Typischer Fall: Betrüger montieren auf den Kartenschlitz des Automaten einen Aufsatz, der die Daten vom Magnetstreifen der Girocard ausliest. Kunden merken das nur, wenn sie am Einzugsschacht rütteln.

Die Tricks der Betrüger

Bank- und Kreditkarten. Kunden können Kartenbetrug vorbeugen. Tappen sie dennoch in die Falle, erstatten die Banken das Geld meist.

Auf seinem Kontoauszug entdeckt Albrecht Vogel* mehrere Abbuchungen aus Costa Rica. Insgesamt fehlen 800 Euro. Der 28-Jährige wundert sich. Er war noch nie in dem mittelamerikanischen Land. Seine Girocard, wie die frühere ec-Karte inzwischen heißt, trägt er in seiner Tasche.

Die Abbuchungen sind Vogel sofort aufgefallen. Er prüft seine Kontoumsätze mehrmals in der Woche im Internet. Bei der Berliner Sparkasse fragt er nach, wer von seinem deutschen Konto in Costa Rica Geld abhebt. Der Mitarbeiter tippt auf Betrug. Er sperrt Vogels Karte.

Die Sperre ist Pflicht, wenn Kunden betrügerische Buchungen feststellen, wenn sie ihre Girocard oder Kreditkarte verloren haben oder wenn eine Karte gestohlen wurde. Zieht der Bankautomat das Plastikkärtchen ein, muss es ebenfalls gesperrt werden. Statt der Bank können Kunden auch gleich die Notruf-Nummer 116 116 anrufen (siehe „Unser Rat"). Sie ist rund um die Uhr erreichbar.

Der Angestellte der Berliner Sparkasse verlangt von Vogel außerdem, dass dieser Strafanzeige bei der Polizei stellt. Betrogene Kartenbesitzer sollten immer ihr Institut fragen, ob es eine Anzeige verlangt. Sonst riskieren sie, dass die Bank oder deren Versicherung das fehlende Geld nicht erstattet.

Meist scheint die Erstattung aber zu klappen. „Bei der Rückerstattung von Geld, das Kunden durch Kartenbetrug verloren haben, zeigen sich die Institute kulant", sagt Margit Schneider vom Sicherheitsmanagement für Zahlungskarten der Euro Kartensysteme GmbH. Hier ist die zentrale Bekämpfungsstelle von Schäden mit der Girocard, die Banken und Sparkassen gemeinsam eingerichtet haben.

So kommen Betrüger an die Daten

Um die Geheimzahl zur Karte auszuspähen, bringen die Betrüger zum Beispiel eine Kamera an Geldautomaten oder an Bezahlgeräten an. Die ist so winzig, dass sie in einem stecknadelkopfgroßen Loch verschwindet. Doch es ist leicht, den Datenräubern die Sicht zu versperren. Es hilft schon, beim Eintippen der Zahl die andere Hand oder das Portmonee darüberzuhalten.

Tückischer sind manipulierte Tastaturen: Die Gangster legen über das Tastenfeld am Automaten ein zweites darüber oder kleben eine Folie auf. Die Geheimzahl wird beim Tastendrücken per Funk übertragen.

Die Betrüger brauchen jedoch nicht nur die Geheimzahl, sondern auch die Karte oder eine Kopie davon. Die stellen sie selbst her, wenn sie die nötigen Daten haben.

Sie montieren einen Aufsatz auf den Kartenschlitz, der die Daten auf dem Magnetstreifen der Girocard liest. Den Aufsatz erkennen Kunden nur, wenn sie am Einzugsschacht rütteln. Das Ausspähen der Daten heißt bei den Experten „Skimming", auf deutsch „Abschöpfen".

Am Werk sind gut organisierte Banden. Doch in Europa – abgesehen von Russland und wenigen anderen Ländern – nützen ihnen Blankokarten mit kopiertem Magnetstreifen nichts. Denn die Automaten fragen einen Prüfwert von dem Chip ab, der seit 2010 fast überall in Europa auf den Karten üblich ist. Diesen EMV-Chip, Kürzel für Europay International, Mastercard und Visa, haben die gefälschten Karten nicht.

Name von der Redaktion geändert.

FOTO: DDP IMAGES / DAPD

Die Banden müssen die Kartendaten in Länder schicken, in denen Kartennummer und Geheimzahl zum Abheben genügen. Dafür benötigen sie nur wenige Stunden.

Häufig schicken die Kriminellen die Daten in die USA. Dort entsteht fast ein Viertel des Gesamtschadens, den deutsche Kontoinhaber im Jahr 2011 bis Oktober hatten (siehe Grafik „Weite Wege …“).

Kartendaten vom Händler gezogen

Inzwischen haben viele Institute ihre Automaten mit Störsendern ausgestattet, die das Kopieren des Magnetstreifens verhindern. Das Öffnen der Tür mit Karte haben die meisten Banken längst abgeschafft.

So sind die Schäden durch Skimming nach Aussage von Margit Schneider in den ersten drei Quartalen dieses Jahres um die Hälfte zurückgegangen. Auch die Zahl der manipulierten Geldautomaten und Bezahlgeräte bei Händlern hat sich dieses Jahr im Vergleich zum Vorjahr halbiert.

Entwarnung gibt es aber nicht. „Solange es Magnetstreifen gibt, müssen Kunden mit Skimming rechnen“, sagt Margit Schneider.

Die Ganoven weichen immer mehr auf die Bezahlgeräte der Händler aus. Die Kriminellen dringen in die Geschäfte ein und fingieren dort die Technik.

