Präventionstipps

- **Schauen** Sie sich den **Karteneingabeschlitz** der Eingangstür und des Geldausgabeautomaten **genau an**, bevor Sie die Karte einführen. Im Zweifel sollten Sie das Personal des Geldinstitutes verständigen.

- Schauen Sie sich den Geldausgabeautomaten genau an, ob z. B. eine **Leiste zur Aufnahme einer Minikamera** angebracht sein könnte. Sie dient der Ausspähung Ihrer PIN.

- Auch **Prospekthalter o. ä. in Automatennähe** könnten eine Minikamera verbergen.

- Schauen Sie sich die Tastatur des Geldausgabeautomaten genau an. **Seien Sie misstrauisch**, wenn die Tastatur nicht richtig sitzt.

- Sprechen Sie mit Ihrem Geldinstitut über eine automatische **Sperrung Ihrer Karte** für Geldabhebungen **im Ausland** und vereinbaren Sie einen persönlichen Verfügungsrahmen für die Dauer Ihrer Auslandsreise.

Immer daran denken! Bei Verdacht:

- Bank informieren
- Karte sperren
- Sperrnotruf 116 116 anrufen
- Anzeige bei der Polizei erstatten

Grußwort

Immer häufiger lesen wir in den Medien Meldungen über das illegale Ausspähen von Bankdaten an Geldautomaten. Täterinnen und Täter erhalten darüber Zugang zu fremden Konten und räumen diese anschließend leer. Dabei gehen sie absolut geschickt vor: Sie installieren ein kleines Kartenlesegerät über dem eigentlichen Kartenschlitz oder spähen die Geheimzahl mithilfe einer Kamera oder einem aufgelegten Tastenfeld aus. Mit den erhaltenen Daten werden Kopien der Geldkarten gefertigt, mit denen dann im Ausland Geld abgehoben wird.
Zwar bekommen die Betroffenen bei einem nachweisbaren Skimming-Angriff ihren finanziellen Schaden ersetzt, doch empfiehlt sich grundsätzlich höchste Aufmerksamkeit beim Geld abheben.
Erste Hilfe zur Orientierung und Präventionstipps bietet Ihnen das vorliegende Faltblatt. Und denken Sie dran: Informieren Sie bei einem Verdacht sofort Ihre Bank, um Ihre Karte sperren zu lassen. Vergessen Sie außerdem nicht, Anzeige zu erstatten. Nur so kann den Skimming-Angriffen Einhalt geboten werden.

Geben Sie Acht!

Ihr

Holger Stahlknecht

Minister des Innern des Landes Sachsen-Anhalt

Skimming

Datendiebstahl an Geldausgabeautomaten

SACHSEN-ANHALT
Ministerium des Innern

Präventionstipps

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

- **Wichtig! Verdecken Sie die Tastatur** bei der Eingabe der PIN immer **mit der Hand** oder z. B. einer Zeitung bei den Kartenleseterminals an den Kassen des Einzelhandels.

- Es wird **zum Öffnen einer Eingangstür niemals die PIN abgefragt**. Wenn doch, verständigen Sie die Polizei und das Geldinstitut.

- Achten Sie auf Personen, die sich Ihnen verdächtig nähern (**Sicherheitsabstand**) und lassen Sie sich nicht ablenken.

- **Geben Sie niemals mehrfach Ihre PIN ein**, auch nicht, wenn Sie eine unbekannte Person dazu auffordert.

- **Erscheint** Ihnen **etwas ungewöhnlich**, die **Karte nicht benutzen**, suchen Sie dann ein **anderes Geldinstitut** auf.

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

- **Nutzen Sie** überwiegend Ihnen **bekannte Geldausgabeautomaten** möglichst zu Banköffnungszeiten.

Skimming

Skimming (englischer Begriff) bedeutet soviel wie „Abschöpfen“ oder „Absahnen“.

Der Begriff steht für eine Methode, illegal elektronische Daten von Zahlungskarten (ec-Karte oder Kreditkarte) „auszuspähen“. Dabei setzt sich die Begehungsweise aus zwei strafrechtlich separaten Tatbeständen zusammen:

- Ausspähen/Abfangen von Daten (§ 202a StGB),
- Vorbereitung bzw. Fälschung von Zahlungsmitteln (§§ 152a, 152b StGB i. V. m. § 149 StGB).

Mit den auf diese kriminelle Art erlangten Daten werden Kopien der Geldkarten gefertigt. Damit können die Täter ausschließlich im Ausland Geld von den Konten abheben.

Welche Automaten sind betroffen?
Wo stehen sie?

Skimming findet vorwiegend in Geld- und Kreditinstituten statt.
Aber auch alle anderen Bereiche des unbaren Zahlungsverkehrs, z. B. Einkaufscenter oder Tankstellen, können von Skimming-Straftaten betroffen sein.

Arbeitsweise der Täter

originale Frontplatte

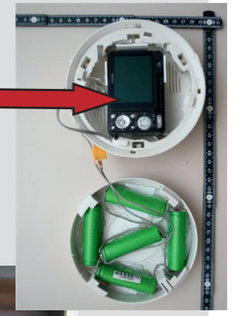
manipulierte Frontplatte

Skimming richtet sich zunächst auf das Ausspähen gespeicherter Daten, die sich auf dem Magnetstreifen der Zahlungskarten befinden. Dies geschieht vor allem durch den Einsatz kleinster elektronischer Bauteile, die rund um die Lesemodule für Zahlungskarten am Geldausgabeautomaten oder anderen Lesegeräten, z. B. an den Eingangstüren, angebracht werden.

Um in den Besitz der Daten auf dem Magnetstreifen zu kommen, installieren die Täter vor dem originalen Karteneinschubschacht zusätzlich ein manipuliertes Aufsatzkartenlesegerät oder vor dem originalen Kartenschacht am Geldausgabeautomaten eine komplette Frontplatte.

Diese manipulierten Kartenleser sehen genauso wie der Kartenleser des Geldausgabeautomaten aus und werden so hergestellt, dass die eingeschobene Bankkarte durch das illegale Lesegerät zum originalen Kartenleser weitertransportiert wird.
So werden die Kontodaten durch das manipulierte Aufsatzkartenlesegerät ausgelesen und gespeichert. Das Geldabheben am Geldausgabeautomaten verläuft für den Kunden störungsfrei.

Daran schließt sich das Ausspähen der PIN an, wofür die Täter unter Zuhilfenahme von fototechnischen Modulen, z. B. Kamera, Fotohandy, die Eingabe der PIN am Automaten optisch erfassen.



Eine weitere Begehungsart ist die Verwendung einer Aufsatztastatur, die die Eingabe der PIN als elektronischen Impuls erkennt.

Impressum

Herausgeber: Ministerium des Innern des Landes Sachsen-Anhalt, Pressestelle
Halberstädter Straße 2/am „Platz des 17. Juni“
39112 Magdeburg
www.mi.sachsen-anhalt.de E-Mail: pressestelle@mi.sachsen-anhalt.de

Landeskriminalamt Sachsen-Anhalt
Lübecker Straße 53-63
39124 Magdeburg
www.polizei.sachsen-anhalt.de E-Mail: praevention.lka@polizei.sachsen-anhalt.de

Gestaltung/Herstellung: Medienzentrum der Polizei des Landes Sachsen-Anhalt
Fachhochschule Polizei Sachsen-Anhalt
Schmidtmannstraße 86
06449 Aschersleben

Fotos: Bundeskriminalamt und Landeskriminalämter

Weitere Hinweise finden Sie im Internet unter: www.kartensicherheit.de
www.polizei-beratung.de