Elektronische Bankgeschäfte:

So schützen Sie Ihr Konto

Foto: tommyS@pixelio

Sie führen Ihr Bankkonto über das Internet oder nutzen Geldautomaten? Neue Betrugsmethoden machen alle elektronischen Bankgeschäfte riskant. Was Sie wissen sollten, lesen Sie hier.

Über 30 Millionen Deutsche führen ihr Konto online – und fast alle Bankkunden haben eine Kundenkarte („EC-Karte"), um Geld am Automaten abzuheben. Dank der elektronischen Fortschritte im Bankgeschäft übernimmt der Kunde zwar immer mehr Aufgaben selbst – aber dabei auch manche Risiken. Heute sind viele Vorgänge durch Geldautomaten, Datenträgeraustausch, Online-Banking usw. Weg und Kosten sparend vom Bankkunden selbst durchführbar. Dabei ist es wichtig zu wissen, welche Verfahren es im elektronischen Bankgeschäft gibt, und welche Risiken diese bergen. Übersicht 1 zeigt, dass es nicht nur das „Online-Banking" in seinen verschiedenen Ausführungen gibt, sondern auch andere elektronische Wege, die modernen Bankräubern die Arbeit mehr oder weniger leicht machen.

Datenträgeraustausch (DTAUS)

Der in die Jahre gekommene Datenträgeraustausch ist immer noch ein gern genutztes Verfahren für Kunden mit vielen Aktivitäten auf ihrem Bankkonto. In den DTAUS-Dateien sind alle gewünschten Transaktionen für die Bank einlesbar enthalten. Papierene Nach- und Beweise sind dauerhafter als elektronische. Durch die notwendigen Begleitscheine mit Unterschrift setzt es aber für Fälscher die gleichen Hürden, wie Überweisungsformulare.

Bank-Karten

Das als „SB-Banking" bezeichnete Selbstbedienen am Geldautomaten ist in letzter Zeit durch spektakuläre Manipulationen riskant geworden: Mit Minikameras und durch aufgeklebte Tastaturen manipulierte Automaten fangen die PINs der Besitzer ab oder ziehen die Karte gar ein. Diese Art der elektronischen Geldabhebung ist vor solchen Angriffen („Skimming" genannt) nicht mehr sicher. Sinnvoll ist, dass Sie den Verfügungsrahmen Ihrer Barabhebungen bei Ihrer Bank begrenzen lassen. Und generell sollten Sie die PIN der Bankkarte niemals auf dieser notieren oder in der gleichen Brieftasche aufbewahren. Weitere Informationen wie Sie sich dagegen schützen können, siehe www.kartensicherheit.de.
Eine **Geldkarte mit aufladbarem Chip** ist nichts anderes als Bargeld in Ihrer Geldbörse: Jeder kann ohne Identifikationsnachweis diese nutzen und mit dem Geld bezahlen, sobald er in den Besitz der Plastikkarte kommt, z.B. durch Diebstahl. Grundsätzlich sollten Sie diese nie mit hohen Beträgen aufladen.
Eine **Kreditkarte** ist für den Bankkunden nicht nur bequem, bei ihr ist das Risiko aber überschaubar: Bis zur Sperrung haftet der Kreditkarteninhaber meist nur bis zu 50 Euro. Nur wenn der Besitzer die Karte- (bzw. -nummer) grob fahrlässig preisgibt, haftet dieser für den entstandenen Verlust. Dies gilt auch, wenn Sie die Karte in einem Fahrzeug unbeaufsichtigt liegen lassen. Im Normalfall haftet jedoch das Kreditkarteninstitut. Besonders für die Bezahlung im Internet ist die Kreditkarte eine der sichersten und für den Besitzer die risikoärmste Bezahlmöglichkeit. Die Beweispflicht liegt bei einem Missbrauch generell beim Kreditkarteninstitut. Der Karteninhaber muss die zugestellten Abrechnungen innerhalb einer Frist von meist 30 Tagen auf deren Korrektheit überprüfen und Ungereimtheiten so-

fort melden. Überprüfen Sie auch den Verfügungsrahmen bei einer Kreditkarte und verzichten Sie möglichst auf eine PIN für Bargeldabhebungen. Sollte ein Verzicht auf eine PIN nicht möglich sein, so öffnen Sie den PIN-Brief nicht, damit Sie nachweislich nicht die Bargeldfunktion nutzen können.

