

ONLINE-BANKING-SICHERHEIT

7., vollständig aktualisierte Auflage



Informationen für Online-Banking-Nutzer

Berlin, November 2007

fokus:verbraucher

Eine Information
der privaten Banken



Vorbemerkung

Neben den enormen Vorteilen und Möglichkeiten sind mit der Nutzung des Internets auch verschiedene Sicherheitsrisiken verbunden. Deshalb führen die Banken umfangreiche Maßnahmen zur Absicherung der im Rahmen des Online Banking übermittelten und bankseitig verarbeiteten Daten durch. Diese Maßnahmen gewährleisten beispielsweise, dass vertrauliche Daten bei der Übertragung über das Internet nicht unberechtigt eingesehen und nicht unautorisiert verändert werden können.

Auf die vom Bankkunden für das Online Banking eingesetzten Systeme haben die Banken in der Regel jedoch keinen Einfluss. Denn ausschließlich die Bankkunden wählen das System aus, das sie für das Online Banking einsetzen. Außerdem wird das jeweilige System, beispielsweise ein an das Internet angeschlossener Rechner (PC), von ihnen in der Regel auch für viele andere Anwendungen genutzt.

Die vom Bankkunden eingesetzten Systeme sind damit potenziellen Gefahren ausgesetzt, die von den Banken nicht kontrolliert werden können. Aus diesem Grund können die Banken keine Haftung für diese Kundensysteme übernehmen.

Typische Gefahren im Internet sind heute

Mitlesen, Verändern und Löschen von Daten bei der Übertragung sowie Erschleichen von Daten durch Vorgabe falscher Tatsachen beispielsweise mit Hilfe der folgenden Methoden:

- Viren, Würmer: Programme, die sich selbstständig verbreiten bzw. über E-Mails im Internet versandt werden und Schäden auf Ihrem PC anrichten können.
- Trojanische Pferde: Programme, die unbemerkt vom Nutzer sicherheitskritische Funktionen, wie zum Beispiel das Abfangen von Passwörtern, durchführen.
- Phishing: Vortäuschung von falschen Namen, Internetseiten und Adressen.
- Pharming: Umleiten einer Verbindung auf gefälschte Server.
- Rootkits: Schadsoftware, die mit den Rechten des Systemadministrators agiert, ohne dass der rechtmäßige Administrator dies bemerkt. Die Grenze zu Trojanischen Pferden ist fließend.
- Hackereinbrüche: Unberechtigte dringen über das Internet in Ihren PC ein.

Für das Online Banking wurden seitens der Banken umfangreiche Sicherheitsvorkehrungen getroffen, die einen wirksamen Schutz gegen Angriffe bei der Übertragung der Daten über das Internet oder der Verarbeitung auf dem Bankenserver bieten.



Was kann jeder Kunde tun?

Damit die von den Banken vorgesehenen Sicherheitsvorkehrungen nicht durch unberechtigte Manipulationen unterlaufen werden können, muss jeder Kunde auch seinerseits technische Vorkehrungen zum Schutz der von ihm eingesetzten Systeme treffen. Dazu gehören weiterhin ein sicherheitsbewusstes Verhalten im Internet sowie eine regelmäßige Kontrolle der Kontobewegungen.



Selbstverständlich lauern nicht überall im Internet Gefahren. Nicht jeder Kommunikationspartner will und wird Online-Banker schädigen. Schon wenn Bankkunden die folgenden **zehn Regeln** beachten, können sie die Sicherheit an ihrem PC um ein Vielfaches steigern und die verbleibenden Restrisiken des Internets und des Systems auf ein Minimum reduzieren. Sollten Bankkunden dennoch einmal den Verdacht haben, auf betrügerische Aktionen von Internetkriminellen gestoßen zu sein, dann sollten sie den Online-Zugang zu ihrem Konto sofort sperren lassen und nicht nachvollziehbare Umsätze umgehend bei ihrer Bank reklamieren. Um den Betrug nachvollziehen zu können, sollten alle relevanten Informationen gesichert werden. In diesem Fall darf deswegen die Festplatte nicht sofort formatiert werden.

Ganz unabhängig von der Nutzung des Online Banking ist die Datensicherung besonders wichtig. Denn es ist meist unmöglich oder zumindest sehr aufwendig, die gespeicherten Informationen zu retten, wenn „das Kind erst einmal in den Brunnen gefallen ist“. Zum bequemen Datensichern können Sie zum Beispiel eine Speicherung auf einer Wechselfestplatte, CD oder DVD vornehmen. Dabei sollten Sie immer darauf achten, dass Sie geänderte sowie neu dazugekommene Daten regelmäßig sichern.

