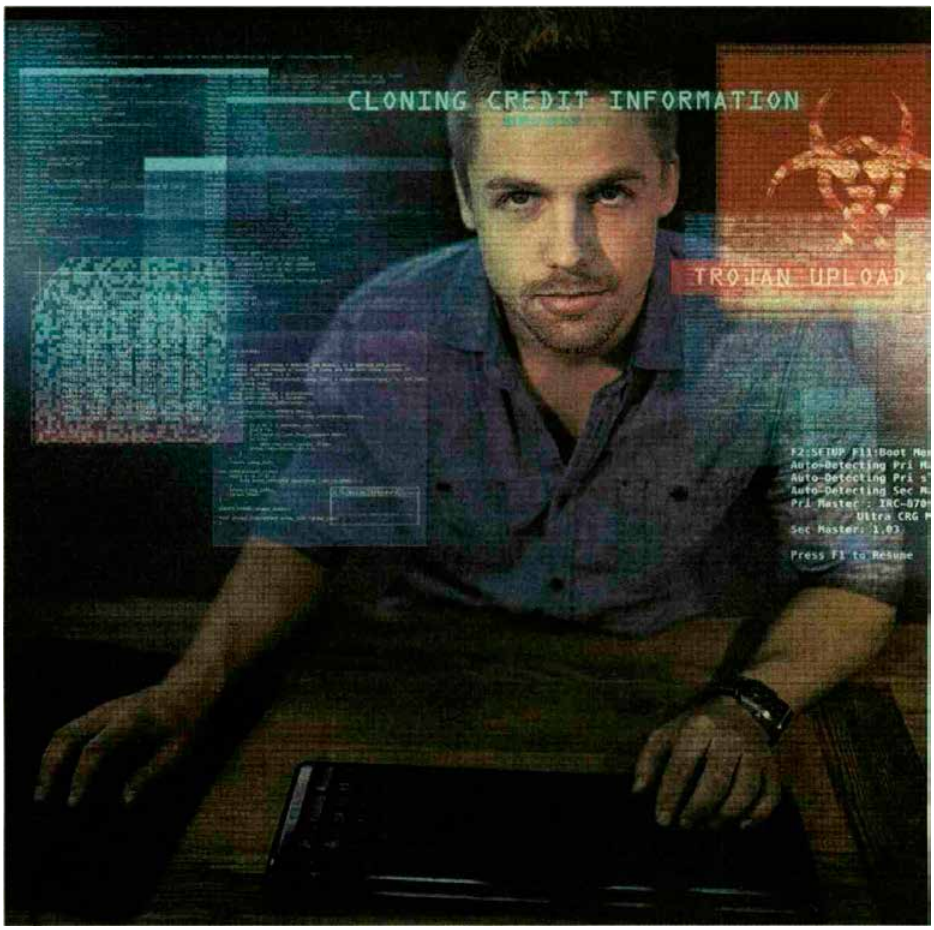
Datum: 27.09.2014

Basler Zeitung

Vorsicht vor modernen Bankräubern

Die Sicherheit beim Online-Banking kann zu einem guten Teil der Kunde selbst gewährleisten



Dreist und raffiniert. Betrüger finden immer neue Methoden, um an Passwörter und Identifikations- und Transaktionsnummern zu gelangen. Foto iStock

Von Valentin Ade

Basel. Die Zeiten, in denen Bankräuber ausschliesslich mit Strumpfmaske und Pistole den Bankangestellten hinterm Schalter zum öffnen des Tresors zwangen, sind längst vorbei. Die grossen Schäden entstanden in den vergangenen Jahren auf raffiniertere Arten. Und diese treffen nicht nur die jeweilige Bank, sondern auch die Kunden. Die Finanzinstitute investieren viel in die Sicherheit beim Banking, doch auch die Bankkunden müssen einiges beachten, um nicht Opfer eines modernen Bankräubers zu werden.

Als Bankkunde kann man durch einfache Vorsichtsmassnahmen stark zur Sicherheit beim Banking beitragen. Denn «der sorgfältige Umgang mit den Identifikationsmitteln im Electronic Banking ist der Schlüssel für die Sicherheit», sagt Michael Baumberger, Leiter Banking Service bei der Basler Kantonalbank (BKB) und damit für die elektronischen Vertriebskanäle im Finanzinstitut zuständig. Eine elementare Regel im Umgang mit den Bankunterlagen: Kontokarte und PIN (Persönliche Identifikationsnummer) niemals zusammen aufbewahren. Einleuchtend, möchte man meinen. Dennoch würden viele Kunden, so Baumberger, die PIN auf ihren Kontokarten notieren. «Dadurch können leider missbräuchliche Bezüge getätigt werden.»

