Vorsicht, Falle! Bei Fake-Mails sollte man doppelt wachsam sein. Betrüger versuchen, mit gefälschten Nachrichten an Kontodaten zu kommen. SYMBOLFOTO: DPA

Vorsicht, Betrüger!

Volksbank warnt vor falschen Mails – und gibt Tipps zum Erkennen und Schützen

VON THOMAS THIMM

Auch bei uns macht die Mail eines angeblichen Volksbank-Kundendienstes die Runde, die dazu auffordert, einem Link zu folgen und Daten zu aktualisieren. Die Volksbank Hameln-Stadthagen mahnt ausdrücklich: Hände weg, dort sind Betrüger am Werk, die Volksbank würde eine solche Mail niemals verschicken.

HAMELN/BAD MÜNDER. Die betrügerische Mail macht für den flüchtigen Leser zunächst einen recht normalen Eindruck, bei näherem Hinsehen jedoch offenbaren bereits diverse Rechtschreibfehler, dass hier offenbar etwas nicht stimmt. Und tatsächlich: Die Volksbank Hameln-Stadthagen wendet sich über unsere Zeitung an ihre Kunden, nicht auf diesen oder ähnliche Betrugsversuche hereinzufallen.

In diesem Fall ist es ein angeblicher Volksbank-Kundendienst, der versucht, an Daten heranzukommen, um dann abzuzocken. Volksbank-Sprecher Patrick Eschert sagt dazu: „Leider häufen sich die Versuche, Bankkunden zu betrügen. Wir als seriöse Bank würden jedoch niemals so auf unsere Kunden zugehen."

Die Banken beobachten seit Jahren eine stetig zunehmende Anzahl an Phishing-Fällen: „Gerade rechtliche oder organisatorische Änderungen, die eine breite Masse an Kunden betreffen, nutzen Betrüger als Vorwand, um Zugangsdaten oder Kreditkartendaten für das Online-Banking abzugreifen." Als vermeintliche Absender solcher E-Mails werden nicht nur Banken vorgetäuscht, sondern auch Zahlungsdienstleister wie PayPal oder Online-Händler wie Amazon, die Deutsche Bahn oder auch Mobilfunkanbieter. Häufig werde auf eine falsche Eingabemaske verlinkt. So können Kunden jedoch betrügerische E-Mails schnell erkennen:

- Häufig ist die Anrede unpersönlich, zum Beispiel heißt es nur „Sehr geehrte/r Kunde/in".
- In aller Regel wird ein dringender Handlungsbedarf vorgetäuscht oder sogar mit Konsequenzen gedroht, sofern etwas nicht getan wird, zum Beispiel „Sollten Sie bis zum XYZ nicht reagieren, wird Ihr Online-Banking gesperrt."
- Sprachliche Ungenauigkeiten: Der Text ist in schlechtem Deutsch verfasst, enthält Fehler, kyrillische Buchstaben, falsch aufgelöste oder fehlende Umlaute – beispielsweise „a" oder „ea" statt „ä".

Was tun, wenn es passiert ist?

- Sperren von Karte und/oder Online-Banking mithilfe des Links „Karte und Online-Banking sperren" auf der echten Volksbank-Homepage oder telefonisch unter 116116
- Unter der folgenden kostenfreien Telefonnummer können sich Kunden melden, wenn sie einen Betrugsverdacht – zum Beispiel einen Fall von Phishing – vermuten: 0800/5053111.

  Anrufe werden von 8 bis 24 Uhr entgegengenommen. Hinter dieser Rufnummer stecken Mitarbeiter des Volksbank-IT-Dienstleisters.
- Anzeige bei der Polizei erstatten. Beweise wie Phishing-Mails und Schriftverkehr sichern.

Diese Schutzmaßnahmen bietet die Bank

Volksbank-Sprecher Patrick Eschert erläutert, dass die Bank Maßnahmen ergriffen habe, um ihre Kunden gegen Betrüger zu schützen.

- So informiert die Volksbank Hameln-Stadthagen regelmäßig auf ihren echten Online-Kanälen wie Online-Banking, Homepage und Social Media über diverse Betrugsmaschen, die meist bundesweit auftreten. Eschert: „Dort findet man aktuelle Betrugsmaschen und Phishing-Warnungen."
- Die Bank habe bereits seit Jahren ein Früherkennungssystem im Einsatz, welches verdächtige Zahlungen anhalte, „die wir dann in Rücksprache mit dem Kunden prüfen".
- Über einen technischen VR-Computer-Check bietet die Bank ihren Kunden einen einfachen System-Check an, der Sicherheitsprobleme auf Computer oder Smartphone erkennt und unterstützt, diese zu beheben.
- Die Volksbank betont: „Wir versenden niemals E-Mails, in denen Kunden dazu aufgefordert werden, ihre Kontodaten einzugeben. Wir werden auch niemals zu Test- oder Sicherheitszwecken Anfragen an unsere Kunden stellen. Der beste Schutz vor Angriffen ist deshalb, derartige E-Mails ungeöffnet zu löschen. Grundsätzlich sollten unsere Kunden niemals einen in der E-Mail enthaltenen Link anklicken oder beigefügte Dateianhänge öffnen."