Sicherheitsregeln

1. Setzen Sie Sicherheitssoftware ein – unter anderem einen aktuellen Virenschanner

Setzen Sie zusätzliche Sicherheitssoftware ein. Denn manche Sicherheitsprobleme lassen sich nicht allein mit „Bordmitteln“ des PC-Betriebssystems lösen. Ein wichtiges Zusatzwerkzeug ist ein leistungsfähiger Virenschanner, der permanent online aktualisiert wird und damit in der Lage ist, auch neue Viren zu erkennen. Fast täglich werden neue Viren entdeckt. Daher ist es durchaus möglich, dass Sie sich bei einem Ausflug in die Online-Welt „infizieren“. Ferner können sich grundsätzlich auch außenstehende Dritte ein Bild von den auf Ihrem PC gespeicherten Daten machen, solange Sie online sind, da Ihr Computer im Netz eine eigene Adresse hat und so von außen erreichbar ist.



Bei unzureichenden Sicherheitsmaßnahmen laufen Sie Gefahr, dass Unbefugte auf die auf Ihrem PC gespeicherten Informationen (z. B. PIN und TANs, die dort nicht gespeichert sein sollten) zugreifen könnten. Kriminelle setzen dazu „**Spyware**“ ein. Diese Spionage-Programme können unbemerkt auf Ihrem Computer installiert werden und sind in der Lage, im Hintergrund nach sensiblen Daten wie Kontoinformationen oder Passwörtern zu suchen oder Ihre Tastatureingaben aufzuzeichnen. Die Daten werden dann ebenfalls unbemerkt an eine fremde E-Mail-Adresse oder einen fremden Server verschickt. Kriminelle bauen Spyware getarnt in Internetseiten, E-Mails oder E-Mail-Anhänge ein. Daher werden solche Programme auch **Trojanische Pferde** genannt. Schadprogramme, die sich besonders auf systemnahe Funktionen des Betriebssystems stützen, werden auch als Rootkit bezeichnet, wobei die Grenzen fließend sind. Sobald ein infiziertes Objekt geöffnet wird, installiert sich die Spyware auf Ihrem Computer – ohne dass Sie es merken. Deshalb löschen Sie verdächtige E-Mails, ohne sie zu öffnen. Öffnen Sie keine verdächtigen Anhänge, auch wenn sie von einer Ihnen

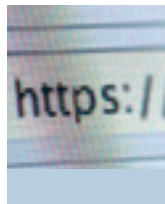
bekannten E-Mail-Adresse zu kommen scheinen. Deaktivieren Sie die „Autovorschau-Funktion“ Ihres Mail-Programms, um ein automatisches Öffnen der Mail zu verhindern.

Gegen diese Angriffe von außen bietet die Installation einer **persönlichen Firewall** Schutz. Eine Firewall ist ein Programm, das den gesamten eingehenden und ausgehenden Netzverkehr überwacht und nur bekannte oder autorisierte Verbindungen zulässt. Im Fachhandel gibt es darüber hinaus eine Vielzahl von Programmen, die Ihnen dabei helfen, das Sicherheitsniveau Ihres PCs zu heben, wie beispielsweise PC-Sicherheitssysteme mit Zugriffsschutz und Verschlüsselung.

Informieren Sie sich regelmäßig über Sicherheitsaspekte bei der Nutzung des Internets sowie geeignete Schutzmaßnahmen. Informationen zur Sicherheit beim Online Banking erhalten Sie auf der Internetseite Ihrer Bank. Darüber hinaus finden Sie Informationen rund um das Thema Sicherheit im Internet beim Bundesamt für Sicherheit in der Informationstechnik unter der Adresse <http://www.bsi-fuer-buerger.de>. Kostenfreie Sicherheitssoftware finden Sie zum Beispiel dort in einer speziellen Rubrik unter <http://www.bsi-fuer-buerger.de/toolbox/tools.htm>.

2. Schützen Sie sensible Daten bei der Übertragung über offene Netze

Jede ungesicherte Datenübertragung im Internet kann von unberechtigten Dritten abgefangen oder ausgespäht werden. Die Banken haben dafür gesorgt, dass die im Rahmen des Online Banking übermittelten Daten verschlüsselt übertragen werden. Geben Sie Ihre PIN und Ihre TANs nur ein, wenn Sie sicher davon ausgehen können, dass Sie sich auf der **geschützten Internetseite der Bank** befinden und Sie eine verschlüsselte Verbindung nutzen. Dies können Sie unter anderem daran erkennen, dass die Internetadresse (URL) Ihrer Bank mit „https://“ beginnt.



Beachten Sie weiterhin, dass die beim Online Banking übertragenen Daten bei der lokalen Speicherung nicht automatisch verschlüsselt werden und deshalb durch weitere Sicherheitsvorkehrungen geschützt werden müssen. Generell sollten Sie sensible Daten niemals unverschlüsselt über offene Netze übertragen. Schützen Sie daher Ihre vertrauliche Korrespondenz durch den Einsatz anerkannter Verschlüsselungsverfahren. Hierzu existieren auch kostenfreie Lösungen, die Sie zum Beispiel auf den Internetseiten der Bundesanstalt für die Sicherheit in der Informationstechnik unter www.bsi-fuer-buerger.de/toolbox/tools.htm finden.

