

Online-Banking



**Mehr Wissen über  
sicheres Online-Banking**

## Notwendige Sicherheitsvorkehrungen am PC

### ! Nur sichere Rechner verwenden

Nutzen Sie nur Rechner für das Online-Banking, die Sie als möglichst sicher einstufen können. Als unsicher müssen dabei schon Rechner gelten, die beispielsweise auch von Familienangehörigen genutzt werden und wo Sie keinen vollständigen Überblick über alle möglicherweise installierten Programme haben. So können Kinder unbemerkt einen „Trojaner“ installieren. Gleiches gilt für die Rechner im Büro.

Internet-Cafés sollten nach Möglichkeit gar nicht für Online-Banking genutzt werden, da hier eine nicht überschaubare Zahl von Personen Zugang zu den Rechnern hat und zusätzlich keine direkte Verbindung zu Ihrer Bank hergestellt wird. Vielmehr läuft die gesamte Datenübertragung vorher über einen Hauptrechner, den so genannten Router, im Internet-Café, wo theoretisch ein technisch versierter Mitarbeiter die Daten abfangen kann. Sowieso ist für den Gast keine Einschätzung über die Zuverlässigkeit der Datenverbindung möglich, auch wenn das Internet-Café einen seriösen Eindruck macht.

### ! Regelmäßig Windows aktualisieren

Neben dem Browser können Angreifer auch direkt über das Betriebssystem Windows auf Ihren Rechner gelangen, wenn eine Schwachstelle entdeckt wird. Beispielsweise hat sich kürzlich ein sogenannter „Wurm“ über eine Schwachstelle auf Rechnern verbreitet und sie für Dritte geöffnet. Um dies zu verhindern, ist es empfehlenswert, regelmäßig die neuesten Sicherheitsaktualisierungen, sogenannte Updates oder Patches, zu installieren. Bei Windows haben Sie hierbei die Möglichkeit, sich die Updates selbst von der Microsoft-Webseite herunterzuladen oder die Update-Funktion von Windows zu nutzen. Bei Letzterem klicken Sie einfach im Start-Menü auf den Punkt „Windows Update“ oder beim Internet Explorer unter „Extras“ auf

„Windows Update“. Die Internetseite von Microsoft analysiert anschließend Ihren PC und empfiehlt dann die Aktualisierungen, die auf Ihrem PC fehlen.

Alternativ können Sie gezielt Updates über die Sicherheits-Webseite von Microsoft herunterladen, wo Sie auch weitere Informationen zu sicherheitsrelevanten Themen finden. Der Link lautet: <http://www.microsoft.com/germany/mslsecurity/default.aspx>

### ! Funktastaturen sind risikoreich

Beachten Sie bitte, dass bei der Verwendung einer Funktastatur die eingegebenen Daten nicht abhörsicher sind. Vielfach reicht es schon aus, wenn im Umkreis von 5 Meter - auch durch Wände - ein Funk-Empfänger des gleichen Tastaturherstellers steht, um sämtliche eingegebenen Buchstaben abfangen zu können. Besonders in Mehrfamilienhäusern oder Büros sollte daher möglichst auf den Einsatz von Funktastaturen verzichtet werden, wenn Online-Banking genutzt wird.

### ! Sicherheitskopien anlegen

Um sicherzustellen, dass auch nach einem vollständigen Zusammenbruch des gesamten PCs, der z.B. durch eine Infektion mit einem Virus oder einen schweren Fehler im Windows verursacht werden kann, noch alle bisher gespeicherten Daten zur Verfügung stehen, sollten Sie regelmäßige Sicherheitskopien (Backups) Ihrer wichtigen Dateien vornehmen. So hält sich der mögliche Verlust von Informationen in Grenzen, wenn sämtliche Daten vernichtet werden. Ein möglicher Rhythmus ist beispielsweise ein Backup einmal pro Monat, wenn nur wenige Dateien von Ihnen erstellt werden, einmal wöchentlich bei intensiver Nutzung des PCs. Wenn Sie wiederbeschreibbare CDs verwenden, halten sich die Kosten hierfür im kleinen Rahmen, wohingegen Sie im Fall der Fälle eine Menge Ärger und Aufwand sparen.