Per Telefon

Bei Telefonbanking kommen meist Sprachcomputer zum Einsatz, die jedem, der die passenden Kontonummern, PINs und TANs erbeutet hat, alle Funktionen zur Transaktion zur Verfügung stellt. Die Aufbewahrung dieser Daten ist somit die Sicherheitslücke Nr. 1: Wer diese z.B. in seiner Brieftasche herumträgt, riskiert bei einem Diebstahl, dass sein Konto bis zum Limit geplündert wird.

Über das Internet

Beim Online- oder Internetbanking kommuniziert der Bankkunde via Computer und Internet mit dem Großrechner der Bank. – Hier ist die Sicherheit Ihrer Bank zugleich eine grundsätzliche Frage der Sicherheit Ihres PCs mit Internetanschluss! Je nach Verfahren, mit dem Sie Ihre Geldgeschäfte erledigen, ist das Risiko groß – oder klein. Unterschiede und Risiken verschiedener Verfahren zeigt Übersicht 2 auf Seite 28.

Die meisten Online-Bankkunden nutzen die **Internetseite ihrer Bank**. Man gibt in dem Internetbrowser die Internetadresse seiner Bank ein, loggt sich dort mit Nutzerkennung und Passwort („Online-PIN") ein, und benötigt für Transaktionen wie eine Überweisung noch eine Transaktionsnummer TAN. Moderne Bankräuber können sich in diesem Verfahren „einschalten", wenn die Bankkunden unaufmerksam sind: Durch Spam-E-Mails mit infizierten Anhängen können Schadprogramme (Trojaner) auf den Computer des arglosen Nutzers installiert werden, oder die Räuber versuchen „Phishing". Das ist eine gefälschte E-Mail, die angeblich von einer Bank stammt und Links zu falschen Internetseiten enthält. Dort wird auf einer Seite, die so aussieht wie die der Bank, die Eingabe der PIN und TANs „aus technischen Gründen" oder gar „aus Sicherheitsgründen" verlangt (siehe Bild nächste Seite). Wer diesen Quatsch glaubt und freimütig seine PIN und TANs eingibt, übermittelt sie direkt an die bösen Buben. Gerichte haben inzwischen entschieden, dass die Bankkunden wissen müssen, dass ihre Bank niemals per E-Mail nach PIN und TAN fragt und stellen die Banken von der Haftung frei. Relativ neu ist auch die Masche, dass man per E-Mail aufgefordert wird, seine Bank oder Kreditkarteninstitut unter einer falschen Nummer zurückzurufen. Dort wird dann persönlich von den Räubern nach PIN, TAN oder Kreditkartennummer gefragt.

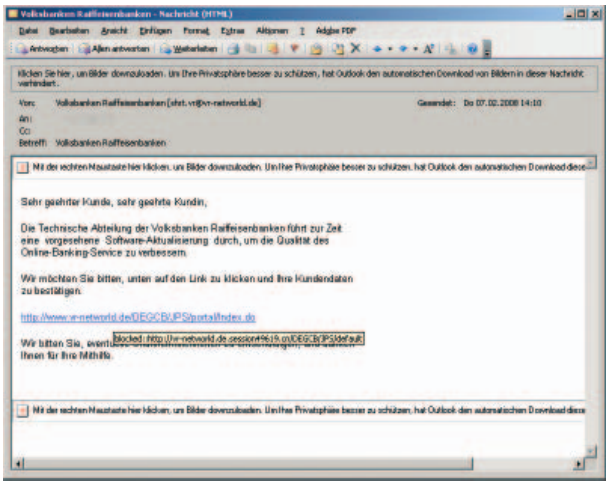
Inzwischen bieten Banken auch die Möglichkeit, mit indizierten Transaktionsnummern zu arbeiten (iTAN). Das heißt, die Liste der TANs ist durchnummeriert und der Bankrech-

