MAIFELD
Sicherheitsberater für Senioren

Betrug an Geldautomaten

Variante 1: Skimming

Wenn Geldautomaten manipuliert werden, um die Daten von Kredit- oder Bankkarten auszuspähen, spricht man von Skimming. Trotz verbesserter Sicherheitstechnik und der steigenden Aufklärung, können Betrugsfälle nicht komplett verhindert werden.

Skimming – Was ist das?

Unter Skimming versteht man das illegale Auslesen von Kredit- oder Girokarten (Debitkarten) an Bankautomaten oder Terminals. Betrüger haben es dabei auf die Bankinfomationen auf den Magnetstreifen der Karten abgesehen. Sie erstellen davon eine Kartendoublette. Zusammen mit der ausgespähten PIN lassen sich Betrüger dann Bargeld auszahlen oder bezahlen damit in Geschäften – zulasten des Karteninhabers. Die gute Nachricht: In Deutschland hat der Magnetstreifen heute keine Bedeutung mehr, da über den Chip in der Karte gezahlt oder Geld abgehoben wird. Im außereuropäischen Ausland nutzen Banken den Magnetstreifen jedoch weiterhin.

Wie kommen Betrüger an Magnetstreifen und PIN?

Um an die wichtigen Bankdaten zu gelangen, manipulieren Kriminelle Geldautomaten oder Kartenlesegeräte in Geschäften. An Automaten bringen sie hierzu ein zusätzliches Lesegerät vor dem Karteneinschub an. Der Magnetstreifen der Karte wird ausgelesen und dann auf einer Kartendoublette gespeichert.

Um die dazugehörige PIN abzufangen, gibt es verschiedene Varianten: Betrüger kleben eine kleine Kameraleiste über die Tastatur und filmen die PIN-Eingabe. Illegale Kameras sind aber auch in Prospekthaltern oder als gefälschte Rauchmelder an der Decke zu finden. Die Tastatur selber kann ebenfalls manipuliert sein. Hier kommt ein zweites Tastenfeld zum Einsatz, das über dem echten Tastenfeld angebracht wird – ein sogenannter Skimmer. Dieser zeichnet die Tastendrücke auf.

Der Kartenbesitzer bemerkt den Betrug häufig erst dann, wenn er die Kontoauszüge kontrolliert oder das Konto überzogen ist.

Auch andere Geräte wie

- Kontoauszugdrucker
- Überweisungsterminals
- Kartenlesegeräte in Geschäften
- Fahrkartenautomaten oder
- Zapfsäulenautomaten an Tankstellen u.ä.
- Kartenlesegeräte in Geschäften

können betroffen sein.

Eine weitere Skimming-Methode ist die Manipulation der Türöffner von Banken. Der Kunde soll seine Karte durch spezielle von den Betrügern angebrachte Aufsätze ziehen und seine PIN eingeben. Die Kartendaten werden dann im Aufsatz gespeichert.

Weniger Skimming durch Sicherheitstechnik

Da die Vorgehensweisen der Betrüger inzwischen bekannt sind, entstehen immer mehr Möglichkeiten, um Skimming zu erschweren oder ganz zu verhindern. Heute haben viele Geldautomaten bereits einen Störsender gegen Magneten und sind so konstruiert, dass das Anbringen von Skimming-Vorrichtungen erschwert wird. Intelligente Automaten erkennen Skimming-Module und schalten sich selber aus.

Magnetstreifen vs. Chip: So sicher ist EMV

Die wichtigste Entwicklung im Kampf gegen Skimming ist jedoch der EMV-Chip. Entwickelt von **E**uropay International, **M**asterCard und **V**isa, ist dieser seit 2012 EU-weit in allen Geldautomaten sowie Girocards (Debitkarten) oder Kreditkarten zu finden. Wie Eingangs erläutert, laufen Transaktionen hier seitdem nicht mehr über den Magnetstreifen, sondern über den Chip. Gefälschte Karten mit gestohlenen Magnetstreifen können in der EU deshalb nicht mehr zur Bargeldauszahlung oder zum Bezahlen verwendet werden.

Ein weiterer Vorteil des Chips: Er ist extrem fälschungssicher. Die sensiblen Bankinformationen sind darauf verschlüsselt abgespeichert. Außerdem kann der EMV-Chip nicht vervielfältigt oder verändert werden.