3. Vergewissern Sie sich, mit wem Sie es zu tun haben

Nicht jeder ist im Internet der, der er zu sein vorgibt. Für Experten ist es vergleichsweise einfach, eine E-Mail-Adresse zu fälschen oder eine ganze Internetseite vorzugaukeln – eventuell auch die einer Bank, bei der Sie sich einloggen möchten.

Überprüfen Sie die URL, das heißt die Adresszeile des Browsers, und damit, ob die Adresse Ihrer Bank korrekt wiedergegeben ist. Bereits minimale Abweichungen könnten auf eine gefälschte Internetseite hinweisen. Überprüfen Sie auch die vom Browser gelieferten Sicherheitsinformationen wie die Ergebnisse einer **„Zertifikatsprüfung“**. Mit diesen wird unter anderem die Richtigkeit der Angaben des Servers,

mit dem Sie verbunden sind, von einer unabhängigen Instanz – dem Zertifikatsaussteller – bestätigt. Sie sollten prüfen, ob der im Sicherheitszertifikat angegebene Name der Internetseite mit dem Namen Ihrer aufgerufenen Seite übereinstimmt. Einer Adresse, bei der der (scheinbare) Adressinhaber gleichzeitig der Zertifikatsaussteller ist, sollten Sie



nicht vertrauen. Das Zertifikat sollte von einer vertrauenswürdigen Institution stammen und gültig sein. Im Zweifelsfall können Sie sich auch bei Ihrer Bank über die vertrauenswürdigen Instanzen informieren, die Serverzertifikate für das von Ihnen genutzte Online Banking ausstellen.

Geben Sie Informationen nur preis, wenn Sie verlässlich wissen, wer diese Daten erhält und was mit diesen geschehen soll. Abweichungen vom gewohnten Ablauf sollten Sie misstrauisch machen, zum Beispiel die Aufforderung zur Eingabe der PIN oder einer TAN zu einem unerwarteten Zeitpunkt.

Um an benötigte Informationen zu kommen, täuschen Hacker gerne Vertrauensfunktionen vor: Hierzu gibt es beispielsweise das so genannte **Phishing** (eine Zusammensetzung aus den englischen Wörtern „password“ und „fishing“), bei dem Sie von kriminellen Betrügern aufgefordert werden, Ihre vertraulichen Zugangsdaten (z.B. PIN und TANs) auf der Internetseite Ihres Instituts zu aktualisieren oder erneut einzugeben. Die Aufforderung dazu kann sowohl mittels einer E-Mail als auch durch manipulierte Internetseiten erfolgen. Der jeweilige Link führt dann allerdings zu einer gefälschten Internetseite des Angreifers, der auf diesem Weg Ihre vertraulichen Zugangsdaten ausspäht.

Stellen Sie sicher, dass Sie Ihre vertraulichen Zugangsdaten immer nur auf der echten Internetseite Ihres Instituts eingeben. Dies können Sie unter anderem dadurch gewährleisten, dass Sie die Internetadresse Ihrer Online-Banking-Verbindung immer nur von Hand in die Adresszeile Ihres Browsers eingeben. Ferner sollten Sie auf Auffälligkeiten beim Online Banking achten, beispielsweise auf Abweichungen im Erscheinungsbild des gewohnten Online-Banking-Auftritts Ihrer Bank.


Eine andere Möglichkeit des Angriffs auf Ihre vertraulichen Zugangsdaten stellt das so genannte **Pharming** dar. Hierbei wird eine Internetverbindung auf einen gefälschten Server umgeleitet. Dafür muss eine entsprechende Schadsoftware entweder die Adressauflösung der „hosts“-Datei auf Ihrem PC fälschen oder es wird



versucht, gleich die für die Adressauflösungen zuständigen „DNS-Server“ zu manipulieren. Unterbinden Sie solche Angriffe mit dem Einsatz aktueller Antivirensoftware und einer persönlichen Firewall. Und prüfen Sie immer, ob die aufgerufene Seite mit einem gültigen Zertifikat ausgestattet ist.

4. Gehen Sie sorgfältig mit sensiblen Daten und Zugangsmedien um

Schützen Sie Ihre Zugangsdaten bzw. Ihr **Zugangsmedium** zum Online Banking (PIN und TANs bzw. Chipkarte) vor unberechtigtem Zugriff. Geben Sie die geheimen Zugangsdaten niemals auf einer anderen Internetseite als der Ihrer Bank ein oder in sonstiger Weise gegenüber einem Dritten preis. Beispielsweise sollten Sie beim Online Shopping Ihre persönlichen Zugangsdaten für das Online Banking weder auf der Shopping-Seite noch auf den Seiten eines Online-Überweisungsdienstes eingeben.