## Großes Augenmerk für den Internet-Browser

### ! Den richtigen Browser auswählen

Bei der Auswahl eines Browsers für das Online-Banking sollten Sie darauf achten, dass dieser von einem zuverlässigen Anbieter stammt. Dies sind unter anderem der Internet Explorer von Microsoft, der Netscape Navigator von Netscape sowie Mozilla, wobei letzterer relativ neu ist. Die Auswahl eines Browsers von einem bekannten Unternehmen stellt sicher, dass der Browser vertrauenswürdig ist und Sicherheitslücken regelmäßig durch entsprechende Updates beseitigt werden.

Beachten Sie dabei aber, dass grundsätzlich keine Beta-Versionen, also Testversionen, verwendet werden sollten, welche die Hersteller auf Ihren Webseiten zum Download anbieten. Diese sind eindeutig als Beta-Versionen gekennzeichnet und weisen unter Umständen noch nicht bekannte Sicherheitslücken auf, so dass sie für sicheres Online-Banking evtl. nicht geeignet sind.

### ! Regelmäßig den Browser aktualisieren

Versuchen Sie, möglichst immer die aktuellste Version Ihres Browsers zu nutzen. So ist sicherge-

stellt, dass alle bis zu diesem Zeitpunkt bekannten Sicherheitslücken, über die Dritte auf Ihren PC zugreifen können, geschlossen sind. Entsprechende Programmaktualisierungen, auch Patches oder Updates genannt, erhalten Sie direkt bei Microsoft für den Internet Explorer oder bei Netscape für den Netscape Navigator. Die entsprechenden Links lauten:

**Internet Explorer:** <http://www.microsoft.com/germany/ms/security/default.mspx>

**Netscape Navigator:** <http://wp.netscape.com/security/notes/index.html> (nur englisch)

### ! Vorsicht bei der Nutzung zusätzlicher Komponenten im Browser

Überlegen Sie sich, ob sie zusätzliche Komponenten, sogenannte Plug-ins, für Ihren Browser nutzen wollen. Diese werden von einigen Webseiten gefordert, um alle Inhalte darstellen zu können (z.B. Flash, Erweiterungen für die Suche nach Telefonnummern, Adressen, Onlineshops etc.). Sie bilden, sofern sie von seriösen Anbietern stammen, kein stark erhöhtes Risiko, aber können gleichzeitig eine Quelle für zusätzliche Schwachstellen sein, über die auf Ihren PC und Ihre Daten zugegriffen werden kann. Daher sollten, wenn überhaupt, nur die wirklich benötigten Erweiterungen installiert werden. Weitgehend vertrauenswürdig sind Plug-ins von großen Unternehmen wie beispielsweise Flash von Macromedia oder Quicktime von Apple, bei denen sichergestellt ist, dass der Anbieter um eine maximale Sicherheit seiner Produkte bemüht ist.

Werden Sie auf einer Webseite dazu aufgefordert, ein Plug-in zu installieren, sollten Sie dies nur dann zulassen, wenn Sie mit absoluter Sicherheit wissen, dass die Seite und die Software, die installiert werden soll, vertrauenswürdig sind. Bestehen Zweifel, brechen Sie den Vorgang direkt ab und versuchen Sie, weitere Informationen über die zu installierende Software zu erlangen. Meist reicht es, den Namen als Suchbegriff in einer Suchmaschine wie Google einzugeben und auf den ersten Treffern

weitere Details zu erfahren. Sind tendenziell un-seriöse Seiten unter den Suchergebnissen, sollte grundsätzlich von der Installation Abstand genommen werden.

