Bankraub online

Stiftung Warentest Juni 2010

Onlinebanking: Jeder dritte Kunde führt sein Konto per Internet oft mit einem unguten Gefühl. Zu Recht, denn viele halten selbst einfache Schutzmaßnahmen nicht ein. Die Zahl der Betrugsfälle steigt.

Für einen Moment nur war der Monitor schwarz, als sei kurz die Leitung unterbrochen. Danach war die Seite sofort wieder da, ebenso alle Daten, die Claudia M.* gerade in ihre Überweisung eingetippt hatte. Nur die Tan-Nummer war weg. „Die habe ich wohl schon verbraucht und vergessen durchzustreichen", dachte sie. Doch dann fehlten 4128 Euro auf dem Konto.

Die Badenerin war Opfer von Computerkriminellen geworden, wie andere Bankkunden auch: 2900 Betrugsversuche, die zu Anzeigen führten, zählte der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) 2009, die Hälfte mehr als im Vorjahr. Das ist zwar wenig angesichts von 40 Millionen Onlinekonten, doch diese Sicht hilft dem einzelnen Opfer nicht: Der durchschnittliche Schaden liegt bei 4 8oo Euro, und die zahlt niemand aus der Portokasse.

Wie sicher also ist Onlinebanking? Und wer zahlt, wenn etwas schief geht? Immerhin haben fünf Prozent der Internetnutzer schon erlebt, dass bei ihnen Zugangsdaten für Shops, soziale Netzwerke oder Onlinebanking ausspioniert wurden, so der Bundesverband Bitkom - Datendiebe lauern überall. Typische Gefahren sind das sogenannte Phishing und Pharming.

Beim Phishing erhält der Nutzer eine E-Mail mit der Bitte, sich bei der Bank einzuloggen und die persönliche Geheimzahl (Pin) und eine Transaktionsnummer (Tan) einzugeben. Als Grund wird meist genannt, es müssten Daten aktualisiert werden. Beigefügt ist ein Link. Doch der führt nicht zur Bank, sondern zu einer gefälschten Seite, die der Banken-Homepage täuschend ähnlich sieht. Gibt das Opfer dort Pin und Tan ein, haben die Betrüger alles, was sie brauchen, um das Konto zu plündern.

Mitunter machen sie sich nicht einmal die Mühe, die beim Onlinebanking übliche SSL-Verschlüsselung nachzuahmen. In der Adresszeile des Browsers - also meist der Internet Explorer oder Mozilla Firefox steht dann nur "http", nicht "https" für erhöhte Sicherheit. Außerdem zeigt der Browser nicht das kleine Vorhängeschloss. Die Gauner setzen einfach darauf, dass routinierte Onlinekunden nicht mehr jedes Mal diese Sicherheitszeichen checken.

Von allen Tricks ist Phishing am einfachsten zu durchschauen. Denn keine Bank mailt ihre Kunden an und verlangt die Eingabe von Pin und Tan. Mitunter stehen in den Phishing-E-Mails sogar Rechtschreib- und Grammatikfehler. Außerdem sollten Kunden nie über einen Link zur Bankseite gehen, sondern über "Favoriten" oder indem sie die Adresse eintippen.

Kaum zu bemerken ist hingegen Pharming. Dabei wird ein sogenannter Trojaner auf den PC geschmuggelt: ein Schadprogramm, das heimlich die Eingabe von Geheimzahlen mitliest und sie an ihre Auftraggeber weiterleitet. Die brauchen nur noch die Kontonummer des Empfängers durch ihre eigene zu ersetzen. Den Schaden sieht das Opfer erst auf dem Kontoauszug. Oft sind Trojaner in Downloads von Gratisprogrammen versteckt oder im PDF-Anhang einer E-Mail, zum Beispiel als ebay-Rechnung "rechnung.pdf.exe" Wird der Anhang geöffnet, nistet sich der Schädling auf dem PC ein. Der Besitzer merkt davon nichts, selbst wenn sich Dutzende solcher Trojaner auf seinem Rechner verstecken.

