# Vorsicht, Quishing!

**QR-Codes sind praktische Helfer in der digitalen Welt und werden deshalb gerne und oft arglos gescannt. Das machen sich Kriminelle zunutze und verstecken Phishing-Webseiten und Schadsoftware hinter der harmlosen Fassade. Aktuell landen die heimtückischen Codes sogar im Briefkasten. So können sich Verbraucher schützen.**

Das Menü eines Restaurants, Informationen zum Bahnfahrplan oder Zahlungsinformationen zu einer Rechnung: Ganz selbstverständlich trifft man im Alltag den „Quick Response“-Code an (auf Deutsch: „schnelle Antwort“), besser bekannt als QR-Code. Mit den gemusterten Quadraten lassen sich vielfältige Informationen verpacken und beispielsweise komfortabel mit dem Smartphone abrufen. Der Code wird mittels Kamera oder spezieller App gescannt, das Gerät erkennt die gespeicherte Adresse der Webseite und öffnet bei Bestätigung einen Link oder lädt eine Datei. Beim Scannen ist jedoch Vorsicht geboten: „Auch Betrüger erzeugen QR-Codes für sogenannte Phishing-Angriffe. Diese haben das Ziel, sensible Informationen – etwa die Zugangsdaten für das Online-Banking – zu erbeuten“, sagt Michael Schwab von der Postbank. „Quishing“ nennt sich diese Masche – eine Wortneuschöpfung, die sich aus „QR“ und „Phishing“ zusammensetzt.

**Tückische Post**

Bevorzugt versenden Kriminelle die QR-Codes per E-Mail, verbunden mit der dringenden Aufforderung, den Code umgehend zu scannen – zum Beispiel, um das Bankkonto zu sichern und sich erneut zu authentifizieren. Der Code führt jedoch auf eine gefälschte Webseite und die vom Nutzer eingegebenen Informationen landen direkt bei den Cyberkriminellen. „Manchmal kann ein einziger Besuch auf einer kriminellen Webseite ausreichen, um den Computer mit Schadsoftware zu infizieren“, warnt der Postbank Experte. Ein kritischer Blick auf den Absender der E-Mail kann eine betrügerische Nachricht leicht enttarnen. Phishing-Mails täuschen den Namen eines seriösen Absenders vor, die Adresse ist aber fehlerhaft – hat zusätzliche Satzzeichen, Buchstabendreher oder eine andere Länderkennung. Deshalb haben Betrüger ihre Masche weiterentwickelt: Sie verschicken seit einigen Monaten immer wieder Briefe per Post, die angeblich von der Hausbank stammen. Das Schreiben enthält einen QR-Code, mit dem der Kunde einen „Aktualisierungsprozess“ durchführen soll. Folgt er den Anweisungen, landet er auf einer gefälschten Webseite.

**Im Zweifel nicht scannen**

„Zwar zeigen Foto-Apps und QR-Scanner in der Regel die Internetadresse vor Aufrufen der Webseite an. Erst wenn man darauf tippt, wird die Seite geöffnet. Die meisten Vorschauen stellen allerdings eine Kurzform der Adresse dar, sodass man sie nur unzureichend prüfen kann“, sagt Michael Schwab. Daher sollte man im Zweifel den QR-Code nicht scannen. Wer den Verdacht hat, Opfer eines Angriffs geworden zu sein, sollte umgehend handeln und die wichtigsten Passwörter ändern, etwa fürs Online-Banking und den E-Mail-Account – allerdings von einem anderen Endgerät. Zudem sollten Betroffene den Vorfall der Polizei melden und ihre Bank kontaktieren.

Quelle: Postbank Mediendienst 4/24

**Bild:**

Ein Bild, das Handy, tragbares Kommunikationsgerät, Kommunikationsgerät, mobiles Gerät enthält.

Automatisch generierte Beschreibung

Foto: 1734 Postbank / © Antonio Gravante