**Vorsicht Quishing – neue Masche bei uns**

 Was ist Quishing?

QR-Codes stellen komplexe Informationen verkürzt dar. Somit können diese rasch abgerufen werden.

**Quishing** ist eine Betrugsmasche, bei der Betrüger QR-Codes manipulieren, um an Ihre Kreditkarteninformationen und Kontodaten zu kommen.

 Betrüger überkleben die echten QR-Codes mit gefälschten, die auf täuschend echte Webseiten führen. Das kann z. B. an Ladestationen für E-Autos sein oder an Parkautomaten.  
Wer dann per QR-Code bezahlen will, gibt so die Kontodaten weiter.

**Tipps der Polizei:**

**Internetadresse prüfen – ist die Website gefälscht?**Scannen Sie den QR-Code nicht ungeprüft, wenn Sie Kontodaten eingeben sollen. Prüfen Sie unbedingt die Internetadresse: handelt es sich wirklich um Ihre Hausbank?

* **Inhalte nicht automatisch öffnen:**Schalten Sie, soweit es geht, die Funktion für ein sofortiges Öffnen eines gelesenen QR-Codes ab.   
  Denkbar ist auch, dass Malware heruntergeladen wird.  
  Manche QR-Code-Scanner zeigen den Link an:   
  Liegt die Quelle im Ausland, kann das ein Indiz auf einen „betrügerischen“ QR-Code sein?   
  Überprüfen Sie in jedem Fall die Link-Adresse.

·        **QR-Code überklebt:**Ist der QR-Code an einer Ladesäule möglicherweise überklebt, scannen Sie ihn nicht.   
Verfügt zum Beispiel eine Ladesäule über ein Display, sollte der Code, wenn möglich, von dort gescannt werden.

Mit dem QR-Code kann Ihnen ähnliches in zugesandten Bank-Briefen passieren:

* **Bank kontaktieren:**Haben Sie Zweifel, dass der Brief der Bank und QR-Code darauf echt sind, nutzen Sie nicht die auf dem Brief angegebenen Kontaktmöglichkeiten, sondern suchen Sie die Kontaktdaten selbst und sprechen Sie persönlich mit dem Ihnen bekannten Bankmitarbeiter. Scannen Sie keine QR-Codes, die in Mails von unbekannten oder dubiosen Absendern dargestellt werden.
* **Allgemeine Formulierungen:**Seien Sie vorsichtig, wenn in einem Brief eine allgemeine Anrede ("Sehr geehrte Kontoinhaberin, sehr geehrter Kontoinhaber") verwendet wird.  
  Geben Sie generell niemals vertrauliche Informationen wie Passwörter oder Bankdaten an unbekannte Absender weiter.
* Aktualisieren Sie regelmäßig Ihre Sicherheitseinstellungen, um Ihren Schutz vor Quishing-Attacken zu verbessern.