«Karten müssen sorgfältig aufbewahrt und bei Bemerken des Verlusts umgehend gesperrt werden», sagt auch Nadine Geissbühler, Sprecherin der Aduno-Gruppe, die grösste Herausgeberin von Kredit- und Debit-Karten in der Schweiz. Passwörter und PIN dürfen nicht an Dritte weitergegeben oder leicht zugänglich gemacht werden. Ebenso wichtig ist es, unbekannte Buchungen sofort zu melden, um weiteren Missbrauch zu verhindern. Dies muss innert

Datum: 27.09.2014

Basler Zeitung

30 Tagen ab Datum der Monatsrechnung erfolgen. Denn «wer seine Sorgfaltspflichten gemäss den Allgemeinen Geschäftsbedingungen vollumfänglich einhält, bleibt im Betrugsfall schadlos», so Geissbühler. Die Aduno-Gruppe wie auch die Banken übernehmen in diesem Fall nämlich die entstandenen Schäden.

Bank kennt Passwörter nicht

Kunden sollten sich zudem vor sogenannten Fishing-Methoden in Acht nehmen. Dabei versenden Betrüger vermeintliche E-Mails der Banken an ausgesuchte Opfer. Mittlerweile sind die Betrüger derart dreist geworden, dass sie sich am Telefon als Mitarbeiter der jeweiligen Bank ausgeben. Sie fordern die Kunden auf, Passwörter und TAN (Transaktionsnummer) herauszugeben. «Die Bank kennt die Passwörter der Kunden nicht und wird auch nie danach fragen, weder telefonisch noch per E-Mail», sagt Michael Baumberger.

Aber auch wenn die PIN nur im Kopf des Kunden Verwahrung findet, sollte sie aus Sicherheitsgründen stets verdeckt am Bancomaten eingegeben werden, um sich vor dem sogenannten Skimming zu schützen. Dabei kopieren Diebe zum einen den Magnetstreifen der Karte durch ein Gerät, das auf respektive statt des sogenannten Mundstücks – dem Kartenschlitz des Bancomaten – angebracht ist. Zum andern wird über eine kleine Kamera oder ein zweites Tastenfeld, das über dem eigentlichen angebracht ist, die PIN ausspioniert.

Viel weniger Skimming-Fälle

Vor zwei Jahren wurden auch Bancomaten der BKB von einer Skimming-Bande manipuliert. Seitdem hat sich laut Michael Baumberger punkto Sicherheit einiges getan. Neue Automaten hätten nun speziell gesicherte Mundstücke. Auch werden die Automaten regelmässig auf Manipulationen überprüft.

Eine neue Technik macht Kredit- und Debit-Karten zudem so gut wie kopiersicher. Denn längst geschehen Kartentransaktionen nicht mehr via Magnetstreifen, sondern über den EMV-Chip, der sich auf jeder Karte befindet. Dieser ist durch eine spezielle Verschlüsselung gegen eine Duplizierung geschützt. «Dadurch haben sich die Schäden aufgrund von Skimming deutlich reduziert», sagt Nadine Geissbühler. Zahlen von SIX Payment Services, Betreiber des grössten Schweizer Netzwerks zur Übermittlung elektronischer Rechnungen, bestätigen dies. Wurden auf dem Höhepunkt der Skimming-Welle rund 15 Millionen Franken betrügerisch bezogen, waren es 2013 noch rund fünf Millionen Franken. In den ersten sechs Monaten des laufenden Jahres wurden rund eine halbe Millionen Franken durch Skimming erbeutet. «Wir hatten bis und mit Juni 2014 nur noch acht Betrugsfälle an Bancomaten – ein Rekordtief», sagt Jürg Schneider von SIX.

Die EMV-Technik findet heute an den meisten Automaten in Europa ihre Anwendung. «Heute ist der Einsatz einer geklonten Karten nur noch in denjenigen Ländern ein Problem, in welchen Chip-fähige Terminals noch wenig verbreitet sind», so Geissenbühler. Wichtig in diesem Zusammenhang: Reist man über Europas Grenzen hinaus, sollte man bei der Bank die eigene Karte für die Benutzung an nicht EMV-fähigen Geräten freischalten lassen.