### ! Kritische Funktionen des Browsers deaktivieren

Deaktivieren Sie kritische Funktionen des Browsers wie beispielsweise ActiveX. Beim Aufruf einer Website können hiermit Programme auf Ihren Rechner geladen und installiert werden, die unter Umständen unerwünschte Funktionen wie beispielsweise die Suche nach Passwörter ausführen. Deaktivieren lässt sich ActiveX folgendermaßen

**Internet Explorer:** Extras ➔ Internetoptionen ➔ Sicherheit ➔ Internet (Stufe anpassen) ➔ Alle Punkte mit ActiveX auf „deaktivieren“ stellen.

**Netscape Navigator:** Start ➔ Systemsteuerung ➔ Internetoptionen ➔ Sicherheit ➔ Internet (Stufe anpassen) ➔ Alle Punkte mit ActiveX auf „deaktivieren“ stellen.

Sollte es doch einmal erforderlich sein, ActiveX zu nutzen, weil sonst eine gewünschte Funktion auf einer Webseite nicht funktioniert, kann ActiveX für diese Seite kurzfristig wieder aktiviert werden, wobei im Anschluss auf jeden Fall wieder eine Deaktivierung erfolgen sollte.

## Schutz vor Viren, Würmern und Trojanern

### ! Gegen fremde Eindringlinge schützen

Grundsätzlich sollte auf jedem PC ein Schutz gegen Viren und Trojaner installiert sein. eMails sind das Haupteinfallstor für Viren und Trojaner, die Daten auf dem Rechner löschen, diesen für Angreifer von außen öffnen oder persönliche Daten ausspionieren können. Im schlimmsten Fall kann entweder ein Totalverlust aller Daten auftreten oder ein Dritter erhält die volle Kontrolle über den eigenen

Rechner. Zuverlässigen Schutz bieten Antivirus-Programme, die alle eMails prüfen und auch einen bereits bestehenden Befall des Computers feststellen können.

**Wichtig:** *Verwenden Sie nur Programme, die von der Fachpresse oder auf Internetseiten wie [www.heise.de](http://www.heise.de) oder [www.chip.de](http://www.chip.de) etc. als seriös bewertet oder empfohlen werden. Sonst kann es leicht passieren, dass Sie ein Programm auf Ihren PC laden, das letztendlich schlimmer als die Viren ist, vor denen es Sie eigentlich schützen sollte.*

Die regelmäßige Aktualisierung der Virens Scanner ist hierbei Pflicht. Möglichst täglich sollten Sie die Aktualisierungsfunktion des Programms nutzen oder eine automatische Aktualisierung einstellen, um zuverlässig gegen neue Viren geschützt zu sein. Denn die Virenschutz-Programme erkennen nur genau die Viren und Trojaner, über die sie vorher durch Aktualisierungen Informationen erhalten haben. Auch ein nur wenige Tage alter Schutz kann somit unter Umständen nicht mehr ausreichen, wenn sich eine neue Variante eines Virus schlagartig im Internet verbreitet. Neben der automatischen Überprüfung der eMails sollte zusätzlich noch eine regelmäßige Überprüfung der Festplatte erfolgen, um evtl. „durchgerutschte“ Viren entdecken zu können.

### ! Gefahren aus dem Internet vermeiden

Um sicherzugehen, dass kein Dritter aus dem Internet auf Ihren Rechner zugreifen kann und auch keine Programme über das Internet gegen Ihren Willen installiert werden, empfiehlt sich der Einsatz einer Firewall. Diese Programme filtern sämtliche übertragene Daten nach Absender und Inhalt und blockieren beispielsweise direkt Kontaktversuche unbekannter Rechner, wenn diese über vom Programm als gefährlich eingestufte Wege mit Ihrem PC Kontakt aufnehmen wollen. Zusätzlich kontrollieren sie auch die ausgehenden Daten, so dass Programme wie Keylogger, die sämtliche Tastatureingaben auf Rechnern aufzeichnen versenden, blockiert werden. Eine Firewall schützt auch vor den in letzter Zeit immer häufiger



auftretenden Wurmern, die sich über das Internet selbst und nicht über eMails verbreiten.