Aber: Außerhalb der EU sind Geldautomaten und Terminals bisher nicht flächendeckend mit EMV-Funktion ausgestattet. **Deshalb haben alle Girocards und Kreditkarten auch heute noch zusätzlich einen Magnetstreifen**. Ohne ihn wäre eine Bargeldauszahlung oder das Bezahlen im außereuropäischen Ausland oft nicht möglich. Aus diesem Grund versuchen Kriminelle noch immer, an die Daten aus dem

Magnetstreifen zu kommen. Sie nutzen die gefälschten Karten dort, wo Sicherheitsmaßnahmen bisher nicht ausreichend vorhanden sind.

Wie gefährlich ist Skimming wirklich?

Durch die vielen Sicherheitsmaßnahmen kommt Skimming bundesweit nicht allzu oft vor. 2017 gab es nur 499 Fälle von manipulierten Geldautomaten. Betrüger entwickeln jedoch immer neue Techniken, um Bankdaten abzugreifen. So nutzen sie mittlerweile auch Kartenlesegeräte in Geschäften, da diese nicht so gut geschützt sind wie Automaten. Auch das sog. „Deep-Insert-Skimming“ taucht immer häufiger auf. Dabei wird eine kleine Wanze in den Kartenschlitz eingeführt, die die Kartendaten ausliest und speichert. Anders als der Aufsatz ist sie mit bloßem Auge nicht zu erkennen.

Wie kann ich mich vor Skimming schützen?

1. Gehen Sie vorsichtig mit Ihren Zahlungsdaten um. Bewahren Sie nie Ihre Karte und Ihren PIN gemeinsam auf.
2. Überprüfen Sie immer den Geldautomaten: Gibt es ungewöhnliche Verblendungen oder Leisten? Versuchen Sie, leicht daran zu ziehen, oft sind diese nicht fest angebracht.
3. Nutzen Sie Geldautomaten nicht, wenn Ihnen etwas komisch vorkommt.
4. Meiden Sie Automaten in Außenbereichen. Diese können häufiger manipuliert sein, da sie nicht beaufsichtigt werden.
5. Schützen Sie die PIN-Eingabe immer mit Ihrer freien Hand.
6. Haben Sie mehrere Karten? Nutzen Sie eine immer zum Öffnen der Filialtür und die anderen zum Abheben und Zahlen.
7. Geben Sie niemals Ihre PIN ein, wenn Sie die Tür zur Filiale öffnen. Keine Sparkasse oder Bank würde das verlangen.

Sie sind Opfer von Skimming geworden – Was jetzt?

Haben Sie den Verdacht, dass eine fremde Person Geld von Ihrem Konto abgebucht hat? Dann setzen Sie sich sofort mit Ihrer Sparkasse oder Bank in Verbindung. Diese nimmt den Fall auf und sperrt Ihre Karte. Wenn es schnell gehen muß, können Sie Ihre Karte auch selber sperren lassen. Das geht unter der Telefonnummer **116116.** Waren Sie nicht grob fahrlässig, ersetzt Ihr Finanzinstitut den gestohlenen Betrag. Melden Sie den Fall unbedingt der Polizei und erstatten Sie Anzeige gegen unbekannt.

Sperr-Notruf

Rufen Sie die 116 116 an.

Der Sperr-Notrufdienst ist die zentrale Anlaufstelle zur Sperrung elektronischer Berechtigungen. Halten Sie einfach Ihre Kontonummer und Bankleitzahl (BLZ) oder Ihre IBAN bereit.

Die Notruf-Telefonnummer 116 116 steht Ihnen rund um die Uhr zur Verfügung und ist in Deutschland kostenlos. Gebühren bei einem Anruf der Nummer +49 116 116 aus dem Ausland sind abhängig vom jeweiligen Telefonanbieter/Netzbetreiber.

Variante 2: Zeigen Sie Datenspionen die kalte Schulter

Ausspähen sensibler Daten

Kriminelle brauchen gar nicht immer besonders raffinierte Methoden, um an ihr Ziel zu kommen. Per Shoulder Surfing werden Geheimzahlen, Passwörter und sensible Daten ausgespäht. Der Begriff lässt sich sinngemäß übersetzen mit „jemandem über die Schulter schauen“. So einfach die Methode, so schwerwiegend oft die Konsequenzen. Hier erfahren Sie, wie Shoulder Surfer versuchen, fremde Daten auszuspähen und erhalten Tipps, wie Sie sich vor der Gefahr am besten schützen können.

