Geheime Kamera filmt Pin

Bankdaten von Kunden werden am Geldautomaten von Betrügern ausgespäht

Das Thema

Einbrüche, Enkeltrick, Phishing, Scamming und Internetbetrug, die Tricks der Kriminellen werden immer raffinierter, und die Opferzahlen steigen. In Kooperation mit der Polizei klären wir auf und geben Tipps zur Prävention.

Gemeinsam gegen Betrüger: In einem Pilotprojekt arbeiten Kasseler Sparkasse, Polizei und Seniorenbeirat jetzt zusammen, um Senioren vor den Gefahren bei Geldgeschäften zu warnen. Von links: Anina Emde (Polizei-Präventionsabteilung), Alexander Heuser (Kasseler Sparkasse) und Ursula Langer (Seniorenbeirat Stadt Kassel). Foto: Ricken

Von Bea Ricken

WOLFHAGER LAND. Auf den ersten Blick sieht das Zahlenfeld aus wie immer. Deshalb schöpft Marion L. keinen Verdacht, als sie ihre EC-Karte in den Schlitz steckt, um Geld abzuholen. Was sie zu diesem Zeitpunkt nicht weiß: Betrüger haben vor dem Karteneinschubfach ein manipuliertes Kartenlesegerät installiert. So werden die Kartendaten von Marion L. ausgelesen und gespeichert, ohne dass die Geldausgabe beeinträchtigt und sie misstrauisch wird.

Was die Frau ebenfalls nicht wahrnimmt: Seitlich an einem Prospekthalter ist eine kleine Kamera installiert, die die Pin-Nummer aufnimmt, die Marion L. eingibt. Als sie den Vorraum der Bank verlässt, ist es zu spät. Sie ist Opfer des sogenannten Skimming geworden. Der englische Begriff bedeutet Abschöpfen oder Absahnen und steht für eine Methode, illegal elektronische Daten von Zahlungskarten auszuspähen.

„Mit den erlangten Daten stellen die Täter Kartendubletten her. Diese können seit 2011 in Ländern mit Euro-Währung nicht mehr eingesetzt werden. Daher werden die Straftaten zum Beispiel in den USA, Indonesien, Indien und Nepal verübt“, erklärt Anina Emde von der Präventionsabteilung der Polizei. Zwei Wochen später entdeckt Marion L. auf ihren Kontoauszügen Barabhebungen aus Südkorea.

Betrugsfälle wie dieser sind laut Emde deutschlandweit wie auch im Raum Kassel seit Jahren rückläufig. „Anti-Skimming-Module und der Zugang in die Geschäftsräume ohne Kartenleser haben es den Betrügern schwerer gemacht“, sagt sie. Besonders bei Geschäfts- und Urlaubsreisen im Ausland sei jedoch nach wie vor besondere Vorsicht geboten, rät die Fachberaterin für Internetprävention. Auch die Aufklärung der Bankkunden scheint zu fruchten. Dennoch sieht Emde keinen Grund zur Entwarnung, zumal es 2016, entgegen der Entwicklung der vergangenen Jahre, wieder eine Zunahme von Skimming-Fällen an Geldautomaten gab. Deshalb haben Polizei, Kasseler Sparkasse und Seniorenbeirat der Stadt Kassel jetzt ein Pilotprojekt gestartet: In der Sparkasse und im Rathaus gibt es in diesem Jahr zwei Auftaktveranstaltungen rund um bargeldloses Zahlen, Sicherheit am Bankautomaten und Onlinebanking. Dabei erhalten Senioren auch praktische Einweisungen am Geldautomaten.

HINTERGRUND

Sicheres Bezahlen und Enkeltrick

Vorträge und praktische Übungen rund um die Themen Skimming, Phishing, richtige Nutzung des Onlinebanking und Schutz vor dem Enkeltrick finden am Samstag, 21. April, von 10 bis 12 Uhr, in den Räumen der Kasseler Sparkasse, Wolfsschlucht 9 und am Dienstag, 28. August, ab 14 Uhr, im Rathaus Kassel statt. (ewa)

Tastenfeld kann Attrappe sein

Polizei gibt Tipps, wie Kunden Manipulationen am Geldautomaten erkennen können

Wie schützt man sich vor Skimming? Die Präventionsabteilung des Kasseler Polizeipräsidiums gibt Tipps:

- Gehen Sie sorgsam mit Ihren Zahlungskarten um und bewahren Sie die Pin stets getrennt von der Karte auf.
- Haben Sie mehrere Zahlungskarten? Betätigen Sie den Türöffner eines Bankinstitutes nicht mit der gleichen Karte, mit der Sie anschließend Geld abheben möchten. (Hinweis: Viele Institute in der Region haben den Türöffner aufgrund der Betrugsfälle abgeschafft. Die Tür öffnet automatisch.)
- Geben Sie Ihre Pin niemals an einem Türöffner eines Bankinstitutes ein. Kein Geldinstitut verlangt für den Zugang zum Geldautomaten die Eingabe der Pin. Der Kartenleser hat immer nur die Funktion des Türöffners. Verständigen Sie in solchen Fällen die Polizei und das Geldinstitut.
- Achten Sie darauf, dass die Eingabe Ihrer Pin nicht von anderen beobachtet werden kann. Sorgen Sie für einen ausreichenden Sicherheitsabstand zum nächsten Kunden.
- Decken Sie während der Pin-Eingabe das Tastaturfeld mit der anderen Hand oder einem Gegenstand (zum Beispiel Geldbörse, Blatt Papier) als Sichtschutz vollständig ab. Das erschwert das Ausspähen per Kamera oder Foto-Handy erheblich.
- Nutzen Sie keinen Geldausgabeautomaten, an dem Ihnen etwas ungewöhnlich erscheint, zum Beispiel angebrachte Leisten oder Verblendungen, abstehende und lockere Teile, Spuren von Kleber rund um den Kartenschlitz.
- Bei Verdacht auf Manipulation sollten Sie den Automaten nicht nutzen. Verständigen Sie die Polizei, um mögliche Spuren sichern zu können.
- Kontrollieren Sie regelmäßig Ihre Kontoauszüge und wenden Sie sich bei Auffälligkeiten sofort an Ihre Bank.
- Bei dem Verdacht der Ausspähung Ihrer Kartendaten lassen Sie bitte umgehend die Karte über Ihre Bank beziehungsweise den bundesweiten Sperrnotruf unter 116 116 sperren und erstatten Sie Anzeige bei der Polizei.

Quelle: Polizei

www.polizei-beratung.de
www.polizei.hessen.de/Praevention

Tastenfeld-Attrappe: Das zweite Tastenfeld sieht täuschend echt aus. Durch diese Manipulation kann die Pin von Bankkunden ausgespäht werden. Foto: Frederik von Erichsen/dpa