Gefälschte Briefe von Finanzinstituten

Immer wieder sind betrügerische Briefe im Umlauf, die täuschend echt wirken und angeblich von Ihrer Bank stammen. Doch die Fälschungen lassen sich entlarven.

Wichtigste Merkpunkte:

- Nutzen Sie für das E-Banking immer die offizielle Website oder die Mobile Banking App Ihres Finanzinstituts.
- Überprüfen Sie die Echtheit postalisch erhaltener Schreiben – genauso wie bei elektronischen Nachrichten –, und melden Sie verdächtige Briefe Ihrem Finanzinstitut.
- Prüfen Sie die Internetadresse von mit der Kamera eingelesenen QR-Codes, bevor Sie dem Link folgen.

Betrügerinnen und Betrüger geben sich grosse Mühe, gefälschte Briefe so authentisch wie möglich zu gestalten, inklusive korrekt wirkendem Logo und professionellem Layout. Ihr Ziel: Sensible Informationen oder Zugangsdaten der nichts ahnenden Opfer erlangen, um sich damit beispielsweise in deren E-Banking unrechtmässig zu bereichern.

Typisches Szenario: Ein QR-Code im Brief führt zu einer gefälschten Website, die wie die Anmeldeseite Ihres E-Bankings aussieht. Dort werden Sie aufgefordert, sensible Informationen wie Ihre Login-Daten einzugeben. Damit verschaffen sich die Kriminellen Zugang zu Ihren Konten.

Das Vorgehen entspricht dem des klassischen Phishing (https://www.ebas.ch/phishing) , mit dem Unterschied, dass anstelle einer elektronischen Nachricht (wie E-Mail, SMS oder Messenger-Post) ein physisches Schriftstück verschickt wird. Oft wird auch Druck auf das Opfer ausgeübt, etwa indem vorgegeben wird, das Konto würde gesperrt, falls die angeblich erforderliche Aktion nicht innerhalb kurzer Zeit durchgeführt wird.

Die Verwendung von QR-Codes bietet aus Angreifersicht den Vorteil, dass das Opfer nicht auf Anhieb erkennt, was für eine Internetadresse sich hinter dem im Mosaik-Bild kodierten Link verbirgt. Denn andernfalls wäre die Fälschung auf den ersten Blick als solche erkennbar.

Dem Schwindel kommen Sie auf die Spur, indem Sie nach dem Einlesen des QR-Codes mit der mobilen Kamera die angezeigte Internetadresse überprüfen, bevor Sie sich zur Website weiterleiten lassen. Oder noch besser, indem Sie die Internetadresse Ihres Finanzinstituts immer von Hand in die Adresszeile Ihres Browsers eintippen oder die Mobile Banking App selber starten – denn so gelangen Sie mit Sicherheit zum echten E-Banking Ihrer Bank.

Kriminelle fälschen Schriftdokumente seriöser Unternehmen wie etwa von Finanzinstituten, oft sehr authentisch. Die Briefe fordern Endkunden auf, sicherheitsrelevante Aktionen durchzuführen. Damit wollen die Betrüger an sensible Informationen oder Zugangsdaten der Opfer gelangen.