

Bankmitarbeiterin getäuscht: Betrüger ergaunern sechsstellige Summe

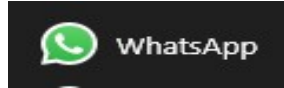
Ein Telefonbetrüger hat am Dienstag eine Bankmitarbeiterin getäuscht und damit erheblichen finanziellen Schaden angerichtet.

Nach Angaben der Polizei kontaktierte der unbekannte Anrufer am Vormittag die Bank und gab sich als Geschäftsführer (CEO-Fraud) eines örtlichen Unternehmens aus. Durch geschickte Gesprächsführung setzte er die Mitarbeiterin so stark unter Druck, dass sie mehrere Überweisungen anordnete. Einige der Überweisungen wurden ausgeführt, bevor der Betrug erkannt wurde. Zwar konnten mehrere Transaktionen rückgängig gemacht werden, dennoch entstand ein Schaden im unteren sechsstelligen Bereich. Die Kriminalpolizei hat die Ermittlungen aufgenommen und warnt vor dieser Betrugsmasche, bekannt als „**CEO-Fraud**“. Dabei geben sich Betrüger als Führungskräfte von Unternehmen aus und wenden sich gezielt an **Mitarbeiter, die Überweisungen tätigen dürfen**. Diese werden unter Druck gesetzt, größere Summen ins Ausland zu überweisen. Die finanziellen Schäden können bis in die Millionenhöhe reichen. Die Polizei rät Unternehmen, Schutzmaßnahmen zu ergreifen: Mitarbeiter sollten klare Vorgehensweisen für finanzielle Transaktionen kennen und bei ungewöhnlichen Anweisungen stets eine Rückversicherung einholen.

Trickbetrüger ruft als Bank-Mitarbeiter an

- Ein Unbekannter gibt sich als Mitarbeiter Ihrer Bank aus.“
- *Ich habe schlechte Nachrichten, Ihr Online-konto wurde gehackt! Wir müssen umgehend Ihre Daten prüfen. Geben Sie mir Ihre IBAN-Nr. an und aktivieren Sie Ihr mobiles TAN“*
- (Puchheim Schaden 250000 €)
- Ihre Bank ruft Sie niemals an, nur auflegen.

Polizei warnt vor neuen Whatsapp-Betrugsmasche



Der Anrufer gibt sich als **Mitarbeiter eines Bank-Sicherheitsservices** aus.

Er behauptet der Bank seien Unregelmäßigkeiten aufgefallen. Die Frau habe ihre letzte Abhebung an einem **manipulierten Kartenterminal** getätigt, wodurch Betrüger an die persönlichen Daten der Frau gelangt seien.

Denken Sie daran: Ihre Bank ruft Sie niemals an!
Also sofort auflegen

Warnung Ihrer Sparkasse

Vorsicht vor „**Quishing**“, einer neuen Betrugsmasche

Neben eMails und Anrufen sind **neuerdings Briefe** - angeblich im Namen des Deutschen Sparkassen- und Giroverbands - aufgetaucht. Die Sparkasse warnt eindringlich.

Sparkasse warnt vor betrügerischen Briefen

In den Briefen wird die Aktualisierung persönlicher Daten gefordert. Dafür ist im Schreiben ein **QR-Code** angegeben. Wird der Code gescannt, wird man automatisch auf eine betrügerische Webseite umgeleitet – auch Phishing-Seite genannt. An dieser Stelle werden neben persönlichen Daten auch die Zugangs-Daten für das Online-Banking sowie die Nummer der Sparkassen-Card oder Kreditkarte abgefragt.

Die Sparkasse warnt nachdrücklich: „Bitte geben Sie niemals Daten auf den Phishing-Seiten ein.“

Nach Kenntnis Ihrer Zugangsdaten wird das Passwort geändert und Sie haben auch als Kontoinhaber hierauf keinen Zugriff mehr, so dass in aller Ruhe Ihr Konto geplündert werden kann

So erkennen Sie den falschen Sparkassen-Brief

Mit fadenscheiniger Begründung für die Daten-Abgabe wird von den Betrügern auf eine „EU-Vorschrift zur Verhinderung von Geldwäsche und den Know Your Customer (KY C) Richtlinien“ verwiesen. Außerdem heißt es, dass das Online-Banking eingeschränkt wird, sollte man den Brief missachten. **Alles nur Fake.**

Was kann man tun, wenn man Daten ein- oder angegeben hat?

Wenn Sie bereits auf die Betrugsmasche hereingefallen sind, wenden Sie sich **auf direktem und offiziellem Weg an die Sparkasse**. Vor Ort können die Mitarbeiter den Zugang zum Online-Banking und die Kredit- und Sparkassenkarte sperren. Dadurch wird finanzieller Schaden verringert oder sogar verhindert.

Häufig sind Betrugsmaschen kompliziert. Bei dieser neuen Methode ist das jedoch anders: Sie ist sehr einfach und bringt den Tätern viel Geld

Unbekannte Abbuchungen vom Konto: **Warnung vor Betrugsmasche**

Gar nicht mal großen Summen wurden abgebucht. Das macht die Masche aus Sicht eines Users so perfide. Ein Ehepaar entdeckte rechtzeitig unbekannte Abbuchungen auf ihrem Konto. Und da hatte ein Betrüger schon regelmäßig unverfängliche Beträge von je 89,90 € abgebucht. Im heutigen Zeitalter des bargeldlosen Zahlungsverkehrs fällt so etwas so schnell einfach nicht mehr auf. Dies fiel eben diesem Geschädigten dann doch auf, nachdem er als Konsequenz ganz engmaschig die Bewegungen auf dem eigenen Konto verfolgt – **und das auch jedem anderen rät**. Sonst drohe schnell eine böse Überraschung. Dabei wurde entdeckt, dass eine unbekannte Adresse regelmäßig Geld vom Familienkonto abbuchte. Eine Summe, die man bei flüchtigem Blick über die Kontobewegungen auch mal übergehen kann – selbst wenn man regelmäßig den Kontostand und die jüngsten Buchungen kontrolliert. Aber nicht so bei der Kontokontrolle im Folgemonat. Da stachen die 89,90 € ins Auge, ab-gebucht als Basislastschrift der **Firma Megatipp Emergency Call Services**. Gemeinsam mit einem Bankmitarbeiter wurde anhand der IBAN eine Bank auf Malta ermittelt. Besagte Summe von 89,90 € war dem Text auf dem Formular zufolge berechnet worden für eine Notfall-Karte, als Telefonnummer war eine Verbindung mit der Ortsvorwahl vermerkt. Vermutlich muss der „regelmäßigen“ Abbuchung ein Telefonat vor Monaten vorausgegangen sein, bei dem das Opfer auf eine bestimmte Frage mit „Ja“ geantwortet hatte. Glücklicherweise bewegten sich die Abbuchungen noch im Zeitraum von acht Wochen und konnten so von der Bank noch zurückgebucht werden. Möglicherweise ist der Kontoinhaber mit der Rückbuchung der beiden Abbuchungen auch noch nicht ganz durch. Selbst wenn erneut abgebucht werden sollte und man dann der Empfehlung der Bank folgt, die Nummer zu sperren. In Internet-Foren ist die Rede davon, dass von „**Megatipp Emergency Call Services**“ möglicherweise noch Schriftverkehr wie etwa Mahnungen folgen könnte. Und dann muss unter Umständen der ungewollt untergejubelte Vertrag noch gekündigt werden, wozu sich manch einer auch schnell mal professionellen Beistand sichert– mit entsprechenden Kosten.