Das Ausspähen von Daten wie PINs, Passwörtern oder sonstigen Zugangsdaten per Blick über die Schulter ist eine einfache Masche, um das Geld von Bürgern zu stehlen oder Zugriff auf ihre online gespeicherten Daten zu ergattern.

Das Phänomen ist bundesweit verbreitet.

Die Tricks der Datenspione sind vielseitig: Unterschieben gefälschter Bankkarten, Vortäuschen defekter Geldautomaten, Analyse von Fingerbewegungen bei Eingaben an Tastaturen. Das Schützen der eigenen Daten ist daher wichtig. Oft gelingt es Kriminellen schon mit einfachsten Methoden, PINs und andere vertrauliche Informationen auszuspähen.

Was ist Shoulder Surfing?

Beim Shoulder Surfing erspähen Betrüger - sogenannte Shoulder Surfer - per Blick über die Schulter persönliche Daten, etwa Geheimzahlen (Persönliche Identifikationsnummer, PIN) von Kredit- oder Bankkarten oder Passwörter von Online-Konten, um an das Geld ihrer Opfer zu kommen..

Sie beobachten dafür ihre Zielpersonen bei der alltäglichen Verwendung elektronischer Geräte in der Öffentlichkeit. Dies geschieht beim Bargeldabheben am Geldautomaten, beim Eingeben von Passwörtern oder Sicherheitscodes am Smartphone, am Tablet- oder Desktop-PC oder an Bezahlterminals an Einkaufskassen.

Schon gewusst: Vielfach ist die Rede von Datendiebstahl. Dabei gibt es genaugenommen keinen Diebstahl von Daten. Denn die Daten bleiben in den allermeisten Fällen erhalten. Angreifer spähen die Daten rechtswidrig aus, kopieren und übertragen sie. Und sie missbrauchen dann die Informationen für ihre Zwecke.

Kriminelle haben häufig leichtes Spiel

Viel zu oft haben Datenspione in unserer digitalen Welt leichtes Spiel: Sie schauen uns über die Schulter, wenn wir in der vollen U-Bahn stehen und uns mit persönlichen Passwörtern in unsere Online-Shopping-Accounts einloggen, Kreditkartendaten und Adressen hinterlegen. In der Mittagspause sind sie dabei, wenn das Lokal um die Ecke kurzerhand zum Büro wird, indem noch schnell die aufgeschobenen Bankgeschäfte am Tablet oder Laptop erledigt werden.

Selten macht man sich in diesen alltäglichen Situationen Gedanken über die Sicherheit geheimer Daten. Personen hinter einem am Tisch, am Automaten oder in der Bahn haben freie Sicht auf Bildschirme und Tastaturen und können Daten abgreifen, indem sie Fingerbewegungen bei der Eingabe erschließen. Die erspähten Nummern werden später für unerlaubten Zugriff auf Daten oder Konten genutzt.

So gehen Shoulder Surfer vor

Um an die Daten zu kommen, gehen Täter unterschiedlich vor. Zwei Aspekte lassen sich hierbei unterscheiden:

1. Direkte Beobachtung

Die Betrüger schauen ihrer Zielperson direkt über die Schulter und erspähen beispielsweise die PIN von Bankkarten, während sie am Geldautomaten eingetippt wird.

Nachdem sie die PIN ausgespäht haben, lenken die Täter ihre Opfer noch am Automaten ab, um deren Bank- oder Kreditkarte zu stehlen. Diese wird dann entweder direkt durch eine gefälschte Karte ausgetauscht, damit der Diebstahl nicht sofort bemerkt wird. Oder die Täter gaukeln dem Opfer vor, die Karte wäre vom Automaten eingezogen worden. Mit der gestohlenen PIN plus Bankkarte können die Shoulder Surfer nun problemlos das Konto der Betroffenen plündern.

Die Tricks der Täter, ihre Opfer am Automaten abzulenken, sind vielseitig.

