

» So schützen Sie sich vor ungewollten Besuchern | Seite 1

» Grundregeln beim Onlinebanking | Seite 4

# Bankgeschäfte im Internet – so gehen Sie auf Nummer sicher

Maßnahmen und Tipps für sicheres Surfen und Onlinebanking

**Das Internet hat in den vergangenen Jahren eine rasante Entwicklung erlebt. Es macht viele Dinge des täglichen Lebens einfach und bequem. Auch Bankgeschäfte können Sie so von zu Hause aus erledigen. Allerdings wittern auch Betrüger ihre Chance. Die unachtsame Nutzung des weltweiten Netzes öffnet schnell eine Tür im PC für ungewollte Besucher. Mit einigen wenigen Verhaltensregeln behalten Sie jedoch die Kontrolle über Ihren Computer. Was Sie beachten sollten, können Sie hier nachlesen.**

Über 60 Prozent aller Deutschen nutzen das Internet, um sich Informationen zu beschaffen, in virtuellen Geschäften Güter und Dienstleistungen zu erwerben, ihre Bankgeschäfte online zu erledigen oder einfach nur so zum Spaß. Die Nutzung des umfangreichen Angebots im Internet wird für die Menschen immer selbstverständlicher. So ist es nicht verwunderlich, dass auch Betrüger und Langfinger sich im Netz tummeln. Vor allem beim Einkaufen und bei Bankgeschäften ist daher Aufmerksamkeit und vorausschauende Umsicht wichtig. Deswegen sollten Sie sich mit dem Thema Sicherheit sowie den möglichen Risiken der PC-Nutzung und den Tricks von Datendieben und Betrügern auseinandersetzen. Durch wenige einfache Verhaltensregeln können Sie die moderne Technik kontrollieren und behalten die Kontrolle über Ihren PC. Wie beim Überqueren einer Straße gilt nämlich auch im Internet: Wer gut informiert und vorbereitet ist, braucht keine Angst zu haben!

## Ungebetene Besucher

Neben den vielen nützlichen Angeboten im Internet, 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 erst einmal im Computer drin sind, können sie dort 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 öffnen, 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 unbe-

merkt auf Ihrem PC installieren. Die Schädlinge können Ihre geheimen Informationen ausspionieren, Ihre wichtigen Dokumente oder Fotos unwiederbringlich löschen oder sogar Ihren ganzen PC zerstören. Je besser Sie über diese Besucher Bescheid wissen, umso leichter können Sie etwas dagegen tun.

## Fischen mit E-Mails

Immer häufiger versuchen Gauner, mithilfe von E-Mails und gefälschten Webseiten Ihre geheimen Daten auszuspionieren, 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 Sie das Onlinebanking Ihrer Bank besuchen, beobachtet das Spionageprogramm die Eingabe der PIN und TAN. Dann unterbricht es die Verbindung mit der Bank und sendet die „abgefischten“ Daten sofort an den Betrüger. Der kann dann mit den ausspionierten Daten in Ihrem Namen schalten und walten und sich Ihr Geld auf sein Konto überweisen. Die Banken können den Versand solcher Phishing-E-Mails nicht verhindern, sondern nur versuchen, die gefälschten Webseiten so schnell wie möglich zu beseitigen.

Beachten Sie unbedingt: Ihre Volksbank oder Raiffeisenbank wird Sie niemals in E-Mails nach Ihren persönlichen Informationen oder vertraulichen Daten fragen oder Sie zum Onlinebanking 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 per E-Mail bekommt.

