BETRUG BEIM ONLINEBANKING: CHECKLISTE FÜR DEN ERNSTFALL

Bankgeschäfte über das Internet abzuwickeln, ist für viele eine Selbstverständlichkeit. Online über den Browser oder per App lassen sich mit wenigen Klicks der Kontostand abfragen und Geldbeträge überweisen – jederzeit und von jedem Ort.

Doch Onlinebanking ist auch für Kriminelle ein lukratives Geschäft. Sie versuchen, mit fingierten E-Mails Zugangsdaten auszuspähen und ihre Opfer auf gefälschte Internetseiten zu locken, um deren 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 Sperr-Notruf 116 116 oder aus dem Ausland über die gebührenpflichtige Sperr-Hotline +49 116 116.
- ✓ **Informieren Sie Ihre Bank.** Nehmen Sie den Kontakt nicht über z. B. einen in einer möglicherweise gefälschten E-Mail angegebenen Link oder eine dort aufgeführte Telefonnummer auf. Suchen Sie diese stattdessen selbst, beispielsweise per Suchmaschine, heraus.
- ✓ **Bitten Sie Ihre Bank um neue Zugangsdaten.** Sprechen Sie 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 dafür den kostenfreien Sperr-Notruf 116 116 oder aus dem Ausland die gebührenpflichtige Sperr-Hotline +49 116 116.
- ✓ **Kontaktieren Sie Ihre Bank,** um zweifelsfrei festzustellen, dass keine unautorisierten Buchungen oder Aufträge vorgenommen wurden. Fragen Sie nach neuen Zugangsdaten.
- ✓ **Erstatten Sie Anzeige bei der Polizei.** Als Opfer von Internetkriminalität haben Sie die gleichen Rechte wie Opfer anderer Straftaten.

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

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

Bundesamt
für Sicherheit in der
Informationstechnik

Wir wollen, dass Sie sicher leben.
Ihre Polizei

SO SCHÜTZEN SIE SICH IN ZUKUNFT VOR BETRUG BEIM ONLINEBANKING

- **Starke Passwörter verwenden:** Das kann zum Beispiel ein kurzes und komplexes Passwort sein, das mindestens 8-12 Zeichen bestehend aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthält.

- **Bankverbindung geheim halten:** Veröffentlichen Sie diese nicht zum Beispiel auf einer eigenen Webseite. Vorsicht gilt auch beim Onlineshopping, etwa wenn Sie sich nicht sicher über die Seriosität des Onlineshops sind.

- **Zwei-Faktor-Authentisierung nutzen:** Dabei bestätigen Sie zum Beispiel beim Login über zwei Faktoren, dass dies wirklich Ihr Benutzerkonto ist. Diese Faktoren können etwa ein Passwort und die Freigabe über eine Smartphone-App sein. Beim Onlinebanking ist das bereits Pflicht. Die Zwei-Faktor-Authentisierung sollten Sie aber auch zum Beispiel bei Ihrem E-Mail-Konto und bei Onlineshops, bei denen Sie Ihre Bankverbindung angeben, aktivieren. Eine gute Alternative zu der Kombination aus Passwort und Zwei-Faktor-Authentisierung sind Passkeys.

- **Transaktionen überprüfen:** Lesen Sie zum Beispiel die Details einer Überweisung, etwa an wen Sie Geld überweisen, genau durch, bevor Sie diese bestätigen.

- **Öffentliches WLAN und fremde Geräte meiden:** Nutzen Sie für das Onlinebanking möglichst nur eigene Geräte. Betreiben Sie Onlinebanking zudem nicht über öffentliches WLAN.

- **Kommunikation hinterfragen:** Mit gefälschten E-Mails oder vorgetäuschten Anrufen versuchen Kriminelle, an Ihre Bankdaten oder an andere sensible Informationen zu gelangen. Klicken Sie daher nicht unüberlegt auf Links in einer E-Mail, egal wie seriös diese wirkt. Kriminelle verschicken oft Links zu gefälschten Internetseiten in täuschend echt aussehenden E-Mails. Ihre Bank fragt jedoch niemals nach Ihren Zugangsdaten zum Onlinebanking, Ihrer PIN oder Ihren TANs.

- **Limit festlegen:** Legen Sie mit Ihrer Bank ein Limit für tägliche Geldbewegungen fest. Das kann im Ernstfall den Schaden reduzieren.

- **Adresse merken oder speichern:** Geben Sie die Internetadresse Ihrer Bank bei jedem Aufruf erneut über die Tastatur ein oder richten Sie ein Lesezeichen ein.

- **Richtige App wählen:** Installieren Sie die entsprechende Banking-App nur von vertrauenswürdigen Quellen. Gehen Sie sicher, dass Sie keine gefälschte App herunterladen. Rufen Sie am besten die Webseite Ihrer Bank auf und suchen Sie dort nach der entsprechenden App.

- **Geräte und Anwendungen auf dem neuesten Stand halten:** Führen Sie Updates für Betriebssystem und Software durch, sobald diese verfügbar sind. Installieren und aktivieren Sie auch Antivirenprogramme.

Mehr Informationen zu Cybersicherheit für Verbraucherinnen und Verbraucher:
www.bsi.bund.de/VerbraucherInnen

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

Bundesamt
für Sicherheit in der
Informationstechnik

Wir wollen,
dass Sie
sicher leben.
Ihre Polizei