Ein Fallbeispiel:

In Rheinland-Pfalz arbeiteten in einem Fall, von dem die Verbraucherzentrale berichtete, zwei Täter gemeinsam: Einer spähte am Geldautomaten die PIN des Opfers aus und lenkte anschließend das Opfer am Geldautomaten ab, um unauffällig die Bankkarte aus dem Eingabefach des Automaten zu stehlen. Beides zusammen steckte er seinem Komplizen zu, der am benachbarten Ausgabeautomaten stand. Vorgeblich wegen der fehlenden Karte lotste er sein Opfer aus der Bank, sodass der Mittäter Geld vom Konto des Opfers abheben und die Karte in den ursprünglichen Geldautomaten zurückstecken konnte. Weil sich die Karte dort wieder anfand, hielt die betrogene Bankkundin den Vorgang für ein folgenloses Versehen. Erst später stellte sie fest, dass man sie betrogen und Geld von ihrem Konto abgehoben hatte.

Manchmal genügen den Kriminellen sogar einfach schon gute Ohren – etwa hier: Ein Familienmitglied ruft Sie an mit der Bitte, einen Online-Einkauf mit Ihrer Kreditkarte bezahlen zu dürfen. Arglos lesen Sie Ihre Kreditkartennummer am Telefon vor – zum Beispiel, während Sie am Flughafen im vollen Terminal auf die Abfertigung warten. Ein fataler Fehler, denn damit öffnen Sie auch kriminellen Zuhörern Tür und Tor für illegale Online-Einkäufe.

2. Mit Hilfsmitteln

Noch argloser sind die Opfer in der Regel, wenn sie von Kriminellen aus der Ferne – etwa mit Kamera oder Fernglas – ausgespäht werden. Denn oft reichen zum Beispiel schon Videos mit den Bewegungen der Finger über das Display eines Smartphones aus, um Eingaben wie den Sicherheitscodes zu ermitteln – selbst wenn das Display selbst nicht oder nur schlecht im Video zu sehen ist. Schließlich können Kriminelle solches Videomaterial ungestört analysieren und die gewünschten Informationen herausfiltern.

Shoulder Surfing – eine nicht zu unterschätzende Gefahr

Mit den gestohlenen Daten und Bankkarten können Täter im Namen der Opfer einkaufen, Geld von deren Konto abheben oder anderen Missbrauch begehen. Aber nicht nur im privaten Bereich kann Shoulder Surfing ernsthafte Schäden verursachen.

Auch für die Datensicherheit von Unternehmen und deren Kundinnen und Kunden stellt diese kriminelle Methode ein Risiko dar. Mitarbeiterinnen oder Mitarbeiter, die in der Öffentlichkeit am Dienst-Laptop beispielsweise Anmeldeinformationen für

Firmen-Tools oder andere vertrauliche Daten eingeben, laufen Gefahr, von Datenspionen beobachtet zu werden.

Das Ausspähen von Daten ist in Deutschland strafbar

und wird mit einer Geldstrafe beziehungsweise einer Freiheitsstrafe von bis zu drei Jahren geahndet. Je nach Missbrauch der Daten sind weit höhere Strafen möglich. Häufig machen sich Betrüger in diesen Fällen nicht nur wegen Ausspähen strafbar, sondern auch wegen Diebstahl, Betrug und Fälschung, zum Beispiel von Bankkarten.

Diese Maßnahmen schützen Sie vor Shoulder Surfing

1. Achten Sie bei der Eingabe von PINs und Passwörtern immer darauf, dass Sie von niemandem beobachtet werden können.
2. Decken Sie Tastaturfelder gegebenenfalls mit einer Hand oder einem Gegenstand ab.
3. Lassen Sie Ihre Bankkarten nicht aus den Augen.
4. Vergewissern Sie sich, dass Sie einen ausreichenden Sicherheitsabstand zu anderen Personen haben.
5. Bitten Sie (angeblich) hilfesuchende Personen darum, zu warten bis Sie fertig sind und bis dahin Abstand zu halten.
6. Überprüfen Sie Bankautomaten: Manipulationen (sogenanntes Skimming), wie montierte Anbauteile, um Magnetstreifen auszulesen oder Kartendaten auszuspähen, sind keine Seltenheit. Fällt Ihnen Ungewöhnliches auf, meiden Sie solche Geldautomaten und informieren Sie Bankmitarbeiterinnen oder -mitarbeiter oder verständigen Sie die Polizei.
7. Lässt es sich nicht vermeiden, in der Öffentlichkeit mobile Bankgeschäfte zu tätigen oder andere sensible Daten an Laptop, Tablet oder Smartphone einzugeben, erhöhen Sie schon mit einfachen Maßnahmen die Sicherheit:
8. Suchen Sie einen geschützten Platz, beispielsweise mit dem Rücken zur Wand.
9. Nutzen Sie Blickschutzfilter für Displays.
10. Verwenden Sie einen Passwortmanager, mithilfe dessen Sie nicht mehr jedes Passwort einzeln, sondern nur noch ein Masterpasswort eingeben müssen, den Rest erledigt der Manager für Sie.
11. Brechen Sie im Zweifelsfall die Transaktion ab.
12. Bei Verdacht auf Kartenmissbrauch lassen Sie umgehend Ihre Karte sperren. Der bundesweite Sperrnotruf: **116 116** (aus dem Ausland mit der Vorwahl für Deutschland +49).

