

16.02.2026

Betrug – was tun, wenn Schaden entstanden ist?

Trotz Vorsicht und Sicherheitsmassnahmen kann es passieren ... Sie wurden Opfer eines Betrugs: Zugangsdaten wurden preisgegeben oder eine Zahlung wurde ausgelöst. Wichtig ist in dieser Situation vor allem eines: Schnell und richtig handeln. Eine rasche Reaktion kann den Schaden begrenzen und die Chancen auf eine Wiederherstellung erhöhen.

Ruhe bewahren und sofort handeln

Wer merkt oder vermutet, Opfer eines Betrugs geworden zu sein, sollte nicht zögern. Jede Minute zählt - insbesondere bei E-Banking, Kreditkarten oder mobilen Bezahlösungen.

Die wichtigsten Sofortmassnahmen:

- Die Bank oder den Zahlungsdienst umgehend kontaktieren und den Vorfall melden.
- Konten gegebenenfalls sperren (lassen).
- Passwörter umgehend ändern, auch bei anderen Diensten mit denselben Zugangsdaten.

Finanzinstitute und Zahlungsdienstleister können verdächtige Transaktionen unter Umständen stoppen oder weitere Abbuchungen verhindern, wenn sie frühzeitig informiert werden.

Zugangsdaten sichern und Geräte prüfen

Wurden Logindaten preisgegeben oder ein QR-Code gescannt, besteht die Gefahr, dass weitere Konten betroffen sind.

Wir empfehlen folgende Schritte:

- Alle betroffenen Passwörter sofort ändern.
- Zwei-Faktor-Authentifizierung (2FA) aktivieren, falls noch nicht geschehen.
- Apps oder Programme entfernen, die ungewollt installiert wurden.
- Smartphone (Android) und Computer mit einem aktuellen Virenschutzprogramm prüfen.

So lässt sich verhindern, dass Betrüger erneut zugreifen.

Betrug dokumentieren und melden

Eine sorgfältige Dokumentation von Betrugsfällen ist wichtig, da sie nicht nur der eigenen Bank, sondern auch den Strafverfolgungsbehörden hilft. Dazu gehören unter anderem Screenshots von E-Mails, SMS oder Webseiten, Zahlungsbestätigungen und Kontoauszüge sowie Angaben zu Datum, Uhrzeit und dem genauen Ablauf des Vorfalls.

In der Schweiz sollte ein Betrug der Polizei gemeldet werden.

Kann das Geld zurückgeholt werden?

Ob ein finanzieller Schaden rückgängig gemacht werden kann, hängt von verschiedenen Faktoren ab:

- Wie schnell der Betrug gemeldet wurde.
- Welche Zahlungsart genutzt wurde.
- Ob der Betrag bereits weitergeleitet wurde.

Je früher reagiert wird, desto grösser sind die Chancen, dass Zahlungen gestoppt oder zurückgebucht werden können. Eine Garantie gibt es jedoch nicht.

Aus dem Vorfall lernen

Auch wenn ein Betrug sehr belastend sein kann, bietet er dennoch die Möglichkeit, die eigene digitale Sicherheit nachhaltig zu verbessern. Die bewusste Auseinandersetzung mit solchen Vorfällen hilft dabei, gängige Betrugs-
maschen besser zu erkennen und zu verstehen. Und regt dazu an, die eigenen Sicherheitsgewohnheiten zu reflektieren und künftig noch vorsichtiger mit Links, QR-Codes und unerwarteten Nachrichten umzugehen.

Fazit

Ein Betrug ist kein persönliches Versagen. Cyberkriminelle gehen zunehmend professionell vor. Entscheidend ist, schnell zu reagieren, Schäden zu begrenzen und konsequent Massnahmen zu ergreifen. Wer vorbereitet ist, kann im Ernstfall souverän handeln und seine digitale Sicherheit nachhaltig stärken.