Unfassbar ist für viele Opfer, dass es nicht einmal hilft, die Adresse der Bank von Hand einzutippen, sie landen dennoch auf einer gefälschten Seite. Das liegt daran, dass der Trojaner die Host-Datei des Betriebssystems manipuliert. Dort sind jede Menge Internetadressen abgelegt. Das könnte etwa www.dorfbank.de sein. Wählt der Kunde diese Adresse, steuert der manipulierte PC nicht die Bank an, sondern die Seite des Fälschers angezeigt wird aber die vom Kunden eingetippte Adresse.

Ganz ähnlich lief es bei Claudia M. Auf ihrem Rechner hatten sich 14 Schadprogramme installiert. Dennoch wollte die Bank das Geld nicht erstatten: Die Kundin habe gegen ihre Sorgfaltspflichten verstoßen.

Antiviren-Software ist Pflicht

Fragt sich nur: Welche Pflichten haben Onlinekunden konkret? Dazu gibt es bisher kaum Gerichtsentscheidungen, schon gar keine höchstrichterliche Rechtsprechung. Denn meist erstatten Banken und Sparkassen lieber das Geld, als schlagzeilenträchtige Prozesse zu riskieren. Als eines der wenigen befasste sich das Landgericht Köln mit Onlinebanking. Ergebnis: Wenn der Normalnutzer eine Antiviren-Software einsetzt sowie eine Firewall, muss er nicht haften (Az. 9 S 195/07). Genauso sah es das Landgericht Nürnberg-Fürth (Az. 10 0 11391/07). Und auch das Amtsgericht Wiesloch gab Claudia M. Recht. Sie hatte den "Norton Antivirus“ installiert. Das sei genug, urteilte das Gericht (Az. 4 C 57/o8). Die Bank muss ihr den Betrag zurückbuchen.

Das ist auch herrschende Meinung unter Rechtsexperten: Antivirenschutz und Firewall sollte jeder Kunde haben. Das gilt auch, wenn er Kontoprogramme benutzt wie Star Money, Quicken oder Wiso-mein-Geld, denn die bringen zwar mehr Sicherheit, vor allem gegen Phishing, sind aber nicht wirklich vor Trojanern gefeit. Dennoch

vernachlässigen viele Kunden diese Minimalanforderung: Laut Bitkom surft jeder fünfte Internetnutzer ohne Virenschutz.

Geld müssen Kunden dafür nicht ausgeben. Der Kauf teurer Software sei Normalnutzern nicht zumutbar, meinten die Kölner Richter. Ein Gratis-Virenscanner reicht. In unserem Test *(siehe test* 4log) haben Antivir Personal Free Antivirus und Alwil Avast 4.8 mit "gut" abgeschnitten. Deren Installation ist einfach.

Software regelmäßig aktualisieren

Damit allein ist es aber noch nicht getan. Die Software muss auch regelmäßig aktualisiert werden. Mindestens einmal wöchentlich, so meinen Juristen, sollten Kunden ein Update laden Vielsurfer mit DSL-Anschluss sogar täglich. Viele Programme haben eine automatische Updatefunktion. Die sollte eingeschaltet bleiben.

Dasselbe gilt für das Betriebssystern. und den Browser: Wenn der Computer meldet, dass ein Update bereitsteht, sollten Onlinebanker es herunterladen- auch wenn das nervig ist, auch wenn sie die neue Version gar nicht wollen oder mit der alten viel besser klarkommen. Denn Updates schließen neu entdeckte Sicherheitslücken.

Firewall gegen Trojaner

Ganz wichtig ist eine Firewall. Ihre Bedeutung wird vielfach unterschätzt: Nach Bitkom-Angaben surft jeder dritte Internetnutzer ohne Firewall. Dabei kann auch sie als Mindestvoraussetzung gelten. Der Virenscanner allein bietet nämlich keinen Komplettschutz. Nur eine Firewall schirmt den Rechner gegen Trojaner ab. Sie verhindert nicht nur das Einschmuggeln, sondern kontrolliert auch ausgehende Aktionen, zum Beispiel während der Nutzer Kontonummer und Pin eintippt.

Windows 7 und Vista verfügen bereits über eine Firewall.