Die handelsüblichen Firewalls warnen Sie, wenn ein Rechner aus dem Internet auf Ihren PC zugreifen möchte oder wenn ein Programm eine Verbindung ins Internet aufbaut. Hier gilt: Blockieren Sie grundsätzlich die Verbindung, wenn Sie nicht zu 100 Prozent wissen, wer der fremde Rechner oder das Programm auf Ihrer Festplatte ist. Sollte eine gewünschte Funktion (z.B. die Aktualisierung eines Programms) dann nicht ausführbar sein, können Sie weitgehend sicher sein, dass dies die Ursache für den unbekanntem Verbindungsaufbau war und diesen bei der nächsten Warnung zulassen. So stellen Sie sicher, dass keine unkontrollierten Verbindungen von Ihrem PC aus aufgebaut werden können.

## Vorsichtiger Umgang mit den Geheimzahlen

### ! PIN und TAN geschützt aufbewahren

Stellen Sie sicher, dass Dritte nicht in den Besitz Ihrer PIN und TAN gelangen. Dies schließt auch ein, dass Ihre Zugangsdaten für das Online-Banking nicht auf Zetteln am Schreibtisch notiert oder in einer Mappe mit der Aufschrift „Online-Banking“ aufbewahrt werden sollten. Optimal ist es, wenn das Passwort in für Dritte nicht erkennbarer Form aufbewahrt wird, sofern es nicht unerreichbar (z.B. im Bankschließfach etc.) aufbewahrt wird.

Grundsätzlich gilt: Bewahren Sie PIN und TAN-Liste immer getrennt voneinander auf, damit selbst in dem Falle, wenn eines von beiden in die Hände eines Dritten fällt, keinerlei Nutzen hieraus entsteht.

### ! Speicherung von Passwörtern

Passwörter sowie die PIN oder die TAN-Liste sollten nach Möglichkeit nicht auf dem Rechner gespeichert werden. Auf keinen Fall darf beispielsweise ein unverschlüsseltes Word- oder Text-Dokument mit dem Namen „Online-Banking“ oder „Passwörter“ erstellt werden. Falls ein Angreifer Zugriff auf Ihren Rechner erhält (z.B. über einen Virus oder Trojaner), kann er diese Dateien zu leicht öffnen und die geheimen Daten lesen.

### ! Absolut sichere Passwörter nutzen

Passwörter sollten, sofern dies Ihr Kreditinstitut zulässt, aus einer willkürlichen Kombination aus Buchstaben und Zahlen sowie evtl. Sonderzeichen wie „\$“ oder „&“ bestehen. Geburtstage sowie Namen von Verwandten oder Haustieren sind zu leicht zu erraten. Eine Hilfestellung kann es beispielsweise sein, einen beliebigen Satz in ein Passwort umzuwandeln. Z.B. „Meine Schwester wurde 1980 in Berlin-Mitte geboren“ als „MSw1980iBMg“. Diese Kombination ist fast unmöglich zu erraten und gleichzeitig durch einen Merksatz leichter zu behalten. Sind nur Zahlen zulässig, sollte die Anzahl von möglichen Zahlen (z.B. 12) weitestgehend ausgeschöpft werden, um das Risiko eines ungewollten Treffers durch Dritte zu minimieren.

**Wichtig:** Verwenden Sie nach Möglichkeit für verschiedene Konten, den Internetzugang etc. verschiedene Passwörter. So steht nicht direkt alles offen, wenn einmal das Passwort in unbefugte Hände gerät.

### ! Die Passwörter regelmäßig ändern

Ändern Sie Ihr Passwort in regelmäßigen Abständen (1-2 Monate) oder falls Sie den Verdacht

haben, irgendjemand könnte in den Besitz des aktuellen Passworts gelangt sein. Sollten Sie wie die meisten Leute Schwierigkeiten mit dem Merken von Passwörtern haben, greifen sie z.B. auf die unter „Sichere Passwörter“ beschriebene Methode der Passwörter aus Merksätzen zurück.