Speichern Sie **sensible Daten** (Passwörter, PIN und TANs, Kreditkartennummern) nicht auf Ihrer PC-Festplatte ab. Dies könnte sonst an PCs, die nicht ausschließlich von Ihnen benutzt werden, wie zum Beispiel am Arbeitsplatz, dazu führen, dass Dritte die von Ihnen gespeicherten Daten einsehen können. Auch spezielle Spyware-Programme, die auf Ihren Rechner gelangt sind, könnten diese Daten ausspähen und zum Beispiel per E-Mail versenden. Wenn Sie zur Erhöhung der Sicherheit zusätzliche Ausrüstung wie zum Beispiel einen Chipkartenleser mit PIN-Eingabetastatur benutzen, geben Sie die dafür vorgesehenen vertraulichen Daten nur dann ein, wenn Sie von diesem Gerät dazu aufgefordert werden. Speichern Sie vor allem Ihr Passwort für die Einwahl ins Internet nicht ab. So erschweren Sie den Aufbau unerwünschter Internetverbindungen.

Vergewissern Sie sich bei jeder Eingabe Ihrer persönlichen Zugangsdaten, dass es sich beim Adressaten um Ihre Bank handelt. Ihre Bank wird Sie niemals zum

Beispiel per E-Mail oder auch Telefon kontaktieren, um nach Ihren geheimen Zugangsdaten wie PIN und TAN zu fragen. Ebenfalls werden Sie niemals nach mehreren TANs gleichzeitig gefragt. Und geben Sie nie eine oder mehrere TANs ein, ohne zuvor einen Auftrag für die Bank verfasst zu haben. Beantworten Sie solche E-Mails nicht. Folgen Sie auch nicht den dort angegebenen Instruktionen – selbst wenn Ihnen mit negativen Konsequenzen wie beispielsweise einer Kontosperrung gedroht wird. Informieren Sie Ihre Bank über diesen Betrugsversuch.

5. Wählen Sie ein sicheres Passwort

Wenn Sie Ihren PC benutzen wollen und beispielsweise eine Anwendung wie das Online Banking starten, müssen Sie sich in der Regel mit einem Passwort ausweisen. Mit Hilfe dieser persönlichen Identifikation zeigen Sie, wer Sie sind, und beweisen, dass Sie berechtigt sind, an diesem Gerät oder mit dieser Anwendung zu arbeiten. Deswegen kommt es darauf an, dass Sie dieses Geheimnis mit niemandem teilen. Das bedeutet aber auch, dass Sie diese Identifikationshilfe nirgendwo aufschreiben sollten und Sie sich Ihr ganz individuelles und schwer zu erratendes Passwort ausdenken.

Ein **gutes Passwort** ist in der Regel sechs bis acht Stellen lang und besteht aus einer Mischung aus Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen. Beim Internetbanking wird diese Sicherheit durch die Kombination aus PIN und TAN erreicht. Auf jeden Fall sollten Sie Eigennamen, wohl bekannte Begriffe (= Begriffe, die sich in einem Wörterbuch wiederfinden lassen), Wiederholungen einzelner Zeichen („AAAAAA“) oder Tastaturfolgen („qwertz“) vermeiden. Verwenden Sie weder das eigene Geburtsdatum noch das Geburtsdatum einer anderen Ihnen bekannten Person. Für die Auswahl eines schwer zu erratenden Passworts gibt es verschiedene Strategien: Eine einfache stellt die Bildung des Passworts aus den Anfangsbuchstaben eines Mottos oder Gedichts dar. Durch Einfügen von Sonderzeichen oder Ziffern kann es noch weiter verfremdet werden. So kann „VinF&HnH“ etwa für „Vorsicht ist



nicht Furcht und Hast nicht Heldenmut“ stehen. Wechseln Sie Ihr Passwort, wenn Sie Grund zur Annahme haben, dass irgendetwas Ihr Geheimnis erfahren haben könnte.

6. Setzen Sie nur Programme aus vertrauenswürdiger Quelle 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. Denn: Mit Programmen können **Viren oder Trojanische Pferde** übertragen werden. Dies kann auch durch das Öffnen eines Anhangs einer E-Mail geschehen. Öffnen Sie deshalb solche Anhänge nicht, wenn Ihnen Absender oder Inhalt unbekannt ist. Speichern Sie den Inhalt zuerst ab, prüfen Sie ihn mit entsprechenden Sicherheitsprogrammen, und öffnen Sie erst dann die fragliche Datei. Überlegen Sie sich genau, ob Sie Zusatzprogramme (Plug-ins) beispielsweise zum Darstellen von 3-D-Welten oder zum Audio-Empfang in Ihren Web-Browser einbinden wollen. Denn auch solche Plug-ins können zusätzliche, unkontrollierbare Sicherheitslücken eröffnen.

