

» Online-Betrügern keine Chance geben

» Sicheres Online-Banking bei Volksbanken und Raiffeisenbanken

Internet und Banking – mit Sicherheit ein gutes Gespann

Wo viele Menschen sind, sind Langfinger oft nicht weit. Das gilt auch im Internet. Die steigende Beliebtheit des World Wide Web lockt auch Betrüger an. Umso wichtiger ist es, die üblichen Tricks der Datendiebe zu kennen und bei der PC-Nutzung auf Sicherheit zu achten. VR aktuell erklärt, mit welchen Sicherheitsmaßnahmen Sie sich am besten schützen können.

Surfen mit Umsicht

Mehr als die Hälfte aller Deutschen nutzt das Internet, um sich Informationen zu beschaffen, in virtuellen Geschäften Waren und Dienstleistungen zu erwerben, ihre Bankgeschäfte online zu erledigen oder einfach nur so zum Spaß. Das umfangreiche Angebot des Internets zieht immer mehr Menschen an und so ist es nicht verwunderlich, dass auch Betrüger und Langfinger „den Braten riechen“ und schnell da sind, um ihr Glück zu versuchen und sich einen Teil davon zu holen. Beim Surfen im Internet und vor allem auch beim Shopping und bei Bankgeschäften ist daher Umsicht von wesentlicher Bedeutung. Es ist wichtig, dass sich die Nutzer mit Fragen der Sicherheit sowie den möglichen Risiken der PC-Nutzung und den Tricks von Datendieben und Betrügern auseinandersetzen, denn nur mit einem bewussten und richtigen Umgang lassen sich die Vorzüge des Internets unbeschwert genießen. Durch wenige einfache Verhaltensregeln lässt sich die moderne Technik kontrollieren und der Nutzer behält die Kontrolle über seinen PC. Wie fast überall im Leben gilt auch

hier: Wer gut informiert und vorbereitet ist, braucht keine Angst zu haben!

Ungebetene Besucher

Das Internet bietet eine Menge Vorteile, die Sicherheit bleibt aber ein entscheidender Faktor. Die unachtsame Nutzung des weltweiten Netzes öffnet nämlich schnell einmal eine Tür im PC für ungewollte Besucher. Neben den vielen nützlichen Programmen, die Ihnen das Leben und Arbeiten leichter machen, gibt es auch Programme, die in böswilliger Absicht geschrieben sind, um auf fremden PCs Störungen zu verursachen. Wenn diese einmal im Computer sind, können sie erheblichen Schaden anrichten. Diese unliebsamen Gäste heißen Viren, Würmer oder Trojanische Pferde. Viren verbreiten sich durch die Weitergabe von infizierten Dateien. Eine Ansteckungsgefahr besteht dort, wo Sie Dateien aus dem Internet oder von CDs auf Ihren Rechner laden. Würmer infizieren dagegen eigenständig über das Netzwerk oder per E-Mail weitere Computer. Manchmal hängen sie sich als Datei an eine E-Mail. Wenn Sie so eine Datei öff-



Ganz entspannt: Wer beim Surfen im Internet und beim Online-Banking einige Sicherheitsregeln einhält, kann sich beruhigt zurücklehnen.

nen, aktiviert sich der Wurm und verbreitet sich dann über weitere E-Mails selbst weiter. Trojanische Pferde sind scheinbar nützliche Programme, die ein schädliches Programm „im Bauch“ tragen. So kann sich dieses unbemerkt auf Ihrem PC installieren. Die Schädlinge können Ihre geheimsten Informationen ausspionieren, Ihre wichtigen Dokumente oder Photos unwiederbringlich löschen oder sogar den ganzen PC zerstören. Je besser Sie über diese Besucher Bescheid wissen, umso leichter können Sie etwas dagegen tun.

