Abzocke per Post

Finanztipp. Ein Brief, der scheinbar von der Hausbank kommt. Logo, Layout, Papier – alles wirkt vertraut. Unten im Brief ist ein QR-Code abgedruckt. Dieser soll zwecks Bestätigung gescannt werden. Geht schnell – und kann sehr teuer werden!

Autor: Bettina Blaß

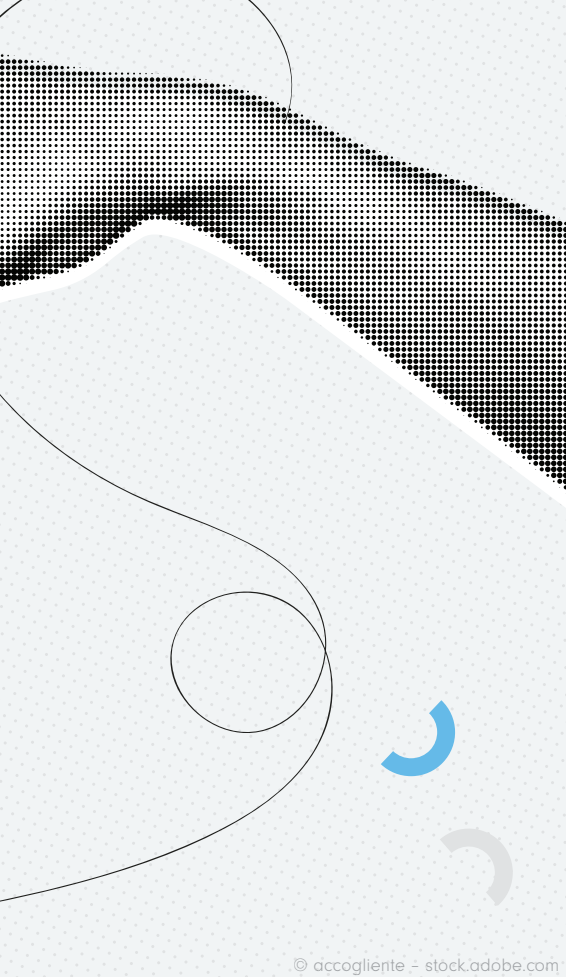
Bei E-Mails oder SMS schauen viele genauer hin. Phishing ist schließlich allgegenwärtig. Kriminelle nutzen jedoch neuerdings auch den Postweg. Ihre Schreiben sehen offiziell aus, tragen bekannte Banklogos und werden vom Briefträger zugestellt. Hinzu kommt: Der Aufwand, einen Brief zu verschicken, ist höher als bei E-Mails oder SMS: Druck, Papier und Versand kosten Geld. Das verleiht den Briefen eine nicht zu unterschätzende Glaubwürdigkeit. Darum warnen sowohl die Polizei als auch Verbraucherschützer vor dieser Methode.

Denn wer den Brief ernst nimmt, kann viel Geld verlieren. In Anlehnung an einen QR-Code heißt der Betrug Quishing. Diese Bezeichnung verdeutlicht auch, dass es eine Verbindung zu Phishing und Smishing gibt, also dem Abgreifen von Bankdaten per Mail und SMS. Die veränderte Masche lebt davon, dass QR-Codes im Alltag inzwischen selbstverständlich geworden sind und selten kritisch hinterfragt werden.

Wer einen QR-Code und eine Link-Vorschau angezeigt bekommt, kann eventuell einen ersten Hinweis auf das Scanz-Ziel bekommen. Dazu muss man aber sehr genau hinschauen. Die Verbraucherzentrale rät: „Achten Sie bei einer Internet-Adresse genau auf die Satzzeichen.“ Laute die Adresse „beispiel.de/123“ führe sie tatsächlich auf eine Unterseite des Auftritts „Beispiel.de“. Die Schreibweise „beispiel.de-123.com“ hingegen führt auf eine Unterseite des Auftritts „de-123.com“. Unterseiten sind üblicherweise mit einem Schrägstrich nach der Länderkennung aufgeführt oder durch einen Punkt von der eigentlichen Adresse getrennt.

Hinweise auf Betrug

Auch im Brieftext gibt es häufig noch Hinweise darauf, dass der Absender gefälscht sein könnte. „Sehr geehrte Kontoinhaberin, sehr geehrter Kontoinhaber“ ist zum Beispiel eine eher ungewöhnliche Anrede in einem postalisch zugestellten Brief. Auch wenn von „bedeutenden Änderungen im Zahlungsverkehr“ die Rede ist, ohne konkret zu sagen, worum es geht, sollte man aufpassen. Klar ist jedoch auch, dass man mithilfe von Künstlicher Intelligenz solche Texte optimieren kann, weshalb es nur eine Frage der Zeit ist, bis die Texte von Betrügern perfekt wirken werden.



Ein weiteres Warnsignal ist der Tonfall. Aufforderungen wie „bitte sofort handeln“ oder die Androhung einer Zugangssperrung setzen die Adressaten gezielt unter Druck. Seriöse Banken arbeiten üblicherweise mit klaren und eher längeren Fristen.

Zusätzlich nutzen Betrüger laut Landeskriminalamt Niedersachsen gerne aktuelle Änderungen im Bankverkehr, um ihre Briefe zu verschicken. Im Oktober 2025 war ein Anlass der neu eingeführte IBAN-Abgleich, bei dem bei Überweisungen der eingegebene Name mit der zugehörigen IBAN abgeglichen wird.

Der Ablauf

Wird der im Brief abgedruckte QR-Code nun mit dem Smartphone gescannt, führt er auf eine täuschend echt gestaltete Internetseite. Dort werden die Bankzugangsdaten abgefragt, die auf diesem Weg unmittelbar bei den Betrügern landen. Die Polizei warnt auf der Internetseite des Landeskriminalamts Niedersachsen ausdrücklich: „Auf keinen Fall sollten der aufgedruckte QR-Code gescannt und auf den dadurch erscheinenden Phishingseiten sensible Daten eingegeben werden.“ Auf der Internetseite hat das Landeskriminalamt auch Abzockbriefe veröffentlicht, die scheinbar im Namen von apobank, ING Bank oder Volksbanken Raiffeisenbanken verschickt worden sind.

Quishing beschränkt sich jedoch nicht nur auf den Bankensektor. Die Verbraucherzentrale warnt auch vor QR-Codes auf Plakaten im öffentlichen Nahverkehr, Strafzetteln, Parkscheinautomaten, Ladesäulen für E-Autos. Teilweise werden auch echte Codes überklebt oder manipuliert. Ziel ist immer dasselbe: Nutzer auf gefälschte Websites zu locken, um dort Daten oder Geld abzugreifen.

Was tun?

Wer einen Brief bekommt, der ihm merkwürdig erscheint, sollte beim Absender nachfragen. Sind bereits Daten preisgegeben worden, sollte man sofort seine Bank kontaktieren und eine Anzeige bei der Polizei aufgeben. ■