7. Nutzen Sie aktuelle Programmversionen



Nutzen Sie nur die aktuelle Version Ihres bevorzugten Internetbrowsers und des Betriebssystems Ihres PCs. Denn nur in der aktuellsten Version können die bis dahin bekannt gewordenen Sicherheitslücken in diesem Programm geschlossen sein. Zusätzlich zu den Programmversionen werden von den Herstellern kleine Programme entwickelt, so genannte Bug-Fixes oder Patches, die entdeckte Sicherheitsprobleme beheben. Diese **Bug-Fixes oder Patches** sollten Sie

schnellstmöglich installieren, um Ihren PC vor den entdeckten Sicherheitslücken zu schützen. Informieren Sie sich deshalb regelmäßig über die neuesten Entwicklungen. Die meisten Hersteller unterhalten entsprechende Informationsdienste.

8. Führen Sie einen Sicherheitscheck auf Ihrem PC durch

Nehmen Sie sich einige Minuten Zeit, bevor Sie Online Banking über Ihren PC durchführen, und machen Sie einen persönlichen Sicherheitscheck. Aktivieren Sie die vorhandenen Sicherheitsmechanismen, mit denen der Zugriff auf Ihren PC geschützt wird. Diese bestehen beispielsweise in der Eingabe eines Passworts, das beim Starten des PCs durch das Betriebssystem oder durch den Bildschirmschoner abgefragt wird. Grundsätzlich sollten Sie im Internet nicht als Administrator, sondern nur mit **minimalen Nutzerrechten** arbeiten. Dadurch werden Manipulationen und unerlaubte Zugriffe erschwert.

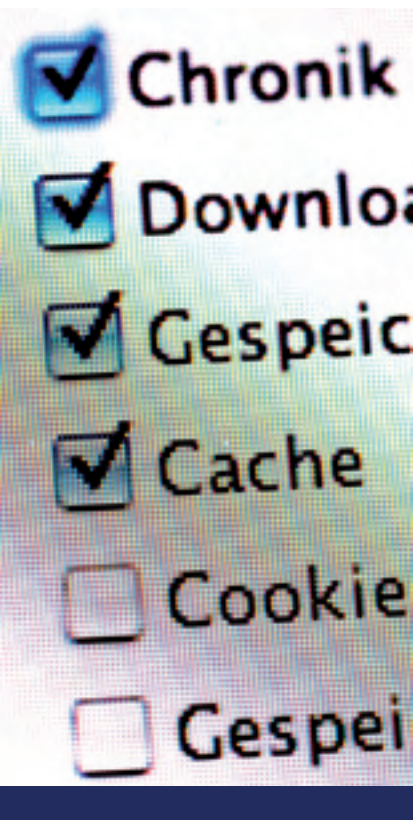
Beachten Sie, dass Sie bei einem nicht nur von Ihnen genutzten PC, wie dies beispielsweise in einem Internetcafé der Fall ist, niemals genau wissen können, inwieweit der Zugang durch aktuelle Sicherheitssoftware geschützt ist und welche Programme im Einzelnen auf diesem PC tatsächlich ausgeführt werden. Auch die Tastaturen können manipuliert sein. Sicherheit können Sie hier nicht erwarten. Deshalb ist von Online Banking von solchen Orten aus generell abzuraten.

9. Aktivieren Sie die Sicherheitseinstellungen des Browsers

Aktivieren Sie die Sicherheitseinstellungen Ihres Internetbrowsers. Ihre Sicherheit im Internet lässt sich beträchtlich steigern, wenn Sie die Sicherheitsoptionen Ihres Internetbrowsers intelligent einsetzen.



Wichtig ist hier vor allem, dass Sie die Zulassung von **ActiveX-Controls ausschließen** und die Ausführung von Java-Applets-Skripten nur nach Rückfrage und Prüfung gestatten. Bei diesen so genannten aktiven Inhalten handelt es sich um kleine eigenständige Programme, die auf Ihrem PC ausgeführt werden und dort unter Umständen unerwünschte Aktionen auslösen können (z.B. Ihre Passwortdatei per E-Mail versenden). Verwenden Sie nicht die „Auto-Vervollständigen“-Funktion Ihres Browsers, durch die die Eingabe von Benutzernamen und Passwörtern gespeichert und Übereinstimmungen vorgeschlagen werden.