Fischen mit E-Mails

Betrüger gibt es nicht nur an der Haustür, sondern auch im Internet. Immer häufiger versuchen Gauner, mit Hilfe von E-Mails und gefälschten Web-Seiten Ihre geheimen Daten auszuspiionieren, um damit Missbrauch zu betreiben. Sie haben es vor allem auf Passwörter abgesehen. Auf verschlungenen Wegen schicken die Gauner an Millionen Nutzer E-Mails mit gefälschten Absendern, z. B. eines Kreditinstituts, in der Hoffnung, dass einer „anbeißt“. Diese E-Mails fordern Sie mit eindringlichen, überzeugend klingenden Worten auf, auf eine besondere Webseite zu gehen, um dort persönliche Angaben, wie Kontodaten, Passwörter und TANs einzugeben. Die Webseiten sind jedoch allesamt gefälscht und liegen meist auf „gehackten“ Rechnern. Die Geheiminformationen landen sofort bei den Betrügern, die mit den so ergaunerten Daten erheblichen Schaden anrichten können.

Vorsicht Schädlinge!

Aber auch wenn Sie keine Daten auf solchen Seiten eingeben, können bereits beim Anklicken dieser Webseiten automatisch Viren oder Würmer auf Ihren PC gelangen. Ein weiteres Ziel der Betrüger ist es nämlich, auf Ihrem PC Spionageprogramme zu installieren, um so später Ihre PIN und TANs abzuhören. Der Betrug läuft dann so ab: Während der Kunde das Online-Banking seiner Bank besucht, beobachtet das Spionageprogramm die Eingabe der PIN und TAN des Nutzers. Dann unterbricht es die Verbindung mit der Bank und sendet die „abgefischten“ Daten sofort an den Betrüger. Der kann sich dann mit den ausspionierten Daten Ihr Geld auf sein Konto überweisen. Die Banken können

den Versand solcher so genannten „Phishing-E-Mails“ nicht verhindern, sondern nur versuchen, die gefälschten Webseiten so schnell wie möglich zu beseitigen. Wenn Sie eine zweifelhafte E-Mail mit dem Namen Ihrer Bank erhalten, informieren Sie am besten Ihre Bank darüber.

Beachten Sie unbedingt:

Ihre Volksbank oder Raiffeisenbank wird Sie niemals in E-Mails nach Ihren persönlichen Informationen oder vertraulichen Daten fragen oder Sie zum Online-Banking auffordern. Wir empfehlen Ihnen, E-Mails mit solchen Inhalten sofort zu löschen. Darin enthaltene Adressen oder Knöpfe sollten niemals angeklickt werden!

Dubiose Angebote

Jeder freut sich, wenn er ein gutes Angebot bekommt. Wenn Ihnen aber Unbekannte per E-Mail hohe Gewinne ohne echte Gegenleistung versprechen, sollten Sie misstrauisch sein. In letzter Zeit bieten vermehrt ausländische Unternehmen lukrative Jobs als Finanzmakler an. Diese Jobs bestehen meist darin, hohe Summen entgegenzunehmen und ins Ausland zu überweisen. Diese Gelder können aus kriminellen Geschäften, wie dem oben beschriebenen Phishing, stammen. Die Überbringer machen sich dabei der Geldwäsche und des bandenmäßigen Betrugs schuldig. Sie sind schnell ermittelt und müssen die gestohlenen Summen dann aus eigener Tasche zurückerzahlen.

Online-Banking mit Sicherheit

Über 60 Prozent der Internetnutzer nutzen regelmäßig auch Online-Banking. Online-Banking bietet ein

hohes Maß an Flexibilität, Bequemlichkeit und spart Zeit. Dazu kommt der Kostenvorteil. Online-Banking von zu Hause aus ist durchweg preiswerter als der Service am Schalter. Deshalb sollten Sie auf die elektronischen Zahlungssysteme setzen. Das Online-Banking ist auf jeden Fall sicher, wenn Sie einige einfache Punkte beherzigen und den Umgang mit Ihrem PC beherrschen.