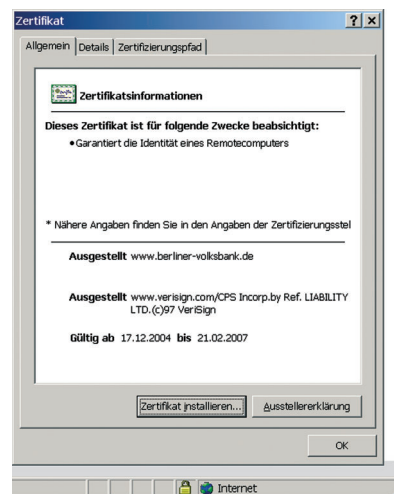
Wenn Ihnen Unbekannte hohe Gewinne ohne echte Gegenleistung versprechen, sollten Sie misstrauisch sein. In letzter Zeit bieten vermehrt ausländische Unternehmen lukrative Jobs als Finanzmakler an. Diese Jobs bestehen meist darin, hohe Summen entgegenzunehmen und ins Ausland zu überweisen. Diese Gelder können aus kriminellen Geschäften, wie auch dem oben beschriebenen Phishing, stammen. Jeder Überbringer macht sich bei der Weiterleitung der Geldwäsche und des bandenmäßigen Betrugs schuldig. Die Spuren können schnell ermittelt werden und die Helfer müssen die gestohlenen Summen dann aus eigener Tasche zurückzahlen.

### Onlinebanking mit Sicherheit

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

### Browser oder Software

Für Ihre Onlinegeschäfte bietet Ihnen Ihre Volksbank oder Raiffeisenbank zwei Zugangswege, die den höchsten Sicherheitsstandards entsprechen: über das Web-Banking oder über eine Finanzsoftware. Für diese Zugangswege werden Ihnen verschiedene Sicherheitsverfahren angeboten. In jedem Fall benötigen Sie die Zugangsdaten Ihrer Bank. Beim PIN-TAN-Verfahren wird mittels Ihrer PIN und Ihren persönlichen Transaktionsnummern (TANs) jede Onlinebuchung eindeutig zugeordnet. Mit



einer elektronischen Signatur wird jeder Auftrag persönlich unterschrieben. 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 sogenannten „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 (Bild).

**Onlinebanking ist sicher, dafür sorgen wir. Sie müssen nur noch auf Ihren PC aufpassen!**

### TAN auf Knopfdruck

Die interessanteste Entwicklung beim Onlinebanking ist Smart-TAN plus. Dies ist ein TAN-Generator im Chip Ihrer VR-BankCard. Sie brauchen damit 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. Das Besondere ist: Indem Sie wesentliche Daten der von Ihnen beabsichtigte Transaktion in den Leser eingeben, wird die TAN eindeutig für diese erzeugt und ist nicht für andere verwendbar. Wenn Sie keinen Kartenleser benutzen wollen und sowieso Ihr Mobiltelefon immer dabei haben, ist die mobileTAN das Richtige für Sie. Bei diesem Verfahren schickt Ihnen die Bank bei Bedarf eine SMS mit einer neuen TAN auf Ihr Handy. In der SMS stehen zur Kontrolle auch die wesentlichen Transaktionsdaten, sodass Sie sicher sein können, dass diese TAN nur für das beabsichtigte Geschäft gilt.

### Signatur mit Karte

Nutzen Sie Onlinebanking bereits intensiv, bietet Ihnen das Onlinebanking mit elektronischer Signatur und Finanzsoftware nach dem bewährten Financial Transaction Standard (FinTS) noch größeren Komfort. Bei einigen Banken können Sie die Signaturkarte auch schon im Webbanking benutzen. FinTS entspricht den höchsten Anforderungen und seine Sicherheit wird von allen Fachleuten gelobt. FinTS mit Chipkarte schützt Ihre Transaktionen durch ein aufwendiges Verschlüsselungsverfahren vor dem Zugriff Dritter. Alle Trans-

aktionen, die Sie durchführen, unterschreiben Sie mit Ihrer elektronischen Signatur. 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 zumindest ein Banking-Kartenleser mit eigener Tastatur eingesetzt werden. Wir empfehlen Ihnen jedoch die neuen Secoder®-Kartenleser, die von der Kreditwirtschaft speziell für das sichere Onlinebanking entworfen worden sind. Die PIN der Signaturkarte wird direkt am Kartenleser eingegeben. So ist sie gegen Abhören geschützt, da sie überhaupt nicht in den PC gelangt. Auf den Secoder®-Kartenlesern werden zusätzlich die wesentlichen Daten jeder Transaktion angezeigt, bevor Sie signieren. Onlinebanking mit Signaturkarte und Secoder®-Kartenleser ist vollkommen geschützt gegen Phishing und kann vorbehaltlos für jeden empfohlen werden