Cookies legen Informationen in ein ganz spezielles Verzeichnis auf der Festplatte ab, lesen aber keine anderen Daten aus. Im Zweifel entscheiden Sie sich gegen solche „Kekse“, die eine fremde Internetseite auf Ihrer Festplatte ablegt, denn diese Daten könnten auch dazu genutzt werden, Benutzerprofile anzulegen. Doch eine grundsätzliche Ablehnung von Cookies ist nicht in allen Fällen die beste Strategie. Lehnen Sie ein Cookie ab, können Sie möglicherweise einige Web-Angebote nicht nutzen. Nehmen Sie die Datenpakete an, erkennt Sie der Web-Server bei jeder Einwahl wieder. Dem Server ist es so möglich, eine „Akte“ zu führen und ein Nutzerprofil zu erstellen. Registriert wird beispielsweise, welche Suchbegriffe verwendet und welche Internetseiten angesteuert werden. Sind Ihre Vorlieben bekannt, könnten Werbebanner zielgerichtet nach Ihren Interessen platziert werden. Durch den Einsatz von zusätzlicher Sicherheitssoftware kann die Erstellung von Nutzerprofilen jedoch verhindert werden. So können Sie die Vorzüge der Cookies nutzen und gleichzeitig verhindern, dass Unbefugte Ihr Verhalten für von Ihnen nicht gewünschte Zwecke auswerten.

10. Stellen Sie Ihr Girokonto nicht für betrügerische Finanztransaktionen zur Verfügung



Auf Internetseiten und per E-Mail sprechen Kriminelle derzeit gezielt Inhaber von Bankkonten in Deutschland an, um sie für eine Tätigkeit als so genannte „Finanzagenten“ zu gewinnen. Über das inländische Bankkonto sollen diese „Finanzagenten“ Zahlungen Dritter entgegennehmen und möglichst umgehend per Bargeldversand an eine im Ausland befindliche Person überweisen.

Als Entgelt winkt eine Provision, die vom Überweisungsbetrag abgezogen wird. Die unseriösen Auftraggeber begründen diese Abwicklungsmethode beispielsweise mit Kostenersparnissen gegenüber teuren Auslandsüberweisungen oder als Maßnahme zum Schutz sensibler Kundeninformationen. Wenn Sie auf ein solches Angebot eingehen, können Sie sich **strafbar und schadensersatzpflichtig** machen. Auch riskieren Sie Ihre persönliche Sicherheit, denn die Täter aus dem Kreis der organisierten Kriminalität schrecken vor nichts zurück.

Prüfen Sie alle Angebote kritisch, bei denen Sie Ihr Girokonto zur Abwicklung von Zahlungen für Firmen oder Personen, insbesondere im Ausland, zur Verfügung stellen sollen. Im Zweifel sollten Sie die Hände davon lassen. Erfolgen unerwartete Gutschriften auf das Konto, die die Kontoinhaber kurze Zeit später zurücküberweisen sollen, sollten diese in Zweifelsfällen mit ihrem Kreditinstitut oder ihrer örtlichen Polizei Kontakt aufnehmen. Etwaige Rückbuchungen sollten grundsätzlich nur auf das jeweilige Ursprungskonto der Buchung ausgeführt werden. Geschädigten Kontoinhabern – sowohl denjenigen, die unbewusst als Finanzagenten missbraucht wurden, als auch allen Opfern betrügerischer Zugriffe auf ihr Konto – wird empfohlen, Strafanzeige zu erstatten.

Glossar

ActiveX-Control	Ein ActiveX-Control ist ein kleines Windows-Programm, das sich beispielsweise mit Hilfe eines Web-Browsers ausführen lässt. Diese Controls können bereits auf dem Rechner vorhanden sein oder werden beim Aufruf einer Web-Seite automatisch heruntergeladen.
Cookies	Ein Cookie ist eine kleine Textdatei, die der Web-Browser auf Anweisung eines Web-Servers in dem PC des Anwenders speichert und die zum Beispiel Angaben über dessen Web-Anfragen enthält. Cookies dienen hauptsächlich als elektronischer Merktettel für den Server, um benutzerspezifische Browser-Abfragen festzuhalten, zum Beispiel, welche Web-Seite ein Nutzer wie häufig und wie lange besucht hat oder ob die angeforderte Web-Seite in einer bestimmten, vom Nutzer festgelegten Version übersandt werden soll.
Firewall	Als Firewall bezeichnet man Rechner, die den Datenverkehr zwischen einem lokalen Netz oder einem allein stehenden Rechner und anderen Netzwerken, zum Beispiel dem Internet, regeln. Die Firewall soll das lokale Netz bzw. den allein stehenden Rechner vor unbefugten Zugriffen schützen. Unter einer persönlichen Firewall wird ein Programm verstanden, das auf Ihrem PC eine Firewall realisiert, das heißt Ihren PC ohne Einsatz eines Zusatzrechners vor unerwünschten Zugriffen bewahrt.
Java-Applet	Java ist eine Anfang der 90er Jahre entwickelte Programmiersprache. Ein Java-Applet ist ein kleines Programm, das, nachdem es aus dem Internet heruntergeladen worden ist, innerhalb eines Browsers interpretiert und ausgeführt wird. Hierzu werden die Java-Befehle in HTML-Seiten eingebunden und beim Laden dieser HTML-Seite ausgeführt.
Patch	Kleines Programm, das zusätzlich zu den Programmversionen entwickelt wird, um entdeckte Sicherheitsprobleme möglichst zeitnah zu beheben.
Pharming	Unter Pharming oder auch DNS-Spoofing versteht man einen Angriff, bei dem ein Angreifer die IP-Adresse eines bekannten Domain-Namens durch seine eigene ersetzt. Bei einem solchen Angriff wird die URL richtig dargestellt, obwohl sich der Nutzer auf einer falschen Seite befindet.