Browser oder Software

Für Ihre Online-Geschäfte bietet Ihnen Ihre Volksbank oder Raiffeisenbank zwei Möglichkeiten, die den höchsten Sicherheitsstandards entsprechen: Web-Banking (HTTPS) oder Finanzsoftware (HBCI). Zunächst benötigen Sie die Zugangsdaten Ihrer Bank. Mittels Ihrer PIN und Ihren persönlichen Transaktionsnummern (TAN), wird jede Online-Buchung eindeutig zugeordnet. Sie können auch mit der elektronischen Signatur jeden Auftrag persönlich unterschreiben. Bei einer Finanzsoftware, wie der VR-Networld-Software, richten Sie nach der Installation die Bank- und die Kontoverbindung ein. Die Software stellt die richtige Verbindung mit ihrer Bank her und die Verbindungsdaten werden für den weiteren Gebrauch verschlüsselt gespeichert. Oder Sie benutzen den Internetbrowser und rufen einfach die Banking-Webseite der Bank auf. Hierbei

ist wichtig, dass Sie darauf achten, dass der Browser nur das macht, was Sie von ihm verlangen. Setzen Sie z. B. die Sicherheitseinstellungen auf „hoch“. Sie sollten dabei keine so genannten „Surf-Beschleuniger“ oder Proxy-Server verwenden, denn diese können Ihre Verbindung mit der Bank unterbrechen und Ihre Kommunikation, einschließlich der geheimen PIN und TANs, mithören. Die Webseite Ihrer Bank hat zur Echtheitsbestätigung ein Zertifikat.

Online-Banking ist sicher, dafür sorgen wir. Sie müssen nur noch auf Ihren PC aufpassen!



TAN auf Knopfdruck

Die interessanteste Entwicklung beim Online-Banking ist Smart-TAN. Dies ist ein TAN-Generator im Chip Ihrer VR-BankCard. Sie brauchen dann keine umständlichen TAN-Listen mehr. Von Ihrer Bank erhalten Sie den handlichen Taschenleser, mit dem Sie überall und jederzeit eine neue TAN aus Ihrer VR-BankCard lesen können, wenn Sie eine brauchen. Und das Wichtigste: Sobald Sie eine neue TAN erzeugen und an die Bank schicken, werden automatisch alle vorherigen TAN ungültig, weil sie nummeriert sind. Auf diese Weise trägt Smart-TAN auch zu Ihrer Sicherheit bei.

Signatur mit Karte

Nutzen Sie Online-Banking bereits intensiv, bietet Ihnen das Online-

Banking mit elektronischer Signatur (HBCI) noch größeren Komfort. HBCI entspricht den höchsten Anforderungen und die Sicherheit wird von allen Fachleuten gelobt. HBCI schützt Ihre Transaktionen durch ein aufwändiges Verschlüsselungsverfahren vor dem Zugriff Dritter. Alle Transaktionen, die Sie durchführen, werden mit Ihrer elektronischen Signatur unterschrieben. Diese ist auf einer Chipkarte geschützt abgespeichert und kann nur mit Ihrem persönlichen Kennwort aktiviert werden. Anschließend werden die Aufträge wie ein E-Mail zur Bank übertragen. Dies sorgt für optimale Sicherheit. Da die Signaturkarte wie eine persönliche Unterschrift ist, verdient die PIN besonderen Schutz. Daher sollte immer ein sicherer Banking-Kartenleser mit Tastatur eingesetzt werden. Die PIN der Signaturkarte wird dann direkt am Kartenleser eingegeben. So ist sie gegen Abhören geschützt, da sie überhaupt nicht in den PC gelangt. Online-Banking mit Signaturkarte und Banking-Kartenleser ist so vollkommen geschützt gegen Phishing und kann vorbehaltlos für jeden empfohlen werden.



Sicherheits-Tipps

Vorbeugen ist wichtig

Wie auch immer Sie das Internet nutzen – einfach um sich zu informieren, um einzukaufen oder Ihre Geldgeschäfte abzuwickeln: Wer

sich nicht schützt, macht es Gaunern einfach, bei ihm einzubrechen und wichtige Dateien zu zerstören oder Geld zu stehlen. Einfache Grundregeln bei der Nutzung des Internets schaffen bereits ein hohes Maß an Sicherheit. So sollten die Sicherheitseinstellungen von Browser und E-Mail-Programm immer so hoch wie möglich eingestellt sein. Verwenden Sie Anti-Viren-Software auf Ihrem PC. Dies ist eine wirksame Möglichkeit, den Computer vor einem Befall zu schützen. Da täglich neue Viren hinzukommen, muss die Anti-Viren-Software regelmäßig aktualisiert werden. Installieren Sie zusätzlich ein Firewall-Programm, das den Rechner vor Angriffen schützt und verhindert, dass Spionageprogramme Kontakt über das Internet aufnehmen können.

