
**THEMA** **Manipulationen von Geldautomaten**

# *Vorsicht Skimming!*

**Wie Ihr Konto „geplündert“ wird …**

Wir wollen,
dass Sie
sicher leben.

Ihre Polizei

Kompetent. Kostenlos. Neutral.

## WAS IST SKIMMING?

Der englische Begriff „Skimming" bedeutet „Abschöpfen" oder „Absahnen" und steht für eine Methode, illegal Magnetstreifendaten und PIN von Kredit- und Debitkarte (z. B. girocard, früher auch als ec-Karte bezeichnet) „auszuspähen". Bundesweit ist bei diesen Straftaten in den letzten Jahren ein Anstieg zu verzeichnen.

Beim „Skimming" werden illegal die Magnetstreifendaten der Karten ausgelesen und auf Kartenrohlinge, sogenannte White Plastics, übertragen. Damit heben die Täter im Ausland – zusammen mit der ebenfalls ausgespähten PIN – Geld vom Konto der Opfer ab. Denn in außereuropäischen Staaten genügt es, den Magnetstreifen zu fälschen, um in Kombination mit der PIN an das Geld der Opfer zu kommen. In Deutschland werden nur Karten mit einem sogenannten EMV Daten-Chip akzeptiert. Da die „echte" Karte in der Regel im Besitz des Eigentümers verbleibt, bemerkt der Inhaber des Kontos diesen Angriff meist erst mit der Abholung der Kontoauszüge oder wenn die Bank nach Überziehung des Dispositionskreditrahmens einschreitet.

## VORGEHENSWEISE DER TÄTER:

Um in den Besitz der Kartendaten zu kommen, installieren die Täter vor dem Karteneinschubschacht der Geldautomaten ein eigens hergestelltes Kartenlesegerät oder sogar eine vollständige Frontplatte.

Diese von den Tätern benutzten Kartenleser sind optisch dem Modell des Geldautomaten angepasst (gleiche Farbe, gleiche Aufkleber) und so hergestellt, dass die eingeschobene Zahlungskarte durch das illegale Lesegerät zum originalen Kartenleser weitertransportiert wird. So werden die Magnetstreifendaten ausgelesen und gespeichert, ohne dass die Bedienung des Geldautomaten beeinträchtigt und der Kunde misstrauisch wird. Der Auszahlungsvorgang erfolgt für sie störungsfrei.

Die Eingabe der PIN wird mit einer Mini-Kamera gefilmt, die oft oberhalb der Tastatur in einer angeklebten Kameraleiste versteckt ist. Diese Kameraleiste ist in der Regel an Form und Farbe des Geldautomaten angepasst und selbst für argwöhnische Benutzer kaum erkennbar. Es kommen aber auch manipulierte Tastaturfelder zum Einsatz, die über die eigentliche Tastatur geklebt werden. Damit kann die per Tastendruck eingegebene PIN aufgezeichnet werden.

## SO SCHÜTZEN SIE SICH VOR SKIMMING:

Eine andere Variante ist – soweit noch vorhanden – die Manipulation des Kartenlesers am Türöffner des Geldinstituts. Die Täter tauschen hierzu äußerlich nicht erkennbar den original Kartenleser gegen einen manipulierten aus. Die PIN-Eingabe wird dann (wie beschrieben) mittels Minikamera am Geldautomaten aufgezeichnet. Ebenso kann der Magnetstreifen an manipulierten Kontoauszugsdruckern oder SB-Überweisungsterminals sowie an Fahrkarten- oder Zapfsäulenautomaten ausgelesen werden.


- Gehen Sie bitte sorgsam mit Ihren Zahlungskarten um und bewahren Sie die PIN stets getrennt von der Karte auf.

- Sofern Sie im Besitz mehrerer Zahlungskarten sind, sollten Sie den Türöffner eines Bankinstituts nicht mit der gleichen Karte betätigen, mit der Sie anschließend Geld abheben möchten.

- Geben Sie Ihre PIN niemals am Türöffner eines Bankinstituts ein. Kein Geldinstitut verlangt für den Zugang zum Geldautomaten die Eingabe der PIN. Der Kartenleser hat immer nur die Funktion des Türöffners.

