BETRUG BEIM ONLINEBANKING: CHECKLISTE FÜR DEN ERNSTFALL

Bankgeschäfte über das Internet abzuwickeln, ist für viele eine Selbstverständlichkeit. Über die Website der Bank oder per App lassen sich mit wenigen Klicks der Kontostand abfragen und Geldbeträge überweisen – zu jederzeit und von jedem Ort.

Doch Onlinebanking ist auch für Kriminelle ein lukratives Geschäft. Sie versuchen mit gefälschten Internetseiten und fingierten E-Mails Zugangsdaten auszuspähen, um Konten leer zu räumen. Wer auf seinem Konto nicht nachvollziehbare Buchungen feststellt, sollte daher sofort handeln.

DAS SOLLTEN SIE TUN, WENN …

… Sie nicht getätigte Abbuchungen auf Ihrem Bankkonto feststellen:

- ✓ Sperren Sie sofort den Zugang zu Ihrem Bankkonto über den kostenfreien Notruf **116 116** oder aus dem Ausland über die gebührenpflichtige Hotline: **+49 116 116**.
- ✓ Informieren Sie schnellstmöglich Ihre Bank oder Ihre Sparkasse über diesen Vorfall. Nehmen Sie den Kontakt nicht über einen Link oder eine in einer E-Mail angegebene Telefonnummer auf. Suchen Sie die Erreichbarkeit selbst im Internet oder über das Telefonbuch heraus.
- ✓ Neue Zugangsdaten zu Ihrem Onlinebanking erhalten Sie von Ihrer Bank. Sprechen Sie dann auch über die Schadensregulierung.
- ✓ Erstatten Sie Anzeige bei der Polizei. Dann können Ihre Daten auch für das Lastschriften-Verfahren gesperrt werden.

… Sie auf einer gefälschten Webseite Ihre Zugangsdaten preisgegeben haben:

- ✓ Sperren Sie sofort den Zugang zu Ihrem Bankkonto. Nutzen Sie dazu den kostenfreien Notruf **116 116** oder aus dem Ausland die gebührenpflichtige Hotline: **+49 116 116**.
- ✓ Kontaktieren Sie Ihre Bank, um zweifelsfrei festzustellen, dass keine unautorisierten Buchungen oder Aufträge vorgenommen wurden. Fragen Sie nach neuen Zugangsdaten.
- ✓ Anzeige bei der Polizei erstatten: Wenden Sie sich an Ihre örtliche Polizeidienststelle oder Ihre Online-Wache. Übersicht unter: **https://www.bka.de/DE/KontaktAufnehmen/Strafanzeigen/strafanzeigen_node.html**

Bundesamt
für Sicherheit in der
Informationstechnik

Wir wollen, dass Sie sicher leben.
Ihre Polizei

DAS SOLLTEN SIE TUN, WENN …

… Sie auch nur einen Verdacht haben, betroffen zu sein:

- ✓ Erkundigen Sie sich bei Ihrer Bank nach ungewöhnlichen technischen Vorkommnissen oder nach Vorfällen bei anderen Bankkunden.
- ✓ Kontrollieren Sie die Buchungsbewegungen auf Ihrem Konto.
- ✓ Ändern Sie die Zugangsdaten zu Ihrem Onlinebanking.

HINWEIS

Grundsätzlich gilt: Sicherer ist Onlinebanking immer auf zwei Geräten, z. B. auf dem Computer und dem Smartphone. Nutzen Sie deswegen die Zwei-Faktor-Authentisierung.

SO SCHÜTZEN SIE SICH IN ZUKUNFT VOR BETRUG BEIM ONLINEBANKING

- **Zugangsdaten sichern:** Bewahren Sie Ihre Zugangsdaten an einem sicheren Ort auf, so dass diese nicht gestohlen oder kopiert werden können. Speichern Sie keine Bankdaten auf Ihrem PC oder auf Ihrem Handy/Smartphone und geben Sie diese nicht an Dritte weiter.
- **Zwei Geräte nutzen:** Zur Freigabe von Transaktionen ist die Verwendung eines TAN-Generators das aktuell sicherste Verfahren. Bankgeschäfte per App sollten immer mit zwei Geräten durchgeführt werden, beispielsweise dem Computer und dem Smartphone.
- **Kommunikation prüfen:** In gefälschten Mails oder vorgetäuschten Anrufen versuchen Unberechtigte, an Ihre Bankdaten zu kommen. Wichtig: Ihre Bank fragt Sie niemals nach Ihren Zugangsdaten zum Onlinebanking.
- **Limit festlegen:** Legen Sie mit Ihrer Bank ein Limit für tägliche Geldbewegungen fest.
- **Kontakt aufnehmen:** Geben Sie die Internetadresse Ihrer Bank bei jedem Aufruf erneut über die Tastatur ein oder richten Sie ein Lesezeichen ein. So vermeiden Sie, auf gefälschte Seiten geführt zu werden. Folgen Sie keinen Links in einer E-Mail, egal wie seriös diese wirkt.

Mehr Informationen zum Schutz vor Betrüger-E-Mails unter:
https://www.bsi-fuer-buerger.de/Onlinebanking

Mehr Informationen für Opfer von Cyber-Crime:
www.polizei-beratung.de/opferinformationen/cybercrime/

Bundesamt
für Sicherheit in der
Informationstechnik

Wir wollen, dass Sie sicher leben.
Ihre Polizei