### **! Sichere Eingabe von Passwort, PIN und TAN**

Stellen Sie grundsätzlich sicher, dass Sie niemand bei der Eingabe von Passwörtern oder der PIN sowie TAN beobachten kann. Dies gilt besonders dann, wenn Sie im Büro oder aus einem Internet-Café Ihre Online-Bankgeschäfte tätigen. Eine weitere Gefahr können kleine Programme aus dem Internet, sogenannte Keylogger, darstellen, die sämtliche Eingaben auf Ihrer Tastatur protokollieren und von Zeit zu Zeit an einen Empfänger versenden. Hierin sind dann alle Eingaben, die sie beispielsweise während einer Online-Banking-Sitzung vorgenommen haben, im Klartext gespeichert.

Zum Schutz vor derartigen Programmen setzen Sie am besten ein Virenschutz-Programm, sogenannte Virenschanner, und eine Firewall ein, die die ungewollte Installation solcher Programme wie Keyloggern verhindern.

## **Sichere Benutzung des Online-Banking-Programms**

### **! Regelmäßige Überprüfung der Kontobewegungen**

Um sicherzustellen, dass ein nicht berechtigter Zugriff auf Ihre Konten zeitnah auffällt, empfiehlt es sich, regelmäßig im Abstand von ein bis zwei Tagen die Kontobewegungen online zu überprüfen. Sollten Sie hierbei auf Ungereimtheiten stoßen, ist es ratsam, den Zugriff auf das Online-Konto bei Ihrer Bank direkt zu sperren. Die meisten Banken bieten hierfür eine eigene Funktion im Rahmen des Internet-Banking sowie Notfall-Telefonnummern an, aber es kann im Zweifelsfall (sollten Sie



bei Ihrer Bank niemanden erreichen und sich über die Vorgehensweise nicht sicher sein) das Konto ganz einfach über die dreimalige Eingabe einer falschen PIN gesperrt werden. Ein neues Passwort erhalten Sie dann persönlich von Ihrem Geldinstitut.

### **! Automatische Speicherung von Passwörtern im Internet-Browser**

Die gängigen Internet-Browser wie der Internet Explorer, Netscape oder Mozilla bieten dem Anwender die Möglichkeit, Benutzernamen und Passwörter zu speichern. Dies ermöglicht beim erneuten Besuch einer Website ein automatisches oder komfortableres Einloggen. Da diese Funktion aber von jedem, der den Rechner benutzt und die entsprechende Seite der Bank aufruft, automatisch genutzt wird, sollten die Passwörter für Online-Banking-Seiten grundsätzlich nicht gespeichert werden. Zusätzlich bietet dies auch bei Angriffen über das Internet eine weitere Quelle für die Ausspionierung von Zugangsdaten, da die Daten unter Umständen nur mit schwachem Schutz auf der Festplatte gespeichert werden.

### **! Vorschriftsmäßiges Abmelden erhöht die Sicherheit**

Verwenden Sie, sofern dies möglich ist, beim Verlassen der Online-Banking-Webseite immer die Logout- bzw. Abmelden-Funktion. Dies stellt sicher, dass sämtliche Informationen über Ihren Besuch gelöscht werden. Ansonsten kann es je nach Browser und Webseite vorkommen, dass bei einem einfachen Klick auf den Zurück-Button im Browser der



Inhalt der vorherigen Seiten wie Kontodaten, Umsätze etc. wieder angezeigt wird.

### **! Auf sichere Verbindungen achten**

Um eine maximal sichere Übertragung aller Informationen für das Online-Banking zu garantieren, nutzen die Banken mittlerweile flächendeckend den 128bit-SSL-Standard.

