Quishing: Der Code, der keiner ist - ARAG IT-Experten informieren über eine neue digitale Betrugsmasche mit QR-Codes

Wirtschaft Finanzen Versicherung News © Pixabay

Ob als Nachricht von der Bank, als Zahlmöglichkeit an der E-Ladesäule oder als Strafzettel für falsches Parken – sie sehen aus wie normale QR-Codes, doch es steckt Betrug hinter diesen kleinen Quadraten und nennt sich Quishing. Betrüger nutzen diese falschen Codes, um an persönliche Daten und sogar Geld zu gelangen. Wie diese neue Betrugsmasche funktioniert, wie man sie erkennt und wie man sich schützen kann, wissen die ARAG IT-Experten.

Was ist Quishing und wie funktioniert es?
Quishing ist ein Kofferwort aus „QR-Code“ und „Phishing“. QR steht für „Quick Response“, auf Deutsch „Schnelle Antwort“. „Phising“ ist ein Kunstwort, zusammengesetzt aus „Passwort“ und dem englischen Wort „Fishing“ (deutsch für „Fischen“). Im übertragenen Sinne meint Quishing also das Fischen nach Passwörtern mittels QR-Code. Ein QR-Code besteht aus vielen kleinen Quadraten, die Informationen, meist eine Internet-Adresse, enthalten. Mit einem Smartphone gescannt, öffnet sich die zugehörige Webseite. Doch hier liegt die Tücke: Nicht alle Smartphones zeigen den Inhalt des QR-Codes an, bevor sie die Webseite öffnen. Einige Geräte leiten Nutzer direkt weiter, ohne zuvor die Adresse der Internetseite anzuzeigen. Gerade dies machen sich Kriminelle zunutze, indem sie ihre eigenen betrügerischen QR-Codes so platzieren, dass sie auf gefälschte Webseiten führen. Dort versuchen sie, sensible Daten abzufangen oder sogar direkte Geldtransfers zu veranlassen.

Quishing-Betrug im Alltag
Die ARAG IT-Experten warnen vor Briefen oder E-Mails von Banken, in denen beispielsweise zur Aktualisierung des photoTAN-Verfahrens aufgefordert wird. Diese gefälschten Nachrichten enthalten einen QR-Code, der jedoch auf eine von Kriminellen betriebene Webseite führt. Von den meisten Virenscannern wird der Code nur als Bild erkannt, so dass betrügerische Mails als ungefährlich eingestuft werden und im Postfach landen. Die echte Bank hat mit dem Schreiben bzw. der Mail nichts zu tun. In der Regel sind diese Fake-Nachrichten nicht personalisiert, sondern sprechen den Kontoinhaber im Allgemeinen an.

Auch vor manipulierten QR-Codes an Ladesäulen für Elektro-Autos warnen die ARAG IT-Experten.

Hier werden gefälschte QR-Codes über die Original-Codes der Anbieter geklebt. Diese Codes sollten eigentlich zur Bezahlung des Ladevorgangs führen, leiten jedoch ebenfalls direkt auf die Internetseiten der Kriminellen.
Eine weitere Quishing-Betrugsmasche wartet an geparkten Fahrzeugen: Dabei werden falsche Strafzettel mit QR-Codes unter die Scheibenwischer parkender Autos geklemmt. Autofahrer sollten hier besonders vorsichtig sein und den vermeintlichen Strafzettel bei der Polizei überprüfen lassen, bevor sie die Strafe bezahlen.

Wie kann man sich vor Quishing schützen?
Die ARAG IT-Experten raten, QR-Codes nur dann zu scannen, wenn man ihre Herkunft kennt und ihnen vertraut. Die Kamera-App des Smartphones sollte nur genutzt werden, wenn diese die gescannte Internetadresse vor dem Öffnen der Seite anzeigt. So können Nutzer die Webseite prüfen, bevor sie auf sie zugreifen. Bei ungewöhnlichen Briefen oder Mails raten die ARAG IT-Experten zur Vorsicht, vor allem, wenn die Nachrichten einen QR-Code enthalten, der den Empfängern suspekt erscheint. Ist dies der Fall, sollte man vor dem Scannen des Codes den Absender recherchieren. Am besten ruft man den Absender direkt an – aber nicht über die im Brief oder in der Mail angegebene Telefonnummer, sondern über die offiziellen Kontaktdaten des Unternehmens.

Nutzer von E-Ladesäulen sollten genau überprüfen, ob der QR-Code an der Säule überklebt wurde. Bestehen Zweifel, sollte man stattdessen andere Zahlungsmethoden wie z. B. eine App oder eine Ladekarte nutzen.

Darüber hinaus raten die ARAG IT-Experten, im Betrugsfall schnell zu handeln und sich sofort an die Polizei zu wenden. Wer bereits Geld überwiesen hat, sollte umgehend seine Bank informieren oder den Sperr-Notruf unter 116 116 anrufen, um weiteren Schaden zu verhindern.

Kann man Quishing-Betrug absichern?
Einige Cyberversicherungen decken solche Betrugsmaschen in der Tat ab. Dann gilt Quishing als eine Unterform des Phishings, das in vielen Policen abgesichert ist. Es lohnt sich also, den Versicherungsschutz genau zu prüfen. Sollte man durch einen Quishing-Betrug persönliche Daten verlieren, greift bei einigen Anbietern der Schutz gegen Identitätsmissbrauch. Doch bei Fällen, in denen der Geschädigte selbst Geld überweist – etwa bei gefälschten Strafzetteln –, besteht laut ARAG IT-Experten in der Regel kein Versicherungsschutz.