Phishing	Angriffsmethode, bei der ein Angreifer die E-Mail-Adresse oder die Internetseite von Banken und Dienstleistern wie Internetservice-providern oder Internetkaufhäusern vortäuscht. Die Kunden werden aufgefordert, ihre Kontodaten sowie dazugehörige PIN, TANs und Passwörter auf einer gefälschten Internetseite einzugeben.
PIN	Persönliche Identifikationsnummer, dient zur Authentifikation einer Person.
Rootkits	Ein Rootkit ist ein betriebssystemnahes Softwarewerkzeug, das einem Computer mit dem Ziel schadet, die Tätigkeiten des Angreifers wie beispielsweise das Ausspähen von vertraulichen Zugangsdaten oder das Kopieren von Dateien zu verbergen. Mit Hilfe des Rootkits kann der Angreifer mit Administratorrechten agieren.
Spyware	Als Spyware werden Softwareprogramme bezeichnet, die Informationen über den PC des Nutzers, dessen Surfgewohnheiten oder auch dessen persönliche Daten (z.B. geheime Zugangsdaten für das Online Banking) ohne dessen Wissen oder gar Zustimmung an Dritte senden.
TAN	Transaktionsnummer, dient zur Autorisierung einer Transaktion.
Trojanisches Pferd	Trojanische Pferde sind Programme, die unbemerkt vom Nutzer sicherheitskritische Funktionen durchführen. Ziel der meisten Trojaner ist es, sensible Daten wie Passwörter auszuspähen und sie per E-Mail/Internet an den „Besitzer“ des Trojaners zu senden. Mit Hilfe von so genannten Backdoor-Trojanern kann der Hacker auf fremde Rechner zugreifen und hat dann praktisch die Fernkontrolle über alle Funktionen.
Viren	Computerviren sind Schadprogramme, die sich selbst reproduzieren und sich beispielsweise per E-Mail über das Internet weiterverbreiten können. Viren können auf den infizierten PCs teilweise erhebliche Schäden anrichten.
Würmer	Würmer sind Schadprogramme, die sich von Computer zu Computer über das Netzwerk selbsttätig weiterverbreiten. Ziel der Würmer ist es, so viele Computer wie möglich innerhalb eines Netzwerks zu befallen und auf diesen Schäden anzurichten.

Checkliste für den Ernstfall

Was Sie unbedingt beachten sollten, wenn Sie das Gefühl haben, dass Ihre Online-Banking-Daten nicht mehr geheim sind.

Immer wieder versuchen Trickbetrüger zum Beispiel mit E-Mails (Phishing) oder Schadsoftware (so genannten Trojanischen Pferden), die geheimen Online-Banking-Zugangsdaten von Bankkunden unbefugt zu erlangen. Was sollten Sie unternehmen, wenn Sie den Eindruck haben, Opfer eines Trickbetruges zu sein, indem Sie beispielsweise auf eine Phishing-Mail bereits reagiert oder ungewöhnliche Abläufe oder Abbrüche beim Online Banking bemerkt haben?



Hier haben wir Ihnen eine kleine Checkliste zusammengestellt:

Schritt 1	Zugang sperren
<input type="checkbox"/>	Wenn Sie vermuten, dass ein Unbefugter Kenntnis von Ihrer PIN und/oder Ihren TANs erlangt hat, so sperren Sie umgehend Ihren Zugang (z. B. durch mehrmalige bewusste Fehleingabe Ihrer PIN bzw. TANs, Spermitteilung gegenüber Ihrer Bank gemäß Teilnahmevereinbarung) und setzen Sie sich schnellstmöglich mit Ihrer Bank in Verbindung.
Schritt 2	Konto- und Depotstände prüfen
<input type="checkbox"/>	Bitte überprüfen Sie Ihre Konto- bzw. Depotumsätze anhand Ihres Kontoauszuges oder, sofern angeboten, über eine Funktion zur Anzeige offener Aufträge. Bei eventuellen Unstimmigkeiten informieren Sie bitte umgehend Ihre Bank.
Schritt 3	Virens Scanner installieren und/oder aktualisieren
<input type="checkbox"/>	Aktualisieren Sie Ihre Antivirensoftware und bringen Sie Ihr Betriebssystem auf den neuesten Stand. Weitere Informationen zum Schutz vor Viren und Trojanischen Pferden erhalten Sie im Internet unter http://www.bsi-fuer-buerger.de/toolbox/tools.htm .
Schritt 4	Virens Scanner aktivieren und Suchlauf starten
<input type="checkbox"/>	Prüfen Sie alle Laufwerke Ihres Computers gründlich auf eventuelle Viren oder Trojanische Pferde und andere Schadsoftware und entfernen Sie diese.
Schritt 5	Ergebnisse des Suchlaufes dokumentieren
<input type="checkbox"/>	Die Ergebnisse bzw. das Protokoll des Antivirenprogrammes sollten Sie speichern bzw. ausdrucken, um diese später ggf. Ihrer Bank / den Ermittlungsbehörden vorlegen zu können.
Schritt 6	Weiteres Risiko ausschließen
<input type="checkbox"/>	Haben Sie sich bei weiteren Online-Diensten (z. B. eBay, Amazon oder Elster – die elektronische Steuererklärung) mit Zugangsdaten über Ihren Computer angemeldet? Dann sollten Sie auch diesen Zugang sperren lassen. Sollten noch weitere Personen Ihren PC benutzen, informieren Sie diese bitte ebenfalls.