- Achten Sie darauf, dass die Eingabe Ihrer PIN nicht von anderen beobachtet werden kann. Sorgen Sie für einen ausreichenden Sicherheitsabstand zum nächsten Kunden und bitten Sie ggf. den hinter Ihnen stehenden Kunden, Abstand zu halten.

- Decken Sie während der PIN-Eingabe das Tastaturfeld mit der anderen Hand oder einem Gegenstand (z. B. Geldbörse, Blatt Papier) als Sichtschutz vollständig ab. Das erschwert das „Ausspähen" per Kamera oder Foto-Handy erheblich.

- Benutzen Sie soweit möglich immer denselben Geldautomaten für Abhebungen, so dass Ihnen mögliche Veränderungen am Gerät auffallen.

- Nutzen Sie keinen Geldautomaten, an dem Ihnen etwas ungewöhnlich erscheint, z. B. angebrachte Leisten oder Verblendungen, abstehende und vor allem lockere Teile, Spuren von Kleber rund um den Kartenschlitz.

- Bei Verdacht auf Manipulation verständigen Sie umgehend die Polizei und das Geldinstitut.

## WEITERE MASSNAHMEN:

- Kontrollieren Sie regelmäßig Ihre Kontoauszüge und wenden Sie sich bei Auffälligkeiten sofort an Ihre Bank.

- Prüfen Sie, ob Sie den Auslandsverfügungsrahmen Ihres Kartenkontos begrenzen oder sogar auf Null setzen können. Ihre Karte – aber auch eine hergestellte Dublette – lässt sich dann im Ausland nur begrenzt bzw. gar nicht einsetzen.

- Bei dem Verdacht der Ausspähung Ihrer Kartendaten lassen Sie bitte umgehend die Karte über Ihre Bank bzw. den bundesweiten Sperr-Notruf unter 116 116 sperren und erstatten Sie Anzeige bei der Polizei.

Fotos:
Bayerisches Landeskriminalamt,
Landeskriminalamt Baden-Württemberg,
Landeskriminalamt Sachsen,
Rüdiger Kottmann und
www.kartensicherheit.de.

Karte verloren oder gestohlen? Dann sperren Sie diese am besten sofort unter der zentralen Notruf-Nummer:

**SPERR-NOTRUF**
**116 116**

Sofern sich Ihr Kartenherausgeber nicht dem Sperr-Notruf 116 116 angeschlossen hat, verwenden Sie bitte folgende Rufnummern:

- **Debitkarte** (früher ec-Karte)**: +49 - 1805 - 021 021** [1]
- **Mastercard** (nur Deutschland)**: 0800 - 819 1040** [2]
  - international (R-Gespräch)**: +1 - 636 7227 111**
- **VISA-Card** (nur Deutschland)**: 0800 - 811 8440** [2]
  - international (R-Gespräch)**: +1 - 410 581 9994**
- **American Express: +49 - 69 - 97 97 1000** [3]
- **Diners Club: +49 - 1805 - 07 07 04** [1]

[1] 14 Ct./Min. (inkl. USt.) aus dem dt. Festnetz, Mobilfunkhöchstpreis 42 Ct./Min. (inkl. USt.), abweichende Gebühren aus dem Ausland

[2] Kostenfrei aus dem dt. Festnetz, abweichende Gebühren aus dem Ausland und über Mobilfunk

[3] Gebühren der dt. Telekom innerhalb Deutschlands, abweichende Gebühren aus dem Ausland

Alle Angaben ohne Gewähr.

**Weitere Informationen erhalten Sie bei Ihrem Geldinstitut, bei den (Kriminal-) Polizeilichen Beratungsstellen und im Internet unter:**

**www.polizei-beratung.de/skimming**
**www.kartensicherheit.de**
**www.sperr-notruf.de**

**Dieses Faltblatt wurde ausgehändigt von:**

(00V)125.2011.07

Herausgeber:
Programm Polizeiliche Kriminalprävention
der Länder und des Bundes,
Zentrale Geschäftsstelle,
Taubenheimstraße 85, 70372 Stuttgart
E-Mail: info@polizei-beratung.de

Wir wollen,
dass Sie
sicher leben.

Ihre Polizei

www.polizei-beratung.de