

02. Februar 2024

Phishing-Mail nimmt Sparkassen-Kunden ins Visier

Mit immer neuen Maschen versuchen Cyberkriminelle, an die Daten von Bankkunden zu kommen. Mit einer Phishing-Mail, die seit Dezember 2023 kursiert, nehmen Betrüger explizit Sparkassen-Kunden ins Visier und versuchen, an ihre Kontodaten zu kommen.

Phishing-Mail warnt vor auffälligen Kontoaktivitäten

Die vermeintliche E-Mail von der Sparkasse mit dem Betreff „Benachrichtigung über auffällige Kontoaktivität“ warnt Kunden vor angeblichen, verdächtigen Login-Versuchen und Transaktionen. Konkret gibt die Mail vor, dass ein Login-Versuch von einem bisher unbekannten Gerät erfolgt und eine Transaktion aus Sicherheitsgründen vorläufig gesperrt worden sei. Um die Transaktion vollständig abubrechen, soll der Kunde auf den Button „Übertragung Jetzt Abbrechen“ in der Mail klicken. Wer dem Folge leistet, wird jedoch auf eine Seite weitergeleitet, auf der die Cyberkriminellen die persönlichen Daten abgreifen können.

Mails wirken täuschend echt

Diese Phishing-Mail an Sparkassen-Kunden ist täuschend echt aufgebaut. Sie enthält zahlreiche Details zu dem vermeintlichen Login-Versuch, z. B. den Standort, von dem aus der Login erfolgt sein soll, die IP-Adresse und den Gerätetyp. So soll der drohende Geldverlust noch glaubwürdiger erscheinen.

In einer weiteren Phishing-Mail werden Sparkassen-Kunden gebeten, das Finanzinstitut bei der Überprüfung und Optimierung der Website zu unterstützen. Über einen in der Mail enthaltenen Link sollen die Kunden ihre Daten prüfen und verifizieren, um eventuell veraltete oder unvollständige Angaben auszuschließen. Wer den Link anklickt, wird auch in diesem Fall auf eine gefälschte

Webseite weitergeleitet, über die Betrüger die persönlichen Daten abfangen.

Wie kann ich mich schützen?

Auf den ersten Blick wirken solche Phishing-Mails absolut echt. Sie weisen die typischen Farben auf und enthalten die Logos der jeweiligen Bank. Trotzdem gibt es Hinweise, die auf einen Betrugsversuch hindeuten. So zeigen sich bei genauerem Lesen Mängel, z. B. fehlende Kommas, Rechtschreibfehler im Text oder inhaltliche Widersprüche.

In der E-Mail mit dem Betreff „Benachrichtigung über auffällige Kontoaktivität“ heißt es beispielsweise im letzten Satz, dass die Transaktion aufgrund veralteter Daten abgebrochen wurde. Diese Aussage weicht inhaltlich vom vorangehenden Text ab. Auch die Absenderadresse ist nicht von der Sparkasse.

Um sich zu schützen, sollten Sie grundsätzlich nicht auf Buttons oder Links in vermeintlichen E-Mails von Ihrer Bank oder Sparkasse klicken. Wenn Sie sich unsicher sind, ob es mit Ihrem Konto wirklich ein Problem gibt, melden Sie sich über die App oder die offizielle Website der Sparkasse bei Ihrem Konto an und überprüfen Sie die Aktivitäten. Achten Sie dabei darauf, die Website der Sparkasse direkt aufzurufen – also durch Eingabe der URL im Browser. Vermeiden Sie es, die Webseite per Google-Suche aufzurufen. Denn auch die Ergebnisse auf Google können manipuliert sein.

Was kann ich im Schadenfall tun?

Wenn der schlimmste Fall eintritt und die Betrüger mit geklauten Daten Ihr Konto geplündert haben, sollten Sie als erstes die Zugangsdaten zu Ihrem Online-Banking-Account ändern und Ihre Bank informieren, um weiteren Schaden zu vermeiden. In manchen Fällen können die Abbuchungen auch noch zurückgeholt werden.

Löschen Sie die Phishing-Mail nicht. Sie dient möglicherweise als Beweismittel. Außerdem sollten Sie sich umgehend anwaltlichen Rat einholen. Abhängig von den jeweiligen Umständen kann ein Erstattungsanspruch gegenüber der Bank bestehen. So wurde die Sparkasse bereits in zwei Fällen zur Erstattung der von den Cyberkriminellen erbeuteten Beträge verurteilt. Wir berichteten darüber. Den entsprechenden Beitrag finden Sie [hier](#). In der Anwaltskanzlei Lenné konnten wir bereits für zahlreiche Mandanten die Verluste zurückholen. Wenn auch Sie Opfer einer Betrugsmasche geworden sind, beraten wir Sie gerne im Rahmen eines kostenlosen Erstgesprächs zu Ihrem individuellen Fall.

[Kerstin Messerschmidt](#)

Angestellte Rechtsanwältin

Wir helfen Ihnen gerne! [Kontaktieren](#) Sie uns. Oder vereinbaren Sie [hier online einen Termin](#) für eine telefonische kostenfreie Erstberatung.

- [Facebook](#)
- [Twitter](#)
- [WhatsApp](#)
- [E-mail](#)

[Zurück](#)