13. Bei Unsicherheiten lassen Sie sich von Ihrer Bank vor Ort beraten. Sie sperrt auch Ihre Karten für Sie.
14. Prüfen Sie das Limit für das Abheben von Bargeld Ihres Kontos. Je höher das Limit, desto höher der Schaden bei kriminellen Übergriffen. Passen Sie die Höhe gegebenenfalls an.

In jedem Fall gilt: Scheuen Sie sich nicht, stets die Polizei zu verständigen!

Zentrale Sperrrufnummer für Karten: (+49) – 116 116

Die Nummer steht Ihnen rund um die Uhr zur Verfügung und ist in Deutschland kostenlos. Kosten bei einem Anruf aus dem Ausland sind abhängig vom jeweiligen Anbieter/Netzbetreiber.

Datenspione können überall sein. Gehen Sie nicht leichtfertig mit Ihren Daten um und achten Sie stets auf erhöhte Sicherheitsmaßnahmen bei der Benutzung elektronischer Geräte in der Öffentlichkeit. So wappnen Sie sich gegen Shoulder Surfing.

Variante 3: Cash-Trapping

Das so genannte Cash-Trapping bezeichnet eine besondere Form des Diebstahls an Geldautomaten. Über den Geldausgabeschacht wird ein täuschend echter Verschluss geklebt. Dieser Verschluss ist innen mit einer Klebefolie versehen. Diese verhindert, dass das Geld ausgegeben oder wieder vom Automaten eingezogen wird - die Geldscheine bleiben buchstäblich im Ausgabeschacht kleben.

Vorgehen: Manipulierter Geldauswurf

Der Geldautomat funktioniert einwandfrei: Der Bankkunde kommt nur nicht an sein abgehobenes Geld, da der Geldauswurf nicht geöffnet wird. Stattdessen erscheint nach einer Weile der Hinweis auf eine Störung. Die meisten Kunden verlassen daraufhin die Bank, um ihr Glück an einem anderen Geldautomaten zu versuchen. Dann ist für den Dieb die Stunde gekommen - er kann die Blende schlicht entfernen und mit den darin „festgeklebten“ Scheinen verschwinden.

So schützen Sie sich vor den Tricks der Diebe am Geldautomaten

1. Bleiben Sie in jedem Fall beim Geldautomaten. Lassen Sie sich nicht von einem vermeintlich hilfsbereiten Fremden vom Automaten weglocken.
2. Bitten Sie einen anderen Kunden, einen Bankmitarbeiter zu holen. Bei Automaten außerhalb von Banken rufen Sie gegebenenfalls per Handy bei der Bank an.

3. Verständigen Sie die Polizei außerhalb der Öffnungszeiten von Banken und Kreditinstituten.

Polizeiliche Kriminalstatistik 2023

Zahlungskartenbetrug in Deutschland (bis 2015 Debitkartenbetrug)

.

2023 wurden insgesamt 26.734 Fälle des Zahlungskartenbetrugs mit PIN erfasst, die Schadenssumme lag bei über 36,6 Millionen Euro. Die Zahl der Betrugsfälle im Bereich rechtswidrig erlangter Zahlungskarten ohne PIN lag bei 16.241, der Schaden belief sich auf 5,0 Millionen Euro. Insgesamt wurden bei Betrugsfällen im Bereich rechtswidrig erlangter Zahlungskarten mit PIN 4.035 Tatverdächtige erfasst, bei den Fällen ohne PIN waren es 1.992. Die Aufklärungsquote lag bei 27,3 Prozent (mit PIN) bzw. 18,5 Prozent (ohne PIN).

Der Text wurde auf der Grundlage amtlicher Daten und Empfehlungen der Kriminalprävention der Polizei und des Bundeskriminalamtes verfasst.