NACHRICHTEN AG

27. August 2024

Vorsicht vor Betrug: Gefälschte Bankschreiben mit QR-Codes im Umlauf

Betrüger verschicken gefälschte Bankbriefe mit QR-Codes. Seien Sie vorsichtig und prüfen Sie immer die Links!

Hannover (dpa/tmn) – In einer besorgniserregenden Entwicklung warnen verschiedene Behörden vor der Gefährlichkeit manipulierte QR-Codes darstellen können. Aktuell versenden Betrüger gefälschte Schreiben, die vorgeben, von deutschen Banken zu stammen. Diese Briefe enthalten QR-Codes, die auf gefälschte Webseiten führen und ahnungslose Nutzer dazu bringen sollen, sensible Daten preiszugeben. Das Landeskriminalamt Niedersachsen schlägt Alarm und rät zur äußersten Vorsicht.

Ein schnelles Scannen eines QR-Codes kann weitreichende Folgen haben. Die Drahtzieher hinter solchen Betrugsmaschen nutzen die Brieferstellung, um mit einer vermeintlich seriösen Kommunikation Vertrauen zu erwecken. In diesen gefälschten Schreiben wird oft die „Notwendigkeit“ betont, die Identität im Rahmen von EU-Vorschriften zu überprüfen. Eine solche Taktik spielt subtil auf das Sicherheitsbewusstsein der Bürger an und nutzt es aus, um private Informationen zu stehlen.

Wie man sich schützt

Im Falle von Unsicherheiten über die Echtheit der erhaltenen Briefe empfiehlt das LKA, sich direkt telefonisch an die eigene Bank zu wenden. Dabei sollte jedoch darauf geachtet werden, die Telefonnummer von der offiziellen Webseite der Bank zu beziehen und nicht aus dem verdächtigen Schreiben zu

entnehmen, um nicht in die Falle der Betrüger zu tappen.

Diese neue Betrugswelle ist nicht einzigartig. QR-Codes sind in der Vergangenheit bereits mehrmals mit Gaunereien in Verbindung gebracht worden, beispielsweise brillierten Betrüger mit Aufklebern, die an E-Auto-Ladesäulen angebracht waren. Auch in Werbe-E-Mails sind gefälschte QR-Codes kein seltenes Phänomen mehr. Die Masche wird zunehmend variabler und kreativer, wodurch es für den Durchschnittsnutzer immer schwieriger wird, Betrug zu erkennen.

Die Gefahren von Quishing

QR-Codes, die bei verschiedenen Angriffen verwendet werden, zielen nicht nur auf Onlinebanking-Zugangsdaten ab. Diese Phishing-Technik, allgemein als „Quishing“ bekannt, kann eine Vielzahl von Informationen abgreifen. Das können Anmeldedaten für unterschiedliche Online-Dienste oder sogar die unauffällige Installation von Schadsoftware auf den Smartphones der Benutzer sein. Es ist alarmierend, dass QR-Codes, die oft als praktisch und hilfreich wahrgenommen werden, auch als Vector für böswillige Aktivitäten missbraucht werden können.

Die Verbraucher müssen stets wachsam sein, nicht nur gegenüber digitalem Phishing aber auch in der physischen Welt. Eine einfache Regel lautet: QR-Codes können überklebt oder manipuliert werden. Selbst wenn ein QR-Code im realen Leben erscheint, sollte man stets kritisch bleiben.

Um sich effektiv zu schützen, gibt es einige Maßnahmen, die Verbraucher beachten sollten:

- Aktivieren Sie die Einstellungen Ihres Smartphones so, dass beim Scannen von QR-Codes der Link nicht sofort geöffnet wird. Viele moderne Scanner zeigen erstmal nur eine Vorschau des Links an, bevor sie auf die tatsächliche Webseite weiterleiten.

- Überprüfen Sie den Link sorgfältig, bevor Sie ihn anklicken. Stimmt die angezeigte URL mit dem überein, was Sie erwarten? Gibt es Tippfehler oder verdächtige Zeichen?
- Seien Sie misstrauisch gegenüber verkürzten Links. Diese können oft die tatsächliche Adresse verschleiern und eine zusätzliche Sicherheitslücke darstellen.

Die Fähigkeit, QR-Codes so einfach zu scannen und darauf zuzugreifen, bringt Verantwortung mit sich. Verbraucher sollten die Anfälligkeit dieser Technologie nicht unterschätzen und stets auf der Hut sein, um nicht Opfer von kriminellen Machenschaften zu werden.

Technologie mit Verantwortung nutzen

Der Umgang mit QR-Codes verlangt ein Bewusstsein für potenzielle Gefahren. In einer Welt, die zunehmend digitalisiert wird, ist es wichtig, informierte Entscheidungen zu treffen und skeptisch gegenüber Informationen zu sein, die auf den ersten Blick echt erscheinen. Die Implementierung von präventiven Schritten und das stetige Hinterfragen können dabei helfen, sich vor den Schattenseiten dieser praktischen Technologie zu schützen.