Benachrichtigung per SMS

Dennoch gilt es, auf der Hut zu sein vor neuen Manipulationsversuchen an Bancomaten. Diese sollten vor Nutzung auf auffällige oder bewegliche Teile (zweite Tastenfelder, Minikameras) kontrolliert werden. Wenn möglich, sollte man stets am gleichen Gerät Geld abheben, um Auffälligkeiten oder Veränderungen sofort zu erkennen. Generell gelten zudem Bancomaten in den Räumlichkeiten der jeweiligen Bank als sicherer als Geräte ausserhalb. Und natürlich sollten am Ende des Monats die Kartenbezüge und Kreditkartenabrechnungen immer auf Unregelmässigkeiten überprüft werden.

Eine weitere Möglichkeit der Sicherung beim Bezug von Bargeld oder beim Zahlen per Karte ist die Benachrichtigung per SMS danach. Sollte man den Diebstahl der eigenen Karte nicht sofort bemerken, weiss man es spätestens, wenn man durch eine SMS über eine Transaktion in Kenntnis gesetzt wird, die man selbst nicht getätigt hat.

Mehrere Sicherheitsebenen

Auch beim E-Banking, dem Zahlungsverkehr via Internet, ist diese Option möglich. Hierbei ist wieder der Kunde gefragt mit einfachen Vorkehrungen, die Sicherheit zu gewährleisten. «Installieren Sie regelmässig die Sicherheitsupdates Ihres Betriebssystems, des Webbrowsers und Ihres Virenschutzes», so Michael Baumberger. Zudem sollte man regelmässig seine Passwörter, auch das des E-Banking-Accounts wechseln.

Um das E-Banking vor Hackerangriffen zu schützen, wurden von den Banken mehrere Sicherheitsebenen eingezogen. Zum einen geschieht die Verbindung vom Kunden-PC zum Bank-Server über ein Verschlüsselungsprotokoll, das TLS (Transport Layer Security). Informationen, die über eine derart verschlüsselte Verbindung übermittelt werden, sind für Dritte fast unmöglich einsehbar. Die Echtheit der Verbindung kann via Einsicht in die Zertifikate-Funktion überprüft werden. Einfach im Webbrowser auf die grüne Schaltfläche neben der Adresszeile klicken.

Damit ist der Sicherheit aber noch nicht Genüge getan. Will man sich beispielsweise bei der BKB in sein E-Banking-Account einloggen, muss man nicht nur ein Passwort, sondern auch die Identifikationsnummer angeben, die man bei Vertragsabschluss erhalten hat. Aber auch danach kann man nicht ungehindert Geld hin und her schieben. Jede Transaktion bedarf der Eingabe einer TAN. Früher bekam man dazu eine Liste von Transaktionsnummern mit der Post zugeschickt. Heute wird allgemein empfohlen, sich die TAN in jedem konkreten Fall via Mobiltelefon zusenden zu lassen. «Die Legitimation über zwei Kanäle – Computer und Mobiltelefon – erhöht nochmals die

Datum: 27.09.2014

Basler Zeitung

Sicherheit», sagt Michael Baumberger.

Ohne Bedenken kontaktlos zahlen

Seit Kurzem ist es möglich, mit Kredit- und Debit-Karte kontaktlos zu zahlen. Bietet die neue Technologie der Near Field Communication (NFC) auch eine neue Möglichkeit für Betrüger? Banken und Kreditkartenfirmen winken ab: «Die Bedenken der Kunden sind unbegründet», sagt Nadine Geissbühler. Beim kontaktlosen Zahlen wird für alle Beträge über 40 Franken (respektive 25 Euro) weiterhin ein PIN-Code benötigt. «Das Kartenprodukt ist somit vollständig vergleichbar mit einer nicht kontaktlos einsetzbaren Karte», so Geissbühler.

Die Erfahrungen der Aduno-Gruppe mit dem kontaktlosen Bezahlen in der Schweiz (seit 2007) würden zeigen, dass keine erhöhte Zahl an Betrugsfällen festzustellen seien. Zudem würden für den Karteninhaber keine finanziellen Risiken bestehen. Banken und Kreditkartenfirmen haften auch bei der neuen Technologie für Schäden, die aus einer missbräuchlichen Verwendung von Karten entstehen, sofern die Sorgfaltspflichten eingehalten wurden.