid!

Betrüger haben dies sofort in der Vergangenheit ausgenutzt und z.B. **gefälschte Strafzettel mit „QR-Codes“** an der Windschutzscheibe des Autos angebracht. **Vorsicht:** Gefälschte **QR-Codes auch an Ladesäulen**, oder postalisch versandte Schreiben **der „Commerzbank“ mit QR-Code! Sie werden damit nur betrogen.**

In einen QR-Code passen **7089 Zahlen und 4296 Buchstaben:** Und damit lassen sich in Kombination viele Betrügereien bewerkstelligen.

Deshalb, Vorsicht beim Abscannen des Codes der „Commerzbank“! Nie darauf reagieren!

Oder telefonische Rückfrage bei Ihrer Bank

Schauen Sie was man damit alles machen kann. Rufen Sie den QR-Code einmal auf.

Beileigender QR-Code ist Test, nur ein Muster

16.04.25

Bußgeldbescheid per QR-Code

Ein Bußgeldbescheid, der nur über einen QR-Code auf einer Postkarte ohne Adressaten zugestellt wird, wäre in Deutschland **rechtlich unzulässig**. Hier sind die wesentlichen Gründe:

Formvorschriften des Bußgeldbescheids:

Ein Bußgeldbescheid muss nach § 66 des **Ordnungswidrigkeitengesetzes (OWiG)** zwingend bestimmte Angaben enthalten, darunter:

Den **Betroffenen namentlich benennen**

Die **Tatbezeichnung**

Die **Rechtsgrundlage**

Die **Beweismittel**

Die **Rechtsbehelfsbelehrung**

Ein QR-Code alleine ersetzt diese Angaben nicht und erfüllt die gesetzlichen Anforderungen nicht.

Zustellungs Vorschriften: Ein Bußgeldbescheid muss in Deutschland in der Regel **per Post mit Zustellungsnachweis** erfolgen (§ 51 OWiG i.V.m. §§ 3, 5 Verwaltungszustellungsgesetz).

Eine **Postkarte ohne Adressaten** wäre **kein sicherer Zustellweg** und könnte leicht verloren gehen oder von Unbefugten eingesehen werden, was **datenschutzrechtlich problematisch** wäre.

Datenschutz & Persönlichkeitsrechte:

Ein Bußgeldbescheid enthält **personenbezogene Daten** und unterliegt dem **Datenschutzrecht (DSGVO, BDSG)**.

Eine offene Postkarte ohne sicheren Briefumschlag wäre ein klarer **Verstoß gegen den Datenschutz**, da Dritte Zugang zu den Daten hätten.

Fazit

Ein Bußgeldbescheid nur per QR-Code auf einer Postkarte ohne Adressaten ist **nicht zulässig**. Sollte dir ein solcher Bescheid zugehen, kannst du **rechtliche Schritte einleiten**, insbesondere einen Einspruch einlegen und ggf. die Rechtswidrigkeit der Zustellung rügen.

Falsche QR-Codes auf Parkautomaten:

Auf Parkautomaten in Hannover wurden vor Kurzem gefälschte QR-Codes der Parkschein-App "EasyPark" entdeckt. Anscheinend sollten Bezahldaten von Nutzern entwendet werden. Die Polizei nahm vorübergehend drei Heranwachsende fest, die eine Rolle mit gefälschten QR-Code-Aufklebern bei sich trugen. Ihren Angaben zufolge hatten sie von „Mitarbeitern der Easy Park“ gegen Entlohnung für ihre Mithilfe zur „Berichtigung“ der „fehlerbehafteten QR-Codes“ durch Überkleben eine Entlohnung in Geld erhalten. Die Polizei Hannover stellte die gefälschten Rollen sicher. Anzeige gegen unbekannt wurde erstattet. Eine weitere Verfremdung durch Überkleben des ursprünglichen QR-Codes durch betrügerische neue Sticker konnte verhindert werden.

Vor neuer Betrugsmasche, bei der Täter über die originalen QR-Codes auf Automaten einen QR-Code klebten, der auf eine gefälschte EasyPark-Internetseite führte, wird gewarnt. Dort wurden die Nutzer laut Landeskriminalamt (LKA) aufgefordert, **neben der Parkzeit ihre Kreditkartendaten** einzugeben.



Vorsicht, Quishing! Virens Scanner erkennen keine QR-Codes !!