Generelle Hinweise zur Sicherheit im Internet

Immer aktuell	Halten Sie Ihr Betriebssystem und Ihre Antivirensoftware stets aktuell. Die Hersteller bieten regelmäßig Service- und Sicherheitsupdates an.
Regelmäßig prüfen	Führen Sie einen kompletten Scanlauf über alle Laufwerke Ihres Rechners durch. Wiederholen Sie dieses regelmäßig (z. B. einmal in der Woche).
Seien Sie skeptisch	Öffnen Sie keine Anhänge von E-Mails unbekannter Herkunft. Im Zweifelsfall fragen Sie vor dem Öffnen der Anlage beim Absender nach.
Daten bewahren	Geben Sie Ihre persönlichen Zugangsdaten nicht weiter. Selbst Ihre Bank und deren Mitarbeiter werden Sie zu keiner Zeit, weder persönlich, telefonisch noch per E-Mail, dazu auffordern, Ihre kompletten Zugangsdaten (Teilnehmernummer in Verbindung mit PIN und TANs) preiszugeben.
PIN/TANs nicht speichern	Ihre PIN und TANs dürfen auf keinen Fall auf Ihrem Rechner gespeichert werden. Sonst haben Trojaner leichtes Spiel.

Weitere Informationen rund um das Thema Sicherheit finden Sie im Internet auf den Seiten Ihrer Bank, des Bankenverbandes (<http://www.bankenverband.de>) sowie den Seiten vom Bundesamt für Sicherheit in der Informationstechnik (BSI) unter <http://www.buerger-cert.de>.

Die Reihe „fokus:verbraucher“

Informationen, die sich gezielt an Verbraucher richten, fasst der Bankenverband in einer eigenen Reihe „fokus:verbraucher – Eine Information der privaten Banken“ zusammen. Alle Publikationen, die sich an diese Zielgruppe richten, sind speziell auf die Bedürfnisse der Verbraucher zugeschnitten. So erhalten diese kostenfrei fundierte Informationen in leicht verständlicher Form.

Folgende Publikationen sind in der Reihe zuletzt erschienen:



Sicher mit Karte

10 Sicherheitstipps zur Bankkarte
Berlin, November 2007



Tätigkeit als Finanzagent

Finger weg von dubiosen Angeboten!
Berlin, Juli 2007



Ombudsmann der privaten Banken

Tätigkeitsbericht 2006
Berlin, Juli 2007



Das Girokonto

Informationen für Privatkunden
Berlin, April 2007



Private Altersvorsorge

Informationen für Privatkunden
Berlin, März 2007



Banken und Verbraucher

Das verbraucherpolitische Gesamtkonzept der privaten Banken
Berlin, November 2006



Kredit-Scoring

Bestandteil der modernen Kreditvergabe
Berlin, Oktober 2006

Alle Publikationen können unter www.bankenverband.de kostenfrei bestellt werden oder als pdf-Datei heruntergeladen werden.

Stand: November 2007.

ONLINE-BANKING-SICHERHEIT

Berlin, November 2007

HERAUSGEBER Bundesverband deutscher Banken
Postfach 040307, 10062 Berlin
Telefon (030) 1663-0
Telefax (030) 1663-1399

GESTALTUNG Manfred Makowski, Berlin

© BUNDESVERBAND DEUTSCHER BANKEN
Der Bankenverband ist die Interessenvertretung
der privaten Banken in Deutschland.

www.bankenverband.de

So erreichen Sie den Bankenverband:



Per Post:

Bundesverband deutscher Banken
Postfach 040307
10062 Berlin



Per Fax:

(030) 1663-1399



Per Telefon:

(030) 1663-0



Per E-Mail:

bankenverband@bdb.de



Im Internet:

www.bankenverband.de