Die fünf wichtigsten Regeln für einen sicheren Umgang mit dem Internet:

1. Überlegen Sie genau, wer Ihr Vertrauen verdient: Neue Programme aus dem Internet sind nicht immer vertrauenswürdig.
2. Setzen Sie Virens Scanner, Firewall und zusätzliche Sicherheitssoftware ein, die Sie regelmäßig aktualisieren.
3. Aktivieren Sie die Sicherheitseinstellungen Ihres Internet-Browsers. Nutzen Sie eventuell alternative, sicherere Browser.
4. Speichern Sie Zugangsdaten wie Passwörter, Kreditkartennummern und auch Ihre TANs niemals auf der Festplatte des PC ab. Andere sensible Daten sollten Sie verschlüsseln.
5. Machen Sie regelmäßig einen persönlichen Sicherheitscheck.

Schneller Sicherheitscheck

Auf den Internet-Seiten vieler Volksbanken und Raiffeisenbanken finden Sie eine einfach anzuwendende Hilfestellung: den kostenlosen Com-

puter-Sicherheitscheck. Wer sich als PC-Anfänger nicht ganz so gut mit dem Computer und mit den Computerbegriffen auskennt, liegt mit diesem Test genau richtig. Die PC-Prüfung startet per Mausklick. Das Prüfprogramm wird augenblicklich vom Computer innerhalb weniger Minuten durchlaufen und begibt sich automatisch auf die Suche nach Fehlern und Sicherheitslücken, die ein Eindringling für einen Angriff auf Ihren Computer nutzen könnte. Am Ende der Prüfung signalisiert Ihnen eine Ampel, ob Ihr PC „gesund“ ist. Blinkt die Ampel grün, ist alles o.k., blinkt sie hingegen rot, wurden Fehler oder Schwachstellen erkannt. In diesem Fall erhalten Sie automatisch einen Vorschlag zur Fehlerbehebung mit einer Schritt-für-Schritt-Anleitung und weitergehenden Sicherheitstipps. Ergänzt wird dieser Service für Sie durch umfangreiche Download-Möglichkeiten für Anti-



Viren-Programme, Firewall-Programme sowie spezielle Programme zur Entfernung unterschiedlichster aktueller PC-Würmer.

Grundregeln beim Online-Banking

- Vor dem Aufrufen des Online-Bankings ...
 - benutzen Sie keine fremden Rechner; diese können Sicherheitslücken haben,
 - schließen Sie alle Browserfenster, bevor Sie das Online-Banking starten,
 - geben Sie die Adresse Ihrer Bank möglichst von Hand in Ihren Browser ein.
- Im Online-Banking: ...
 - Das Symbol eines Vorhängeschlosses unten rechts im Browserfenster zeigt Ihnen die gesicherte Verbindung an.
 - Klicken Sie auf das Schloss und prüfen Sie die Echtheit der Seite anhand des Serverzertifikats.
 - Überprüfen Sie vor und nach der Nutzung Ihre Kontoumsätze: Sie sollten sofort allen neuen Transaktionen sehen können.

- Bei der Dateneingabe und -übertragung ...
 - vergewissern Sie sich, ob die geforderten Eingaben für die von Ihnen gewünschte Aktion sinnvoll sind,
 - melden Sie Abbrüche und andere Unregelmäßigkeiten während des Online-Bankings sofort Ihrer Bank.
- Im Verdachtsfall ...
 - verlassen Sie das Online-Banking sofort und befolgen Sie keinesfalls die angegebenen Anweisungen. Informieren Sie Ihre Bank und lassen Sie gegebenenfalls Ihren Online-Zugang sperren.
 - So sperren Sie Ihr Online-Banking notfalls selbst: Geben Sie dreimal eine falsche PIN ein.

Lassen Sie sich beraten

Weiterführende Informationen zum Thema Sicherheit erhalten Sie bei Ihrer Volksbank oder Raiffeisenbank bzw. auf deren Internetseiten sowie in den Sonderbedingungen zum Online-Banking. Übrigens – die Volksbanken Raiffeisenbanken bieten Ihnen mit **VR-Web** einen günstigen und prämierten Internet-Zugang!