Das Kölner Landgericht ist außerdem der Ansicht, dass Kunden darauf achten müssen, ob in der Adresse "http" steht oder das sichere "https" Und sie müssen die Warnungen der Banken beachten, Pin und Tan nie am Telefon oder auf Anforderung per E-Mail herauszugeben. Wer so einen Betrug nicht bemerkt, handelt fahrlässig und muss einen Teil des Schadens selbst tragen (Landgericht Berlin, Az. 37 0 4/og):Das sei vergleichbar mit dem Missbrauch der ec-Karte. In dem Fall musste die Kundin 10 Prozent aus eigener Tasche beisteuern.

Kunden, die über WLan ins Internet gehen, sollten es unbedingt verschlüsseln. Standard ist der WPA2-Kode, noch sicherer ist WPS. Ganz ohne Verschlüsselung WLan zu nutzen, gilt als grob fahrlässig (Oberlandesgericht Düsseldorf, Az. 1-20 W 157/07).

Wer diese Schutzvorkehrungen einhält, kann verlangen, dass die Bank den Schaden übernimmt. Falls sie ablehnt und darauf verweist, auf ihrer Homepage würden weitere Maßnahmen gefordert, sollten Kunden sich nicht verunsichern lassen: Unter Juristen gilt es als unwahrscheinlich, dass Normalkunden zu noch mehr Aufwand verpflichtet werden können - zum Beispiel zu Änderungen am Betriebssystem oder zum Einrichten von Administratorrechten. Kein Gericht hat das bisher verlangt. "Schließlich können Banken nicht erwarten, dass jeder Durchschnittsnutzer zum EDV-Experten wird" meint Bankrechtsexperte Markus Feck von der Verbraucherzentrale Nordrhein-Westfalen.

Freiwillige Schutzmaßnahmen

Dennoch können Kunden schon aus eigenem Interesse ihre Sicherheit erhöhen. Etwa indem sie die Sicherheitseinstellungen des Browsers aktivieren. Beim Internet Explorer geht das unter "Extras", dann "Internetoptionen", dann "Sicherheit", bei Firefox unter "Extras", "Einstellungen", "Inhalt".

Außerdem schmuggeln sich Trojaner oft über ein Active-X-Element oder Javascript auf den PC. Wer sichergehen will, schaltet unter "Extras" diese Elemente ab oder stellt ein, dass Java-Applets nur nach Rückfrage ausgeführt werden. Vorsichtige schalten auch das "Auto-Vervollständigen" ab. Diese Funktion schlägt den vollen Namen und das Passwort vor, sobald jemand die ersten Buchstaben eingibt. Und falls der Browser vor einer Seite warnt, sollten Nutzer dem lieber Glauben schenken. Es kann sein, dass sonst ein Trojaner eingeschleust wird.

Fazit: Wenn der Kunde mit Virenschutz und Firewall surft, Pin und Tan sorgfältig behandelt, hat er seine Pflicht getan. Falls dann doch etwas passiert, ist die Bank dran.

Nur schade, dass die Hoffnung, Betrüger könnten ohnehin nur Geld auf ihr Konto umleiten und dann als Kontoinhaber identifiziert werden, nicht greift: Die 4128 Euro von Claudia M. waren an eine ebay-Verkäuferin geflossen. Die wiederum hatte als "Finanzagentin" einer russischen Firma den Betrag sofort nach Sankt Petersburg transferiert. Solche Agenten müssen zwar wegen Beihilfe zur Geldwäsche haften. Doch obwohl der Betrug schon nach einem Tag aufflog, war das Geld weg.

Das System aus Pin und Tan - persönlicher Geheimzahl und Transaktionskode - ist mittlerweile technisch überholt . Dagegen schließen moderne Tan-Generatoren Trojanerangriffe weitgehend aus. Als sehr sicher gilt auch die mobile Tan, die per SMS aufs Display des Handys geschickt wird..