Übersicht 1: Electronic-Banking und dessen Risiken

	Datenträgeraustausch	SB-Banking	Geldkarte	Kreditkarte	Telefonbanking	Online-Banking	Mobile Banking
Beschreibung	Überweisungen und Lastschriften werden in Dateiform auf Disketten oder anderen Datenträgern in der Bank eingereicht. Datei-Format ist „DTAUS".	Kunden bedienen sich mit EC-/Kundenkarte selbst an Geldautomaten, Kontoauszugsdruckern etc.	Mit Geld an Automaten der Bank aufladbare EC-/Kundenkarte der Bank.	Bezahlung durch Angabe der Kreditkartennummer, online mit zus. Code	Aufträge werden persönlich bei der Bank (Call-Center oder Sprachcomputer) via Telefon gegeben.	Der Zugriff auf das Bankkonto erfolgt mittels Datenfernübertragung via Internet.	Abwicklung von Bankgeschäften mit Mobiltelefonen und PDAs mit Unterstützung von SMS oder Internet.
Risiko und Sicherheit	**Unterschriftenfälschung.** Legitimation durch einen Datenträgerbegleitzettel mit Unterschrift des Kontobevollmächtigten.	**Karten- und PIN-Diebstahl** durch „Über-die-Schulter-Blicken". Legitimation nur durch PIN.	**Kartenverlust.** Aufgeladenes Geld kann ohne Legitimation verwendet werden.	**Karten- bzw. Nummerverlust.** Risikoträger ist Kreditkartenfirma!	**PIN/TAN-Diebstahl durch Einbruch.** Legitimation durch Telebanking-PIN und TAN	siehe Übersicht 2	siehe Übersicht 2
Risikostufe	mittel	mittel	hoch	gering	mittel	Niedrig bis hoch	Noch nicht abschätzbar

ner fragt z.B. nach der 23. TAN auf der Liste. Bei klassischem Phishing mag das helfen, wenn aber durch ein Schadprogramm der Rechner des Bankkunden so manipuliert ist, dass hinter einer gefälschten Bankenwebsite die Zugangsdaten zeitnah an die echte weitergegeben werden können, ist jedoch auch dieser Schutz nutzlos. Auch sogenannte eTANs, die der Bankkunde mit einem elektronischen Zusatzgerät erzeugt, können prinzipiell bei einer solchen „man-in-the-middle-attack" abgefangen und missbraucht werden.

Nur zwei Schutzverfahren können derzeit beim Online-Banking per Internetseite ausreichend schützen: mTAN und eTAN plus. Bei ersterem sendet die Bank dem Kontoinhaber eine TAN als SMS auf sein Handy. Diese mobile TAN (mTAN) hat nur eine kurze Gültigkeit und der Kunde sieht in der SMS nochmals die Höhe des zu transferierenden Betrages und seine Kontonummer. Nur wenn der Bankräuber auch das Handy erbeutet hat, wäre dieser Schutz wirkungslos. Die komplizierte eTAN-plus-Technik setzt ein signierendes Gerät zum TAN-Erzeugen beim Bankkunden voraus. In dieses muss seine EC-Karte eingelegt werden, um es zu nutzen. Für eine Transaktion erhält man auf der Banken-Seite zwei Codes: einen Banken- und einen Transaktionscode, der aus den ersten sechs Stellen der Empfänger-Kontonummer besteht. Beide werden in dem Signaturgerät eingegeben, in dem dann eine Überweisungs-TAN erscheint. Das komplizierte Verfahren wird aber nur von wenigen Banken angeboten.