Hierbei werden alle zwischen Ihrem Rechner und der Bank übertragenen Daten so verschlüsselt, dass Dritte die Daten nicht mehr lesen oder manipulieren können. Sie können leicht erkennen, ob die Verbindung zur Webseite Ihrer Bank beim Online-Banking mit 128bit verschlüsselt ist. Zu erkennen ist dies daran, dass die Internetadresse im Browser mit „https://“ beginnt und an dem Schloss-Symbol am unteren rechten Rand des Browsers.

Sollte das Schloss-Symbol zu Beginn einer Online-Banking-Sitzung, wenn Sie beispielsweise Kontonummer und PIN eingeben müssen, nicht erscheinen oder geöffnet sein, ist keine sichere Verbindung aufgebaut. Brechen Sie hierbei bitte sofort den Vorgang ab. Sollte trotz mehrmaliger Versuche keine gesicherte Verbindung zustande kommen, setzen Sie sich möglichst umgehend mit der Bank in Verbindung, um herauszufinden, ob ein Problem seitens der Bank vorliegt oder Sie möglicherweise auf eine falsche Seite weitergeleitet wurden.

Beim Internet Explorer wird unten im Browser-Fenster in der rechten Hälfte ein kleines gelbes Schloss angezeigt, wenn die Verbindung sicher ist. Wenn Sie mit dem Mauszeiger über das Schloss-Symbol fahren, wird ein Text-Fenster angezeigt, in dem bei gesicherter Verbindung folgender Text angezeigt wird: „SSL Secured (128 Bit)“.

Beim Netscape Navigator wird generell ein Schloss am unteren Bildrand angezeigt. Dieses ist bei nicht gesicherten Verbindungen geöffnet und bei einer 128bit-Verbindung geschlossen.

### **! Schutz vor Phishing durch Zertifikatprüfung von Webseiten**

In letzter Zeit spielt das Phishing eine immer größere Rolle. Hierbei werden entweder eMails mit der Aufforderung verschickt, Passwörter etc. zwecks Sicherheitsüberprüfung zuzuschicken oder Internetnutzer werden auf Webseiten gelockt, die nur scheinbar die Webseite der eigenen Bank sind, um PIN etc. herauszufinden. Da es nur einen geringen Aufwand erfordert, Tausende eMails zu verschicken und der Ertrag sehr hoch sein kann, verbreitet sich dieses Phänomen immer stärker im Internet. Schützen kann man sich hiergegen, indem grundsätzlich keinerlei Informationen über persönliche Passwörter, PIN, TAN etc. Dritten mitgeteilt werden. Banken oder Ihr Internetanbieter fragen nie nach diesen Daten und auch andere seriöse Einrichtungen und Unternehmen verfahren ebenso.

Um zu garantieren, dass man sich tatsächlich auf einer Webseite der eigenen Bank befindet, kann das Zertifikat der Internet-Seite überprüft werden. Doppelklicken Sie hierfür einfach auf das Schloss-Symbol im Browser (am unteren Bildrand). Im darauf folgenden Fenster finden Sie verschiedene Informationen darüber, auf welche Internetadresse das Zertifikat ausgestellt ist, ob es noch gültig ist und wer es herausgegeben hat. Die im Zertifikat angegebene Adresse muss mit der im Browser angezeigten übereinstimmen. Sobald eine Abweichung vorliegt, sollte der Vorgang sofort abgebrochen werden. Benachrichtigen Sie auch Ihre Bank, damit diese dem Problem nachgehen kann.

**Wichtig:** Vielfach verwenden Banken beim Online-Banking Variationen der eigentlichen Internetadresse. Beispielsweise <https://banking02.meinebank.de>. Um sicherzugehen, dass die angezeigte und zertifizierte Adresse auch wirklich zu Ihrer Bank gehört, erfragen Sie bei dieser bitte im voraus die möglichen Adressen, die angezeigt werden können. So können Sie auch bei sonderbaren Internetadressen sicher sein, nicht auf eine betrügerische Seite geraten zu sein.