So gehen die Cyberkriminellen vor. In der neuen Variante des Quishings geht es angeblich um die regelmäßige Überprüfung der Identität eines Bankkunden aufgrund von EU-Vorschriften. Um dies so einfach wie möglich zu gestalten, soll man den auf dem Anschreiben abgebildeten QR-Code einscannen. Beim Online-Quishing wird in der Betreffzeile der E-Mails zum Beispiel auf ein Sicherheitsproblem hingewiesen, bei dem die Nutzer aktiv werden müssten. Das Ziel der Betrüger ist immer, dass die Nutzer den QR-Code auf ihrem Smartphone einscannen-

Tipps, um nicht auf Quishing hereinzufallen

Prüfen Sie sorgfältig, ob es sich bei der Mail oder dem Brief um eine Fälschung handeln könnte. Kontaktieren Sie den vermeintlichen Absender über offizielle Kanäle. Meist ist die angegebene Telefonnummer nicht geschaltet. Bei einem Post-Brief sollte man sicherheitshalber den persönlichen Bankberater anrufen und den Sachverhalt offiziell abklären. Der Empfänger eines solchen eMail bzw. Brief sollte bei der Polizei Anzeige erstatten und dabei das eingescannte oder originale Täterschreiben vorlegen. Wer darauf hereingefallen ist, sollte unverzüglich sein Kreditinstitut informieren und den Zugang sperren lassen. Hierfür kann auch der Sperrnotruf genutzt werden. +49 116 11

Angriffe über Tricks mit QR-Codes

Die Angriffe kommen per E-Mail und umgehen viele üblichen Sicherheitsscans. Liest man die eMails dann auch noch mit aktivierter HTML-Darstellung, wird man leicht zum Opfer.

QR-Codes sind bei Verbrechern beliebt, weil sich darin Hyperlinks kodieren lassen, die Menschen nicht lesen können. Damit lassen sich sehr leicht falsche Hyperlinks unterjubeln. Wird der Code einge-scant, landet man auf einer vom Angreifer kontrollierten Webseite und wird so zum **Ernten Ihrer Zugangsdaten** genutzt.

Separate Dateien ergeben zusammen ein Bild

Eine verblüffend einfache Methode besteht darin, einen irreführenden **QR-Code in zwei (oder mehr) Teile zu teilen**. Diese Bilddateien werden beispielsweise einer Phishing-eMail angehängt. Sicherheitssysteme versuchen in der Regel, die Bilddateien einzeln auszuwerten, finden in den einzelnen QR-Schnipseln aber nichts Verwertbares und lassen die gefährliche Nachricht passieren. **Mittels HTML** können die Bilder allerdings am Endgerät des Nutzers so angeordnet werden, dass sie optisch **wie ein einzelnes Bild** wirken.

Werden **zwei QR-Codes in einander zu verschachtelt**, kann Ihr Smartphone entscheiden wenn es lesen will.

ASCII-Code QR

Bereits im Oktober hat Barracuda über gefinkelte QR-Codes berichtet, die gar nicht als Bilddatei daherkommen, sondern aus ASCII-Codes zusammengesetzt sind, damit lassen sich Textgebilde erstellen, die von Smartphones als QR-Code erkannt werden

Angreifer profitieren mit QR-Codes von einem speziellen Vorteil: Sie lassen sich in der Regel nicht mit demselben Endgerät auswerten, auf dem sie angezeigt werden und man muss so in aller Regel zum Smartphone greifen.

Deshalb sind außerhalb geschlossener Systeme **QR-Codes grundsätzlich verdächtig** und mit einer gehörigen Portion Argwohn zu begegnen.

Mit postalisch zugestellten Briefen täuschen Betrüger Bankkunden über QR-Codes.

Im Kreis Böblingen erhielt ein 63-jähriger Bankkunde einen Brief mit stimmigem Briefkopf seiner „Bank“. Darin wurde er aufgefordert, seine Mobilgeräte für das Online-Banking neu einzurichten. **Der Brief wirkte echt und klang plausibel, sodass er den QR-Code scannte** und die Anweisungen mit eigens dazu erzeugten TAN's quittierte.

Dabei installierte er jedoch unbewusst ein Gerät der Betrüger. Diese transferierten damit Geld vom Tagesgeld- auf sein Girokonto und buchten anschließend zweimal jeweils knapp 10.000 Euro ab.

01.06.2025

Mit Tageslimit wäre das nicht möglich gewesen. Zur Änderung des Limits ist hier das Passwort erforderlich