Alle Märkte, in denen Kunden gern mit Karte zahlen und hohe Tagesumsätze gemacht werden, lohnen sich für Betrüger, vor allem Baumärkte, Supermärkte, aber auch Tankautomaten mit Kartenzahlung. Auch hier gilt wie am Geldautomaten: Beim Tippen der Geheimzahl Hand davorhalten.

Geld am Klebestreifen

Ein anderer Betrugstrick ist Cash Trapping, auf Deutsch: Bargeld fangen. Klebestreifen im Geldausgabeschacht halten das Geld fest. Der Kunde wundert sich, dass nichts herauskommt und geht. Dann erscheint der Täter und fingert das Geld raus. Diese Fälle werden von Euro Kartensysteme nicht erfasst.

Kunden sollten den Automaten nicht verlassen, wenn ihr Geld ausbleibt. „Lassen Sie sich nicht von anderen helfen, sondern rufen Sie die Polizei, wenn die Bank geschlossen ist“, rät Joachim Grande, Beauftragter für Kriminalprävention der Polizei Braunschweig.

Ohne Probleme Geld erstattet

Berliner Sparkasse und Euro Kartensysteme können nachvollziehen, ob die Betrüger Vogels Daten im Laden oder am Geldautomaten abgegriffen haben. Das Ergebnis geben beide aber nicht preis.

Vogel bekommt seine 800 Euro schnell zurück. Dass er Kriminellen auf den Leim gegangen ist, hat die Sparkasse beim Anblick der Kontoabhebungen aus Costa Rica akzeptiert, weil ihr Kunde in dieser Zeit nicht dort gewesen sein konnte. Mit der Verlagerung der falschen Abbuchungen ins entfernte Ausland ist es für Kunden einfacher geworden, Betrug nachzuweisen.

Schlechte Chancen haben sie jedoch, wenn sie grob fahrlässig gehandelt haben und dann etwas mit ihrer Karte passiert. Sie dürfen nicht die Geheimzahl auf der Karte notieren oder Geheimzahl und Karte zusammen ins Portmonee stecken.

Unser Rat

Kontrolle. Prüfen Sie regelmäßig Ihre Kontoauszüge und melden Sie Ihrer Bank Buchungen, die Sie nicht veranlasst haben. Schauen Sie regelmäßig, ob Sie noch alle Zahlungskarten haben. Lassen Sie Karten sofort sperren, wenn etwas nicht stimmt.

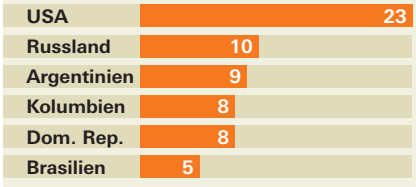
Sperre. Unter der bundesweit kostenlosen Notrufnummer 116 116 können Sie jederzeit Ihre Karten sperren lassen. Nennen Sie dort den Namen Ihrer Bank, Sie werden dann mit ihr verbunden. Die Bank lässt die Karte sperren. Aus dem Ausland erreichen Sie den Notruf mit der Vorwahl (+49). Alternativ geht auch diese Nummer: +49 30/40 50 40 50.

Anzeige. Wenn Sie Strafanzeige erstatten, sollten Sie sich den genauen Zeitpunkt und den Namen des Beamten notieren, der sie aufgenommen hat. Ein Exemplar Ihrer Anzeige sollten Sie gut aufbewahren, falls Ihre Bank einen Nachweis verlangt.

Hilfe. Die Beratungsstellen der Polizei geben Auskunft, wie Sie Kartenbetrug vorbeugen. Im Internet finden Sie Beratungsstellen in Ihrer Nähe unter www.polizei-beratung.de und weitere Informationen mit dem Suchwort „Skimming“. Unter www.kartensicherheit.de bekommen Sie Tipps für den Schadensfall.

Weite Wege für Betrüger

Wollen Diebe mit kopierten Karten Geld holen, müssen sie Automaten im Ausland nutzen, die nur Magnetstreifen prüfen. Leichtes Spiel haben Betrüger in den USA und Russland.



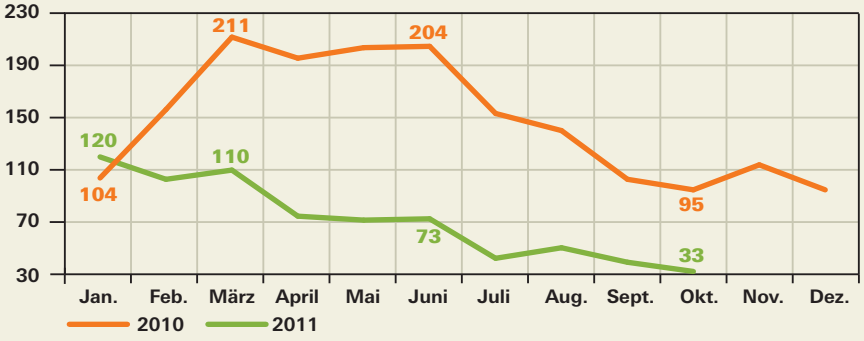
Betrug mit Karten aus Deutschland von Jan. bis Okt. 2011
(Prozent des Gesamtschadens)

Quelle: Euro-Kartensysteme GmbH

Weniger Geldautomaten manipuliert

Der neue Sicherheitschip auf den Bank- und Kreditkarten sowie Störsender in Geldautomaten lassen Manipulationen zurzeit zurückgehen.

Zahl manipulierter Geldautomaten und Händlerkassen



Quelle: Euro-Kartensysteme GmbH