Bankraub online

Bankraub online

Sicherungsverfahren

Pin und Tan technisch überholt
Die Banken entwickeln ständig neue Sicherungsverfahren, um Transaktionen sicher durchs Internet zu bringen. Teils unterscheiden sie sich von Bank zu Bank. Besonders gängig sind:

Pin/Tan: Das System aus Geheimzahl (Pin) und Transaktionskode (Tan) ist überholt. Dasselbe gilt für den Nachfolger Pin/iTan, wo der Kunde nicht aus einer langen Tan-Liste eine Zahl wählt, sondern die Bank eine bestimmte Tan, die "indizierte", aus der Liste verlangt,

iTan plus: Sie wird von Volks- und Raiffeisenbanken verwendet. Dabei zeigt der Monitor ein Kontrollbild, das mit einem maschinell kaum lesbaren Raster unterlegt ist, was Trojanerattacken erschweren soll. Zusätzlich zeigt es das Geburtsdatum des Kunden an.

Tan-Generatoren: Das sind Taschenrechner große Geräte, die der Kunde statt einer Tan-Liste erhält. Ältere zeigen auf Knopfdruck eine Tan an. Da sie nicht mehr den Sicherheitsanforderungen der Banken genügen, gelten sie ebenfalls als überholt. Bei modernen eTan-Plus-Geräten schiebt der Kunde seine Bankchipkarte, zum Beispiel die Girokarte, in den Generator und erhält eine Tan. in deren Berechnung fließen Betrag und Zielkonto ein, sodass Kriminelle das Geld nicht auf ein anderes Konto umleiten können. "Selbst wenn der Generator verloren wird, ist Missbrauch unmöglich, denn alle Authentifizierungsschlüssel liegen auf der Chipkarte", so Dr. Waldemar Grudzien vom Bundesverband deutscher Banken. Geräte mit optischer Schnittstelle hält der Kunde vor den Monitor. Über Fotodioden erkennen sie die Darstellung und zeigen eine Tan, die die Transaktionsdaten einbezieht.

mTan: Die "mobile Tan" wird von der Bank per SMS aufs Handy des Kunden geschickt. Das gilt als sehr sicher, da zwei Übertragungswege beteiligt sind: Internet und Mobilfunk. Beide zu knacken, ist extrem schwierig. Außerdem fließen in die Tan Daten aus der Transaktion ein. Zusätzlich nennt die SMS auch Kontonummer und Betrag. Wird die mTan nicht verwendet, verfällt sie nach kurzer Zeit. Vorsicht: Wer die Überweisung nicht am PC eingibt, sondern am Handy, nutzt nur einen Übertragungsweg. Die Banken weisen deshalb darauf hin, dass Aufträge nicht am Handy eingegeben werden sollen

HBCI/FinTS: HBCI und die Weiterentwicklung FinTS gelten als sehr sicher. Der Kunde braucht dafür einen Kartenleser. Moderne Geräte der Klasse 2 oder 3 haben einen Prozessor und eine eigene Tastatur. Der Nutzer braucht also seine Pin nicht am PC einzugeben. Eine Chipkarte verschlüsselt die Daten. Phishing, Pharming und Trojaner werden abgewehrt. Trotz der hohen Sicherheit hat sich HBCI/FinTS nicht durchgesetzt, denn die Software muss auf dem PC installiert werden, was nicht auf allen Rechnern problemlos gelingt

HBCI+: Einen Rückschritt bei der Sicherheit bedeutet hingegen HBCI auch HBCI 2.2 oder HBCI Pin/Tan genannt. Hier wird nicht per Chipkarte verschlüsselt, sondern per SSL-Verbindung. Der Kunde braucht weiter TanListen. Ab der Version 3.0 können aber auch Tan-Generatoren oder die mTan mit HBCI/FinTS kombiniert werden.

USB-Stick: Hier wird ein USB-Stick mit integrierter Chipkarte und eigenem Browser an den Computer angeschlossen. Die Girokarte oder ec-Karte ist nicht nötig, denn ein Chip im Stick trägt alle nötigen Daten. Es gibt auch Sticks mit Tastatur und Anzeige. Das lässt Trojanerangriffe ins Leere laufen .

Passwort: Ein Motto hilft
Ein gutes Passwort besteht aus mindestens acht Stellen und enthält Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Begriffe und vor allem Namen sollten besser nicht darin vorkommen, auch nicht Tastaturfolgen wie "qwertz" oder Wiederholungen einzelner Zeichen.

