Konto gehackt! Was nun?

Es ist der Albtraum jedes Bankkunden: Kriminelle verschaffen sich Zugriff aufs Konto und plündern dessen Inhalt. Wenn dies bereits passiert ist, geht es um die Begrenzung des Schadens – und darum, daraus zu lernen.

Das ist bei unberechtigtem Zugriff aufs eigene Bankkonto zu tun:

- Bei verdächtigen Transaktionen oder Fehlern bei der Anmeldung im E-Banking informieren Sie umgehend Ihr Finanzinstitut und lassen Sie den betroffenen E-Banking-Vertrag und die Konten sowie Ihre Karten sperren.
- Trennen Sie alle Geräte, die von Hackern oder Malware betroffen sein könnten, sofort vom Netz und schalten Sie sie aus oder versetzen sie den Flugmodus. Setzen Sie die Geräte aber nicht unmittelbar zurück, da sie von der Polizei für forensische Analysen benötigt werden könnten.
- Ändern Sie Ihre Passwörter von einem separaten, nicht infizierten Gerät aus. Richten Sie wo immer möglich die Zwei-Faktor-Authentifizierung ein.
- Wenn tatsächlich ein Betrug vorliegt, erstatten Sie Strafanzeige bei der Polizei. Notieren Sie sich möglichst alle Ihnen verfügbaren Informationen zum Betrug bzw. Angriff.
- Schützen Sie sich zukünftig vor unberechtigten Zugriffen mit unseren «5 Schritten für Ihre digitale Sicherheit» und den Tipps für sicheres E-Banking.

Wie lässt sich ein Bankkonto hacken?

Die E-Banking-Portale der Schweizer Finanzinstitute sind gegen Hacker-Angriffe sehr gut abgesichert. Dass Kriminelle direkten Zugang zu den Computer-Systemen einer Bank erlangen, kann heute eigentlich ausgeschlossen werden.

Eine Schwachstelle ist aber der unachtsame Bankkunde: Kommen die Hacker an seine Zugangsdaten, können sie sich damit in seinem Namen unbemerkt am E-Banking anmelden und Transaktionen auslösen oder auf vertrauliche Informationen zugreifen. Dies kann beispielsweise mittels eines Phishing-Angriffs (https://www.ebas.ch/phishing/) oder durch eine Infektion mit spezieller Malware (https://www.ebas.ch/malwareinfektion/) geschehen. Dem Geschädigten bleibt dann oft nur noch die Schadensbegrenzung.

Wie reagiert man im Schadensfall richtig?

Das Wichtigste vorweg: Im Verdachtsfall ist schnell zu reagieren! Liegt tatsächlich ein Betrug vor, muss der betroffene E-Banking-Vertrag und die dazugehörigen Konten sofort gesperrt werden, um weiteren Geldabfluss zu verhindern.

In jedem Fall eines Betrugsverdachts, zum Beispiel bei verdächtigen Transaktionen oder Fehlermeldungen im E-Banking, sollten Sie umgehend Ihr Finanzinstitut informieren, um die notwendigen Schritte zu koordinieren. Im Falle eines bestätigten Betruges erstatten Sie zudem Anzeige bei der Polizei.

Falls auch nach Rücksprache mit Ihrem Finanzinstitut nicht bekannt ist, wie sich die Kriminellen Zugriff verschaffen konnten, sollten Sie primär davon ausgehen, dass Fremde im Besitz Ihrer Zugangsdaten sind, und

dass Ihr Gerät von einer Malware, zum Beispiel einem Banking-Trojaner, befallen wurde.

Um weiteren Missbrauch Ihrer mutmasslich entwendeten Zugangsdaten zu unterbinden, sollten Sie das Passwort Ihres E-Mail-Postfaches sowie die Passwörter (https://www.ebas.ch/4-schuetzen-der-online-zugaenge/) all Ihrer Online-Konten vorsorglich ändern – aber nicht mit Ihrem potentiell infizierten Computer oder Mobilgerät, sondern von einem separaten Gerät aus. Ihr E-Banking-Zugang wurde bereits vorgängig gesperrt, eine Passwortänderung erfolgt hier erst zu späterem Zeitpunkt, wenn die Sachlage zusammen mit Ihrem Finanzinstitut geklärt wurde.

Wo immer möglich, sollte zudem eine Zwei-Faktor-Authentifizierung eingerichtet werden – damit erreichen Sie einen wesentlich höheren Zugangsschutz.

Ihr Gerät sollten Sie vom Netz trennen und ausschalten oder in den Flugmodus setzen, aber erst nach einer allfälligen polizeilichen Untersuchung neu aufsetzen (https://www.ebas.ch/neuinstallation-windows-10/) .

Und nicht zuletzt werden Sie sich gegen künftige Betrugsversuche wirksam schützen wollen. Befolgen Sie daher unbedingt die «5 Schritte für Ihre digitale Sicherheit» (https://www.ebas.ch/5-schritte-fuer-ihre-digitale-sicherheit/) und die Tipps für sicheres E-Banking (https://www.ebas.ch/tipps-fuer-sicheres-e-banking/)– denn mit den richtigen Vorsichtsmassnahmen geben Sie Hackern keine Chance!

Sofortmassnahmen bei Verdacht:

- *Finanzinstitut informieren und Konto sperren lassen*
- *Internetverbindung trennen*
- *Passwörter ändern*
- *Strafanzeige erstatten*

Weiterführende Informationen für Interessierte

Kann die Bank Missbrauch erkennen und stoppen?

Einzelne Finanzinstitute verfügen über ein Betrugserkennungssystem, welches verdächtige Transaktionen meldet oder sogar automatisch stoppt. Diese Systeme werden immer besser, bieten aber keine 100%-ige Sicherheit. Und die Betrüger gehen immer geschickter und unauffälliger vor, um solche Systeme zu überlisten.

Nehmen Sie daher Ihre Eigenverantwortung war und verlassen Sie sich nicht darauf, dass Ihre Bank Ihre Konten in jedem Fall vor unberechtigtem Zugriff wie etwa Phishing-Angriffen schützen kann.

Wer haftet im Schadensfall?

Die Haftungsfrage lässt sich nicht generell beantworten und muss von Fall zu Fall beurteilt werden. Neben der eigentlichen Schuldfrage ist hier die Sorgfaltspflicht entscheidend.

Da die Täter meistens unbekannt sind und vom Ausland operieren, gestaltet sich eine Strafuntersuchung oft schwierig. Häufig werden auch unwissende Mittelsmänner, sog. Money Mules (https://www.ebas.ch/money-mules-finanzagenten/) , eingesetzt, um die Transaktionen zu verschleiern. Das transferierte Geld ist in vielen Fällen verloren.

Grundsätzlich müssen sowohl die Finanzinstitute als auch deren Kunden ihre Sorgfaltspflichten im Umgang mit Bankkonten und den darauf liegenden Geldern erfüllen. Ein Gericht wird somit eine allfällige Verletzung dieser Sorgfaltspflicht prüfen, welche unter Umständen beim Kunden vorliegen kann – zum Beispiel, wenn dieser seine Zugangsdaten jemand Fremdem verraten hat, bewusst oder auch unbewusst.

Um sich daher gar nicht erst mit Haftungsfragen auseinandersetzen zu müssen, schützen Sie Ihr Konto vorbeugend (https://www.ebas.ch/tipps-fuer-sicheres-e-banking/)!