## Besondere Gefahren beim mobilen Online-Banking

### ! Online-Banking unterwegs vom Laptop

Sollten Sie Online-Banking mobil über einen Laptop erledigen wollen, muss darauf geachtet werden, über welchen Zugang in das Internet eingewählt wird. In vielen öffentlichen Gebäuden gibt es mittlerweile Zugangspunkte ins Internet, so genannte Hotspots, über die Sie sich drahtlos in das Internet einwählen können. Erforderlich ist hierfür nur eine Erweiterungskarte für den Laptop, die auf ein WLAN (Wireless Local Area Network = Schnurloses lokales Netzwerk) zugreifen kann.



Dieser Komfort bietet allerdings das Risiko, dass Sie vielfach nicht mit Sicherheit bestimmen können, wer genau den Internetzugang anbietet. Beispielsweise ist es möglich, dass Sie über ein schlecht gesichertes Funknetzwerk aus einer naheliegenden Privatwohnung einen Internetzugang erhalten. Die Nutzung eines solchen Hotspots bedeutet, dass alle Daten von Ihrem Rechner über einen Zentralrechner, einen sogenannten Router, laufen, der den schnurlosen Internetzugang anbietet. Hierbei können unter Umständen wie beim Internet-Café die Daten herausgefiltert werden, die Sie an Ihre Bank versenden.

Nutzen Sie beim mobilen Banking von unterwegs daher ausschließlich solche Internetzugänge, bei denen Sie sich über die Vertrauenswürdigkeit des

Anbieters hundertprozentig sicher sein können. Beispielsweise bieten Telekommunikationsprovider mittlerweile Internetzugänge in Form von Hotspots an, bei denen eine vergleichsweise hohe Sicherheit zu erwarten ist. Diese liegt jedoch immer unterhalb der Sicherheit Ihres Heim-PCs, da auch der reine Funkverkehr zwischen Ihrem Rechner und dem Hotspot mit relativ einfachen technischen Mitteln abgefangen werden kann.

### ! Gefährliches Online-Banking im Internet-Café

Nach Möglichkeit sollte es vermieden werden, seine Online-Banking-Geschäfte in Internet-Cafés abzuwickeln. Hier verfügen Sie im Regelfall über keinerlei Informationen, welche Programme auf dem Rechner installiert sind, über welche Wege eine Verbindung zu Ihrer Bank hergestellt wird und wer den Rechner vor und nach Ihnen benutzt. So läuft beispielsweise die gesamte Datenübertragung bei Internet-Cafés über einen Zentralrechner (Router), wo die übertragenen Informationen mit entsprechenden Hilfsmitteln unter Umständen herausgefiltert werden können. Es besteht also KEINE direkte Verbindung zu Ihrer Bank.

Ein weiteres Risiko stellt die Tatsache dar, dass jeder die Rechner nutzen und daher auch, trotz aller Sicherheitsvorkehrungen der Betreiber eines Internet-Cafés, je nachdem bösartige Programme wie beispielsweise Keylogger installieren kann, die den gesamten eingegebenen Text aufzeichnen und an denjenigen versenden, der das Programm installiert hat. Ihm steht dann im ungünstigsten Fall z.B. Ihre PIN im Klartext zur Verfügung.

Lässt es sich nicht vermeiden, dass Sie einmal aus einem Internet-Café Überweisungen vornehmen müssen, sollten Sie auf jeden Fall ein seriös wirkendes Café und nicht irgendeinen Telefonladen um die Ecke aussuchen. Im Anschluss an Ihre Überweisung ist auch unbedingt der Zwischenspeicher (Cache) des Browsers zu löschen, damit nach Ihnen niemand erkennen kann, auf welchen Seiten Sie sich aufgehalten haben.



FIDUCIA IT AG

Fiduciastraße 20  
76227 Karlsruhe  
Telefon (07 21) 40 04 - 43 21

[info@fiducia.de](mailto:info@fiducia.de)  
[www.fiducia.de](http://www.fiducia.de)