

Betrug am Geldautomaten (Skimming)

Wie schützen Sie sich? Was sind Ihre Rechte im Schadensfall?

Seit einigen Monaten lässt sich in der Schweiz eine massive Zunahme des sogenannten Skimmings beobachten: Die Täter manipulieren Geldautomaten, Billettautomaten und sogar Zahlstellen in Einkaufshäusern, um Kredit- oder Debitkarten (z.B. Maestrokarte) zu kopieren. In diesem Merkblatt werden die wichtigsten Fragen zum Thema Skimming beantwortet und erklärt, wie ein solcher Betrug abläuft und wie man sich dagegen schützen kann.

1. Was ist Skimming?

Beim Skimming versuchen Betrüger, Bargeld von einem fremden Bankkonto abzuheben. Dazu benötigen sie nur zwei Dinge: Daten, die im Magnetband einer Bankkarte gespeichert sind und den dazugehörigen PIN-Code. Um an diese Informationen zu gelangen, genügen kleine technische Manipulationen an einem Geldautomaten, Billettautomaten oder einer anderen Zahlstelle. Mit einem über dem normalen Kartenschlitz angebrachten Lesegerät wird der Magnetstreifen gelesen und durch manipulierte Tastaturen, Minikameras oder eine Beobachtungsperson wird der PIN-Code ermittelt. Sobald die Betrüger im Besitz dieser Daten sind, können sie eine Kopie der Bankkarte herstellen und damit irgendwo auf der Welt Bargeld vom betroffenen Konto abheben.

2. Wie schützen Sie sich vor Betrügern?

Um sich vor einem derartigem Betrug zu schützen, gilt es folgende Verhaltensregeln zu beachten:

- Prüfen Sie vor einer Transaktion, ob am Geldautomaten/Lesegerät Manipulationen vorgenommen wurden. Achten Sie dabei insbesondere auf auffällige Abdeckungen oder bewegliche Teile. Vermuten Sie, dass ein Automat manipuliert wurde, benutzen Sie diesen keinesfalls und informieren Sie die betreffende Bank oder die Polizei.
- Achten Sie bei der Eingabe des PIN-Codes darauf, dass Sie die Tastatur mit der freien Hand abdecken. Stellen Sie zudem sicher, dass Sie nicht beobachtet werden. Sollte Ihre Karte in einem Geldautomaten stecken bleiben, nehmen Sie sofort Kontakt mit Ihrer Bank auf, um die Karte zu sperren. Bleiben Sie dabei beim Automaten, bis Ihre Karte gesperrt ist.
- Kontrollieren Sie regelmässig Ihre Kontoauszüge auf verdächtige Ausgaben oder Bargeldbezüge.

3. Was ist zu tun im Schadensfall?

Wird Ihre Karte eingezogen oder stellen Sie unerklärliche Abbuchungen auf Ihrem Konto fest, melden Sie dies unverzüglich Ihrer Bank (bzw. Sparkasse oder Postfinance).

4. Muss mir die Bank das Geld ersetzen?

Bisher (Stand Juni 2011) haben alle Banken die gestohlenen Beträge zurückerstattet. Einige Banken stellen sich auf den Standpunkt, dass sie dies aus „Kulanz“ gegenüber Ihren Kunden tun. Die SKS sieht dies anders: Die Banken sind verpflichtet, das Geld zurückzuerstatten, wenn der Bankkunde die üblichen Sorgfaltspflichten im Umgang mit Kredit- oder Debitkarten eingehalten hat. „Übliche Sorgfaltspflichten“ sind zum Beispiel, dass Sie den PIN-Code nicht auf der Karte notieren und auch nicht Ihr Geburtsdatum, Auto- oder Telefonnummer als Code verwenden. Zudem Sie sind verpflichtet, regelmässig Ihre Kontoauszüge zu überprüfen. Ihre detaillierten Sorgfaltspflichten finden Sie in den Allgemeinen Geschäftsbedingungen (AGB) Ihres Finanzinstituts.

Sind Sie Opfer eines Skimming-Betrugs geworden, haben alle Sorgfaltspflichten eingehalten und Ihre Bank weigert sich, den Schaden zu ersetzen? Melden Sie sich bei uns!

Stiftung für Konsumentenschutz SKS
Monbijoustrasse 61
Postfach
3000 Bern 23
Tel. 031 370 24 24
Fax: 031 372 00 27
info@konsumentenschutz.ch

5. Ist eine Versicherung gegen den Kartenmissbrauch sinnvoll?

Der Versicherungskonzern Allianz Suisse bietet eine Versicherung (Kontoschutzbrief) gegen den missbräuchlichen Zugriff auf Bankkonten an. Die SKS empfiehlt den Abschluss einer Versicherung allerdings nicht, da sie kaum je zum Tragen kommen wird: Einerseits wird die Allianz wohl bei grober Fahrlässigkeit den Schaden nicht übernehmen, andererseits haftet bei Einhaltung der Sorgfaltspflichten die Bank für den entstandenen Schaden.

Bern, Juni 2011