

LKA Niedersachsen warnt vor Phishing mit QR-Codes per Briefpost

Per Briefpost suchen Betrüger Opfer, die einen QR-Code scannen und auf den dadurch geöffneten Phishing-Link hereinfliegen, warnt das LKA Niedersachsen.

🇬🇧 📄 🔊 💬 109



Kriminelle phishen nach monetarisierbaren Informationen. (Bild: Bild erstellt mit KI in Bing Designer durch heise online / dmk)

06.08.2024, 15:28 Uhr | Lesezeit: 3 Min. | Security

Von Dirk Knop

Die Phishing-Mails mit der Absicht, an sensible und monetär missbrauchbare Informationen von Opfern zu gelangen, sind weitreichend bekannt. Das LKA Niedersachsen warnt nun jedoch davor, dass Betrüger in einigen Fällen per Briefpost Druck auf potenzielle Opfer aufbauen, den abgedruckten QR-Code einzuscannen und auf der dadurch geöffneten Webseite wertvolle Daten einzugeben.

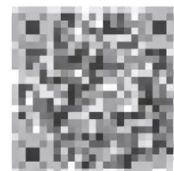
Auf dem Portal polizei-praevention.de des LKA Niedersachsen warnen die Beamten, dass diejenigen, die den QR-Code scannen und dem Link folgen, auf einer gefälschten Banking-Seite landen. Diese imitiert die Optik der jeweils im Brief angegebenen Bank.

Deutsche Bank 

Deutsche Bank, 60325 Frankfurt am Main



QR-Code führt zu gefälschter Seite



QR-Code führt zu gefälschter Seite

Sehr geehrte Frau Müller

Wir möchten Sie über eine wichtige Angelegenheit im Zusammenhang mit Ihrem Konto informieren.

Gemäß den EU-Vorschriften zur Verhinderung von Geldwäsche (AML) und den Know Your Customer (KYC) Richtlinien sind wir als Kreditinstitut verpflichtet, die Identität unserer

Kunden genau festzustellen und diese in regelmäßigen Abständen erneut zu überprüfen. Diese Maßnahmen sind unerlässlich, um sicherzustellen, dass die Daten unserer Kunden stets korrekt und aktuell sind. Änderungen wie Umzüge, Heirat oder andere Lebensereignisse können zu Abweichungen führen, die es erforderlich machen, Ihre persönlichen Daten zu aktualisieren.

Wir bitten Sie daher, Ihre aktuellen Daten zu überprüfen und gegebenenfalls zu aktualisieren. Dies ist ein wichtiger Schritt, um Ihre Sicherheit und die Integrität unseres Bankensystems zu gewährleisten.

Um Ihnen diesen Prozess so einfach wie möglich zu gestalten, haben wir einen QR-Code beigefügt. Scannen Sie diesen bitte mit der Kamera Ihres Smartphones. Der Scan des QR-Codes wird Sie durch den gesamten Aktualisierungsprozess führen, welcher nur wenige Minuten in Anspruch nimmt und lediglich Ihre Adressdaten abfragt.

Wir bitten Sie, diesen Prozess bis zum 29.07.2024 abzuschließen

Hochachtungsvoll,
Ihre Deutsche Bank

Deutsche Bank
Kasernenstr. 10
60325 Frankfurt am Main
Email: info@db.com

Deutsche Bank



AG Frankfurt am Main,
HR: HRB 32000
Ust-ID: DE114103514
<https://db.com>

Angeblich von der Deutschen Bank stammt dieser Brief. Der Link im QR-Code führt auf eine Phishing-Seite.
(Bild: LKA Niedersachsen)

Die Inhalte der Briefe sind bereits aus früheren Phishing-Wellen bekannt, die E-Mails als Medium nutzen. In den vom LKA Niedersachsen gezeigten Beispielen behaupten die Betrüger: "Gemäß den EU-Vorschriften zur Verhinderung von Geldwäsche (AML) und den Know Your Customer (KYC) Richtlinien sind wir als Kreditinstitut verpflichtet, die Identität unserer Kunden genau festzustellen und diese in regelmäßigen Abständen erneut zu überprüfen." Dazu müssten die Empfänger die Daten überprüfen und gegebenenfalls aktualisieren. "Um Ihnen diesen Prozess so einfach wie möglich zu gestalten, haben wir einen QR-Code beigefügt. Scannen Sie diesen bitte mit der Kamera Ihres Smartphones", geben sich die Kriminellen vermeintlich hilfreich. Um den Druck zu erhöhen, ist auch ein Datum abgedruckt, bis zu dem das zu erfolgen hat.

Unterschiedliche Banken imitiert

Mit ähnlichem Text sind zwei Briefe versehen, bei denen die Absender sich jedoch unterscheiden. Einmal stammt der Brief angeblich von der Commerzbank, ein andere soll von der Deutschen Bank kommen. Wenn Opfer den Links folgen, landen sie auf einer optisch entsprechend angepassten Phishingseite. Die Angreifer leiten die "Opfer durch die diversen Prozesse und bekommen somit schließlich Zugriff auf das echte Onlinebanking", ergänzt das LKA Niedersachsen, auch "die Abfrage von sicherheitsrelevanten TAN oder die Bestätigung per TAN-App" sei möglich.

Die Links im QR-Code sind etwa mit Link-Shortener verkürzt oder nutzen die Top-Level-Domain .ru und können dadurch aufmerksamen potenziellen Opfern als nicht legitim auffallen. Das LKA empfiehlt, im Smartphone die Option zu deaktivieren, Links aus QR-Codes sofort zu öffnen. Die Täter könnten die URLs auch so gestalten, dass auf einem Handy-Display lediglich einen Teil der Adresse steht, der plausibel aussieht.

In Niedersachsen seien bislang noch wenige bekannte Fälle angezeigt worden. Es sei auch noch kein Schaden entstanden. Potenzielle Opfer kontaktierten die Bank-Hotline und fragten bezüglich der Echtheit des Schreibens nach oder erkannten den Link beim Öffnen als Fälschung, was das LKA Niedersachsen als korrektes Verhalten lobt. Möglicherweise gibt es aber auch Opfer, die auf die Masche hereingefallen sind und diese nicht angezeigt haben.

Lesen Sie auch



Online-Betrug: Verbraucher fürchten Künstliche Intelligenz

An die Adressdaten können die Täter durch frühere Einbrüche und Datenlecks etwa in Online-Shops gelangt sein. Ein Brief im Briefkasten ist daher inzwischen auch kein Garant mehr, dass es sich um ein echtes Dokument handelt. Gegebenenfalls sollen Empfänger bei ihrer Bank unter der bekannten Rufnummer anfragen und bei Fälschungen Anzeige etwa über die Onlinewache erstatten.

(dmk)