Hannover (dpa/tmn) – Briefpost mag grundsätzlich einen seriösen Eindruck machen. Verlassen sollte man sich auf dieses Gefühl aber nicht. Denn derzeit versenden Betrüger gefälschte Schreiben deutscher Banken mit QR-Codes, warnt das Landeskriminalamt (LKA) Niedersachsen. Wer einen dieser Codes scannt und dem darin hinterlegten Link folgt, landet auf einer gefälschten Banking-Seite und wird zur Eingabe sensibler Daten aufgefordert.

Das sollte man natürlich nicht tun, denn die Kriminellen verfolgen das Ziel, Zugriff aufs eigene Onlinebanking zu erhalten. Aufhänger in den Briefen ist den Angaben zufolge die Behauptung, aufgrund von EU-Vorschriften die Identität der

Kundinnen und Kunden überprüfen zu müssen.

Griff zum Hörer bringt Klarheit

Wer sich unsicher ist, ob so ein Schreiben echt ist, dem rät das LKA, telefonisch bei der Bank nachzufragen. Vorsicht: Man sollte nur eine bekannte Nummer wählen und bloß nicht dem womöglich gefälschten Brief einen Kontakt entnehmen.

Zuletzt hatten etwa an E-Auto-Ladesäulen aufgedruckte QR-Codes für Schlagzeilen gesorgt, die Betrüger mit QR-Code-Stickern überklebt hatten. Aber auch gefälschte QR-Codes in vermeintlichen Werbe-Mails sind seit Jahren ein Problem.

Quishing kann viele Ziele haben

Neben Zugängen zum Onlinebanking können es die Kriminellen bei solchen QR-Code-Phishing-Angriffen (auch als Quishing bezeichnet) auf Anmeldedaten für alle möglichen Dienste und Konten abgesehen haben. Ebenso kann es sein, dass QR-Codes den Download und die Installation von Schadsoftware anstoßen sollen.

Egal, ob digital, auf Papier oder irgendwo aufgedruckt: Verbraucherinnen und Verbraucher sollten immer im Hinterkopf behalten, dass QR-Codes überklebt, manipuliert werden oder bereits mit betrügerischen Absichten erstellt worden sein können.

Vorsichtsmaßnahmen beim Umgang mit QR-Codes:

– Am Smartphone sollte man das sofortige Öffnen von Links aus QR-Codes heraus möglichst deaktivieren, rät das LKA. Stattdessen sollte erst einmal nur der Link oder ein Vorschaubild der Webseite hinter dem Link angezeigt werden. Solche Vorschauen sind meist voreingestellt, wenn man die

Smartphone-Kamera oder einen Browser wie Firefox als Scanner nutzt.

– Links aus QR-Codes vor dem Öffnen ganz genau anschauen: Handelt es sich um die erwartete Webseite ohne Tippfehler, Zahlen- oder Buchstabendreher? Ist die eigentliche Domain vielleicht gar nicht auf einen Blick zu erkennen, sondern steht ganz am Ende eines sehr langen Links? Ist die eigentliche Adresse verborgen, weil der Link von einem Dienst zum Verkürzen von Internetadressen stammt?

Hintergrundinformationen zu QR-Code-Betrugsmaschen

Die Verwendung von QR-Codes hat in den letzten Jahren erheblich zugenommen, insbesondere während der COVID-19-Pandemie, als kontaktlose Transaktionen populär wurden. Viele Unternehmen und Banken haben QR-Codes eingesetzt, um Zugang zu Informationen oder Dienstleistungen zu bieten. Dies hat jedoch auch eine Schattenseite geschaffen, da diese Technologie von Kriminellen ausgenutzt wird, um Phishing-Angriffe durchzuführen.

Das LKA Niedersachsen hat festgestellt, dass nach einer steigenden Anzahl solcher Betrugsfälle zunehmend Menschen Opfer von Quishing werden. Diese Form des Betrugs ist besonders ernst zu nehmen, weil sie sich durch die vermeintliche Seriosität der verwendeten Medium, wie Briefpost oder E-Mails, stark tarnen kann. In vielen Fällen sind die Angreifer sehr geschickt darin, die Designs und die Sprache, die von legitimen Firmen genutzt wird, nachzuahmen.

Statistische Daten und Trends

Laut einer Studie des Bundesverbandes für Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) haben im Jahr 2022 fast 40 % der Befragten

angegeben, in irgendeiner Form von Cyberkriminalität betroffen gewesen zu sein. Unter diesen fielen auch Phishing- und Quishing-Angriffe, die signifikant zugenommen haben. Zum Beispiel zeigen Berichte, dass die Anzahl der gemeldeten Phishing-Vorfälle in Deutschland im Vergleich zum Vorjahr um etwa 30 % gestiegen ist.

Zusätzlich wies eine Erhebung des Verbraucherzentrale Bundesverbands darauf hin, dass jedes Jahr Millionen von Euro durch solche Betrugsmaschen verloren gehen, was die Notwendigkeit einer verstärkten Sensibilisierung der Verbraucher unterstreicht. Daher ist die Aufklärung über Quishing und die richtigen Vorsichtsmaßnahmen unerlässlich, um die Sicherheit der Nutzer im digitalen Raum zu gewährleisten.

Details