Eine klassische „Phishing-E-Mail mit falschem Absender und Link.

Generell gilt, dass man beim Internetbanking via Banken-Homepage immer aufmerksam sein muss, auf welcher Seite man sich tatsächlich befindet. Banken-Websites beginnen meist mit https:// und da die Übertragung verschlüsselt ist, kann man sich durch Klick auf das Schloss-Symbol rechts neben der Adresszeile im Internetbrowser das sog. SSL-Zertifikat anzeigen lassen: Hier muss der Name der Organisation identisch mit der Bank sein. Leider sind bei manchen Banken die registrierten Firmennamen nicht identisch. So ist z.B. bei den Volksbanken das Zertifikat auf „Fiducia IT AG" eingetragen. Inzwischen sind auch Fälle bekannt, dass selbst bei korrekter Anzeige in der Adresszeile eine falsche Seite angezeigt wird. Diese „Pharming" genannte Methode wird durch Schadprogramme (Trojaner) bewirkt. Hier hilft nur, immer das SSL-Zertifikat zu prüfen – und generell einige Regeln zu beachten, siehe Kasten „Tipps".

Nummer sicher: Mit Banking-Software und Internet

Sicherer ist es, die Kontenführung mit einer Finanz-Software zu erledigen und darüber via HBCI-Verfahren Online-Banking zu betreiben. Bekannte Programme sind z.B. StarMoney, Lexware Quicken oder VR-Networld Software. Bei HBCI (HomeBanking Computer Interface) kommt entweder eine Chipkarte mit Lesegerät zum Einsatz,

Übersicht 2: Varianten des Online-Bankings und dessen Risiken

	Internetseite der Bank (Browserbasiert)	Mit Banking-Software	Mobile Banking
Beschreibung	Bankkunden nutzen Internetbrowser und die Internetseite der Bank	Bankkunden nutzen Software, um Kontostände abzurufen oder Transaktionen zu starten. Vorbereitung kann offline erfolgen.	Bankkunden nutzen entweder speziell an Handies angepasste Internetseiten oder haben Bank-Software auf Handy/Smartphone installiert.
Sicherheitsverfahren	• PIN/TAN[1)] • iTAN[2)] • mTAN[3)]	• PIN/TAN[1)] • iTAN[2)] • HBCI/HBCI+[4)]	• PIN/TAN[1)] • mTAN[3)]
Risiken	Hoch: Phishing, Pharming	Mit HBCI keine	Noch nicht abschätzbar

1) PIN = Persönliche IdentifikationsNummer, TAN = TransAktionsNummer
2) iTAN = indizierte TransAktionsNummer
3) mTAN = mobile TransAktionsNummer
4) HBCI = HomeBanking Computer Interface

oder eine sog. Schlüsseldatei, die auf Diskette oder USB-Stick gespeichert wird. Aber nur Lesegeräte der Klasse 2 oder höher können garantieren, dass die eingegebene PIN und der daraus erzeigte Schlüssel nicht über ein Schadprogramm auf dem PC des Nutzers missbraucht werden kann. Das Restrisiko, dass das Finanzprogramm selbst manipuliert wird, kann durch eine Desktop-Firewall, die auf eine plötzliche Veränderung der Software hinweist, verringert werden. Die Gefahr von Phishing und Pharming ist hier nicht vorhanden.

Bankgeschäft via Handy

Der letzte Schrei ist heute „Mobile Banking" – wenn das Handy zur Fernbedienung des Bankkontos wird. Allerdings ist hiermit nicht der klassische Anruf gemeint: Mit Handies oder „Smartphones" mit Internetbrowser und Datenverbindung via GPRS oder UMTS kann der Bankkunde über speziell gestaltete Seiten auch „Online-Banking" unterwegs betreiben. Als Sicherheitsverfahren kommt das klassische PIN/TAN oder auch die mTAN via SMS zum Einsatz. Schadprogramme auf Handies sind zurzeit noch relativ unbekannt – allerdings warnen Sicherheitsexperten vor der Aufrüstung der Online-Räuber in diesem Bereich. Auch hier gilt: Aufmerksamkeit schafft Sicherheit.

