NACHRICHTEN AG

23. August 2024

„Achtung vor Quishing: Polizei warnt vor gefälschten Kreditinstitutsbriefen“

Achtung! Die Polizei warnt vor der Betrugsmasche "Quishing": Gefälschte Briefe von Banken mit QR-Codes im Umlauf. Schützen Sie Ihre Daten!

Düsseldorf (ots) – Betrüger haben eine neue Masche gefunden, die als „Quishing“ bekannt ist und sich auf die zunehmende Nutzung von QR-Codes stützt. Bei dieser betrügerischen Vorgehensweise versuchen Kriminelle, durch gefälschte Briefe, die von bekannten Kreditinstituten stammen sollen, an sensible Daten ihrer Opfer zu gelangen. Aktuell wurden solche Schreiben in mehreren Bundesländern entdeckt. Die Briefe wirken auf den ersten Blick professionell und sollen dadurch das Vertrauen der Empfänger gewinnen, was die Gefahr erhöht, dass viele Menschen darauf hereinfallen.

Im Rahmen des Quishings enthalten diese gefälschten Mitteilungen einen QR-Code, den die Empfänger scannen sollen. Hinter diesem Code verbirgt sich jedoch kein legitimer Link zur Bankwebsite, sondern eine betrügerische Seite. Sobald die Opfer den QR-Code scannen und den Anweisungen auf der Fake-Seite folgen, geben sie ungewollt ihre Zugangsdaten oder Bankinformationen preis. Diese Art des Betrugs ist besonders gefährlich, da es für die Opfer oft schwierig ist, auf den ersten Blick zu erkennen, dass sie auf einer gefälschten Plattform sind.

Wie funktioniert der Betrug?

Die Kriminellen nutzen den weit verbreiteten Gebrauch von QR-Codes, um an wertvolle persönliche Daten zu gelangen.

Menschen scannen QR-Codes oft ohne darüber nachzudenken, insbesondere wenn sie in einem scheinbar offiziellen Kontext angeboten werden. Die Täter laden ihre Opfer dazu ein, ihre Daten zu offenbaren, indem sie geschickt eine vertrauenswürdige Situation simulieren.

Ein erhaltener Brief könnte beispielsweise mitteilen, dass es ein Problem mit dem Konto gibt und dass zur Lösung ein QR-Code gescannt werden muss. Dieser Code leitet die Betroffenen auf eine Webseite weiter, die aussieht wie die ihrer Bank, jedoch in Wirklichkeit eine Fälschung ist. Bei Eingabe ihrer Daten glauben die Opfer, sicher zu handeln, während sie in Wirklichkeit den Betrügern einen Zugang zu ihren Konten ermöglichen.

Die Polizei hat bereits eindringlich gewarnt, dass die Empfänger solcher Briefen äußerst vorsichtig sein sollten. Sie rät den Menschen, nicht auf die Forderungen in solchen Schreiben zu reagieren. Stattdessen sollten Betroffene auf Nummer sicher gehen und direkt über offizielle Kommunikationswege Kontakt zu ihrer Bank aufnehmen.

Schutzmaßnahmen und Prävention

Um sich gegen solche betrügerischen Angriffe zu schützen, ist es wichtig, wachsam zu sein. Wenn man einen QR-Code scannen möchte, sollte man zuerst sicherstellen, dass der Absender des Codes vertrauenswürdig ist. Hierzu empfiehlt es sich, Rücksprache mit dem offiziellen Kundenservice des betreffenden Unternehmens zu halten.

Ebenfalls hilfreich ist die Nutzung von Multi-Faktor-Authentifizierung beim Online-Banking und anderen sensiblen Datenanwendungen. Selbst wenn es Betrügern gelingt, Zugangsdaten zu erlangen, haben sie dadurch Schwierigkeiten, auf Konten zuzugreifen, da ein weiterer Identifikationsfaktor benötigt wird.

Im Falle eines Betrugsversuchs sollten Opfer sofort die Polizei

benachrichtigen. Wenn bereits Geld abgehoben wurde oder Transaktionen stattfanden, sollte das Kreditinstitut kontaktiert werden, um das Konto zu sperren. Die Hotline 116116 ist hierfür ein hilfreiches Mittel. Darüber hinaus ist es ratsam, alle Verdachtsmomente und Entwicklungen den zuständigen Behörden zu melden.

Wachsamkeit als Schlüssel zur Sicherheit

In der heutigen digitalen Welt ist Wachsamkeit entscheidend, um sich vor Betrügern zu schützen. „Quishing“ ist nur eine von vielen Möglichkeiten, wie Kriminelle versuchen, unvorsichtige Opfer zu täuschen. Daher ist es von enormer Bedeutung, jeder Kommunikation, insbesondere im digitalen Raum, mit gesundem Misstrauen zu begegnen und stets sicherzustellen, dass die Informationen aus vertrauenswürdigen Quellen stammen.

Hintergrundinformationen zu „Quishing“

Die Methode des „Quishing“ ist ein neues Phänomen in der Welt des Online-Betrugs, das sich insbesondere in den letzten Jahren verstärkt hat. QR-Codes sind in vielen alltäglichen Anwendungen und Dienstleistungen weit verbreitet geworden, angefangen von Kontaktinformationen über Speisekarten in Restaurants bis hin zu Bezahlsystemen. Dieser Aufschwung macht QR-Codes zu einem attraktiven Ziel für Betrüger, die diese Technologie missbrauchen, um ahnungslose Opfer zu täuschen.

Die Entwicklung von QR-Codes hat sich stark mit der Digitalisierung des Zahlungsverkehrs verbunden. Während die Nutzer zunehmend moderne Technologien und Zahlungsarten akzeptieren, scheinen viele nicht in der Lage zu sein, die Risiken zu erkennen, die mit dem Scannen solcher Codes verbunden sind. In einer Zeit, in der Cyberkriminalität immer raffinierter wird, ist es für Verbraucher von entscheidender Bedeutung, über die neuesten Betrugsmaschen und Cybersicherheitspraktiken informiert zu sein.

Statistiken und Daten zur Cyberkriminalität

Die Zahlen hinsichtlich Cyberkriminalität in Deutschland sind alarmierend. Laut dem aktuellen Bundeslagebild Cybercrime 2022 des Bundeskriminalamts (BKA) wurden im Jahr 2021 über 100.000 Delikte im Zusammenhang mit Internetkriminalität registriert, was einem Anstieg von rund 12,5 % im Vergleich zum Vorjahr entspricht. Insbesondere Phishing-Attacken sind ein häufiges Problem, bei dem Kriminelle versuchen, persönliche Daten und Bankinformationen zu stehlen.

Eine Umfrage von Bitkom Research aus dem Jahr 2022 ergab, dass 49 % der Befragten angaben, in den letzten zwei Jahren eine Form von Cyberangriff erlebt zu haben. Diese Statistiken verdeutlichen nicht nur die Gefährlichkeit von Betrugsmaschen wie „Quishing“, sondern auch die Notwendigkeit, sich ständig über Sicherheitsmaßnahmen und -praktiken auf dem Laufenden zu halten. Verbraucher sollten sich bewusst sein, dass sie nicht allein sind und dass der Schutz ihrer Daten höchste Priorität haben sollte.

Details