***Tipp:** Um sich ein Passwort besser merken zu können, hilft es, wenn die Anfangsbuchstaben eines Mottos oder eines Gedichts den Ausgangspunkt bilden. Beispiel: "Alle acht Tage hole ich Bargeld und Kontoauszüge" könnte als Passwort "a8ThiB&K" lauten.*

Passwörter, Pin und Tan sollten nicht auf dem Computer gespeichert werden. Auch sollte nie dasselbe Passwort für verschiedene Internetseiten, Handy oder PC gelten. Und wer befürchtet, ein Fremder könnte das Passwort kennen, sollte es umgehend ändern.

Bankraub online

Tipps
Geheimzahl: *Beim Einloggen fragen Banken nur nach Kontonummer und Pin, nie nach einer Tan. E-Mails mit der Bitte, Pin und Tan einzugeben, , kommen nur von Betrügern*

Zuletzt: *Viele Banken nennen beim Einloggen den Zeitpunkt, an dem der Kunde zuletzt auf der Seite war. Prüfen Sie, ob der Termin korrekt ist.*

Tastatur: *Einige Institute bieten für die Pin-/Tan-Eingabe eine Tastatur am Bildschirm, die per Maus bedient wird. Das lässt "Keylogger" ins Leere laufen: Spionageprogramme, die alle Tastatureingaben mitlesen.*

Cafè: *Bankgeschäfte nie an fremden Rechnern erledigen, wie im InternetCafè. Auf dem Computer können Spuren bleiben, die der nächste Nutzer lesen könnte - auch wenn Sie den Cache des Browsers löschen.*

WLan*: Verschlüsseln Sie unbedingt das heimische WLan. WLan-Netze im Hotel oder im Cafè sind bevorzugte Orte für Hacker, da sie dort gleich mehrere Opfer finden.*

Download: *In Downloads von Gratis-Software werden gern Trojaner versteckt. Neue Programme daher nur von sicheren Seiten laden, etwa von bekannten PC-Zeitschriften.*

E-Mail: *E-Mail-Anhänge sind ein klassisches Einfallstor für Trojaner. Löschen Sie Mails zweifelhafter Herkunft. Öffnen Sie die Anhänge auf keinen Fall.*

Turbo: *Auch einige Surf-Turbos, die den PC schneller machen sollen, sind eine Einladung an Betrüger zum Mitlesen, warnt das Bundesamt für Sicherheit und Informationstechnik.*

Limit: *Zur Begrenzung möglicher Schäden hilft ein Überweisungslimit. Wer nicht ständig Geld ins Ausland verschickt, sollte das Konto für Auslandsüberweisungen ganz sperren.*

Kontrolle: *Mindestens wöchentlich den Kontostand kontrollieren.*

Geld zurückholen
Tippfehler und Zahlendreher gehen zulasten des Kunden. Seit vergangenem Jahr sind Banken nicht mehr verpflichtet, Empfängername und Kontonummer abzugleichen - auch nicht bei Überweisungen auf Papier.

Achtung: Zahlendreher passieren oft schon, wenn zum Beispiel ein Bekannter seine Kontonummer telefonisch durchgibt und sich dabei eine Verwechslung einschleicht.

Wer den Fehler rasch bemerkt, kann oft noch alles rückgängig machen. Viele Banken bieten auf der Internetseite einen Button dafür. Denn eine Überweisung, die der Kunde beispielsweise abends in den PC tippt, wird nicht sofort erledigt, sondern landet zunächst im elektronischen Briefkasten der Bank. Ausgeführt wird sie am nächsten Vormittag.

Doch sobald das Geld auf dem falschen Konto liegt, ist nichts mehr zu machen. Dann kann die Bank aber die Fremdbank kontaktieren, damit sie ihren Kunden bittet, das Geld zurückzuzahlen. Dazu ist der Empfänger verpflichtet. Weigert er sich dennoch, bleibt aber nichts anderes, als die Rückzahlung einzuklagen.

Tipp: Wer häufiger an denselben Empfänger überweist, kann sich Auftragsvorlagen anlegen. Das hilft, Zahlendreher zu vermeiden. Kontrollieren Sie trotzdem die festgelegte Kontonummer. Denn ein Hacker könnte sie verändert haben.