### Sicherheits-Tipps

#### Vorbeugen ist wichtig

Sie haben es in der Hand, wie Sie das Internet nutzen: Schützen Sie sich und machen Sie es den Gau-



nern schwer, bei Ihnen einzubrechen und dabei wichtige Dateien zu zerstören oder Geld zu stehlen. Indem Sie die folgenden einfachen Grundregeln bei der Nutzung des Internets beherzigen, schaffen Sie bereits ein hohes Maß an Sicherheit: Stellen Sie die Sicherheitseinstellungen von Browser und E-Mail-Programm immer so hoch wie möglich. Verwenden Sie Anti-Viren-Software auf Ihrem PC, um den Computer vor einem Befall zu schützen. Aktualisieren Sie die Anti-Viren-Software regelmäßig, da täglich neue Viren auftauchen. Installieren Sie zusätzlich ein Firewall-Programm, das den Rechner vor Eindringlingen schützt.

#### Schneller Sicherheitscheck

Auf den Internet-Seiten vieler Volksbanken und Raiffeisenbanken fin-

#### 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.

den Sie eine einfach anzuwendende Hilfestellung: unseren kostenlosen Computer-Sicherheitscheck. Die PC-Prüfung startet per Mausklick. Das Prüfprogramm wird vom Computer innerhalb weniger Minuten durchlaufen und begibt sich 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. Bei „Grün“ ist alles o.k., bei „Rot“ wurden Fehler oder Schwachstellen erkannt. In diesem Fall erhalten Sie einen Vorschlag zur Fehlerbehebung mit einer Schritt-für-Schritt-Anleitung und weitergehenden Sicherheitstipps. Diese PC-Prüfung kann andere Sicherheitsprodukte, wie Firewall und Antivirensoftware allerdings

nicht ersetzen, sondern nur ergänzen.

Weiterführende Informationen zum Thema Sicherheit finden Sie auf den Internetseiten Ihrer Volksbank oder Raiffeisenbank sowie in den Sonderbedingungen zum Onlinebanking.

Übrigens – die Volksbanken Raiffeisenbanken bieten Ihnen mit **VR-Web** einen günstigen und prämierten Internet-Zugang!

## Grundregeln beim Onlinebanking

### ■ Vor dem Aufrufen des Onlinebankings ...

- Benutzen Sie keine fremden Rechner; diese können Sicherheitslücken haben.
- Schließen Sie alle Browserfenster, bevor Sie das Onlinebanking starten.
- Geben Sie die Adresse Ihrer Bank möglichst von Hand in Ihren Browser ein.

### ■ Im Onlinebanking ...

- Das Schlossbild im Browserfenster zeigt Ihnen die gesicherte Verbindung an.
- Klicken Sie auf das Schloss und prüfen Sie die Echtheit

der Seite anhand des Zertifikats.

- Überprüfen Sie bei jeder Nutzung Ihre Kontoumsätze: Alle neuen Transaktionen sollten sofort sichtbar sein.

### ■ Bei der Dateneingabe und -übertragung ...

- Vergewissern Sie sich, ob die geforderten Eingaben für die gewünschte Aktion zutreffen.
- Melden Sie Abbrüche und andere Unregelmäßigkeiten während des Onlinebankings sofort Ihrer Bank.

- In den Smart-TAN-plus-Leser nur die Daten der eigenen Transaktion eingeben.
- Bei mobiler TAN die Daten in der SMS überprüfen.

### ■ Im Verdachtsfall ...

- Verlassen Sie das Onlinebanking sofort und informieren Sie Ihre Bank und lassen gegebenenfalls Ihren Onlinezugang sperren.
- So sperren Sie Ihr Onlinebanking selbst: Geben Sie dreimal eine falsche PIN beim Anmelden ein.