Fazit

Wenn Sie elektronische Bankgeschäfte, insbesondere Online-Banking betreiben, müssen Sie diese Sachverhalte wissen! Da hilft es Ihnen nicht, im Schadens- und Streitfall vor Gericht zu sagen, dass Sie den Computer zwar zu Geldgeschäften nutzen, aber sonst keine Ahnung von Computern und Sicherheit im Internet haben. Die aktuelle Rechtsprechung setzt schließlich immer mehr Know-how über Computersicherheit bei Bankkunden voraus.

DLG-Arbeitsgruppe Anwenderberater Wilfried Richarz, Renke Harms, Hartmut Heller, Dierk Koch, René Pommer, Rüdiger Warnecke, Rainer Winter

Tipps zur Sicherheit beim Online-Banking mit dem Internetbrowser

1. **Geben Sie die Internetadresse Ihrer Bank direkt in die Adresszeile des Browsers ein.** Prüfen Sie, ob die Seite verschlüsselt angezeigt wird (Adresse beginnt mit „https://", ein Schloss in Statuszeile des Browsers wird angezeigt). Klicken Sie nicht auf Links in E-Mails, die angeblich von Ihrer Bank kommen, sondern
2. **vergewissern Sie sich, mit wem Sie es zu tun haben.** Nicht jeder ist im Internet der, der er vorgibt zu sein. Es ist relativ einfach, eine E-Mailadresse zu fälschen, oder eine ganze Internetseite vorzugaukeln – eventuell auch die Seite einer Bank, bei der Sie sich einloggen wollen. Überprüfen Sie die Adresszeile des Browsers daraufhin, ob die Adresse Ihrer Bank korrekt wiedergegeben ist und prüfen Sie das SSL-Zertifikat anhand Klick auf das Schlosssymbol neben der Adresszeile.
3. **Gehen Sie sorgfältig mit sensiblen Daten und Zugangsmedien um.** Speichern Sie Passwörter, PINs und TANs, Kreditkartennummern nicht auf Ihrer Festplatte ab.
4. **Nutzen Sie auf Ihrem PC eine Desktop-Firewall und einen laufend aktualisierten Virenscanner.** Infos dazu unter www.bsi-fuer-buerger.de „Schützen – aber wie?"
5. **Nutzen Sie Mozilla Firefox als Internetbrowser.** Der Microsoft Internet Explorer ist beliebtes Angriffsziel von Schadsoftware und hat oft Sicherheitslücken.
6. **Aktualisieren Sie Ihr Betriebssystem und Internetbrowser regelmäßig.** Aktivieren Sie dazu bei Windows „Automatische Updates" in der Systemsteuerung.
7. **Konfigurieren Sie den Internetbrowser korrekt.** Deaktivieren Sie die AutoVervollständigen-Funktion.
8. **Setzen Sie nur Programme aus vertrauenswürdigen Quellen ein.** Laden Sie nur solche Programme aus dem Internet auf Ihre Festplatte, deren Quelle Sie als seriös betrachten können, und stellen Sie sicher, dass es sich wirklich auch um diesen Anbieter handelt. Mit Programmen können Viren oder trojanische Pferde übertragen werden. Klicken Sie nie auf Anhänge in E-Mails von Absendern, die Ihnen unbekannt sind.
9. **Nutzen Sie, wenn Ihr PC mit dem Internet verbunden ist, ein Benutzerkonto, das als „Eingeschränkter Nutzer" eingestellt ist.** Dadurch werden Schadprogrammen Manipulationen erschwert.
10. **Betreiben Sie niemals von fremden öffentlichen Rechnern Online-Banking mit dem Internetbrowser.** Diese Rechner können manipuliert sein.