Achtung vor Quishing: So schützen Sie sich vor gefälschten Bankbriefen!

Immer mehr Deutsche erhalten gefälschte Briefe, die über QR-Codes persönliche Daten abgreifen wollen. Experten warnen vor der Betrugsmasche „Quishing“.

Die Welt des digitalen Betrugs zeigt sich einmal mehr in einem beunruhigenden Licht, als immer mehr Menschen in Deutschland mit gefälschten Dokumenten konfrontiert werden. In einem bemerkenswerten Vorfall berichtete ein Unternehmer namens Mirko Lange von einem manipulierten Brief, der versuchte, ihn in eine Falle zu locken. Auf den ersten Blick schien alles legitim, doch bekannte Details und das sagende Fehlen einer Kundenbeziehung zur Commerzbank weckten seine Skepsis. Lange hatte Glück, doch die Methode, die hinter diesem Versuch steckte, ist besorgniserregend.

Am 27. August erhielt Lange einen Brief, angeblich von der Commerzbank. Darin wurde er aufgefordert, sein Photo-TAN-Verfahren zu aktualisieren, verbunden mit dem scannen eines QR-Codes. „Boah, das ist ja krass“, dachte Lange, als er den Brief las. Der Absender wirkte vertrauenswürdig, und selbst das Porto von 85 Cent ließ keinen Verdacht aufkommen. Erst die Erkenntnis, dass er nicht einmal Kunde dieser Bank ist, brachte ihn auf die richtige Spur.

Betrugsmasche „Quishing“ aufgedeckt

Die Betrugsmasche, mit der sowohl Lange als auch viele andere in Deutschland konfrontiert wurden, trägt den Namen „Quishing“. Dabei handelt es sich um einen raffinierten Trick, bei

dem Kriminelle versuchen, persönliche Informationen der Opfer über gefälschte QR-Codes zu erlangen. Die Gefahr, die von dieser Methode ausgeht, ist nicht zu unterschätzen. Laut dem Landeskriminalamt Nordrhein-Westfalen (LKA NRW) informieren solche Briefe nicht nur über angebliche Kontoinformationen, sondern zielen gezielt darauf ab, sensible Daten zu stehlen.

Lange erreichte die betrügerische Nachricht in München, wo auch das Bayerische LKA von solchen Fällen Kenntnis hat. In einem Kommentar an BuzzFeed News Deutschland bestätigte eine Sprecherin des LKA, dass man in stetigem Austausch mit den zuständigen Behörden in Nordrhein-Westfalen steht.

Um sich vor dieser Betrugsmasche zu wappnen, rät das LKA NRW, bei solchen Mitteilungen stets wachsam zu sein. Es ist wichtig, die Echtheit des Absenders stets zu überprüfen und QR-Codes nur zu scannen, wenn ihre Herkunft vollkommen klar ist. Außerdem sollten sicherere Methoden zur Bestätigung von Banken und anderen Institutionen verwendet werden, wie beispielsweise die Multi-Faktor-Authentifizierung beim Online-Banking.

Anzeichen erkennen und Schutzmaßnahmen ergreifen

Für Lange waren die Anzeichen eines Betrugs zwar verborgen, aber nicht unerkannt. „Ich hatte einen Verdacht, aber konnte es nicht glauben“, berichtete er. Nachdem er die Namen der Absender überprüfte, stellte er fest, dass die angebliche Unterschrift von Arno Walter stammte, der die Commerzbank vor mehr als einem Jahr verlassen hatte. Solche Entdeckungen sind entscheidend, um die echte Identität der Absender zu verifizieren.

Die Commerzbank selbst bestätigte, dass sie von diesen Phishing-Attacken Kenntnis hat und aktiv daran arbeitet, die Verbreitung von Phishing-Versuchen zu unterbinden. „Naturgemäß tragen wir keine Schuld“, sagte eine Sprecherin

der Bank in einer Mitteilung, in der die Kooperationsmaßnahmen gegen die Täter erklärt wurden. Lange warnte auf LinkedIn und bezeichnete die neue QR-Code-Betrugsmasche als „unfassbar und gruselig“. Die Welle solcher Betrugsversuche zeigt, dass die Technologie, die unser Leben erleichtert, auch anfällig für Missbrauch ist.

Olaf Classen, ein Experte für Informationssicherheit, erklärt, dass die Methoden der Betrüger sehr viel ausgeklügelter werden. „Leider geht das Thema noch viel weiter“, sagt Classen und zitiert Beispiele aus anderen Ländern, in denen QR-Codes an Tankstellen manipuliert wurden. Diese Art des Betrugs ist ein Trend, der sich schnell ausbreiten könnte, denn QR-Codes sind heutzutage allgegenwärtig, sei es beim Bezahlen an Parkautomaten oder im Marketing.

Classen warnt, dass der Großteil der Bevölkerung mit der Masche des „Quishings“ noch nicht vertraut ist. Viele Menschen sind sich der potenziellen Gefahren nicht bewusst und könnten einfach versuchen, einen QR-Code zu scannen, ohne darüber nachzudenken, ob er echt oder gefälscht ist. Die Anzeichen für Betrug sind oft sehr subtil.

Mit der zunehmenden Digitalisierung sind die Verbraucher mehr denn je gefordert, die Augen offen zu halten. Die Botschaft ist klar: Seien Sie vorsichtig und hinterfragen Sie stets die Echtheit der Informationen, die Ihnen zugestellt werden. Nutzen Sie Technologien wie QR-Codes mit Bedacht. Das Bewusstsein für diese neue Form des digitalen Betrugs wird entscheidend sein, um weitere Opfer zu verhindern.

Details

Besuchen Sie uns auf: n-ag.de