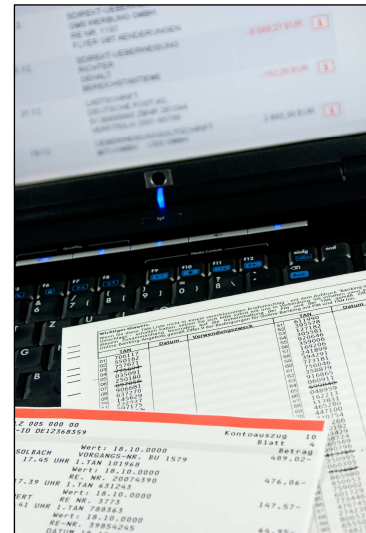


## Online-Banking – aber sicher!

**Ob Unternehmer oder Privatanwender, das Online-Banking ist heute für viele nicht mehr wegzudenken. Die Vorteile liegen auf der Hand. Unabhängigkeit und Flexibilität – Überweisungen egal wann und wo! So können Berufstätige Ihre Bankgeschäfte bequem nach dem Feierabend ohne Wartezeiten erledigen – völlig unabhängig von den Öffnungszeiten einer Bank. Dabei ersparen Sie sich zudem Kosten für herkömmliche Überweisungen und Daueraufträge.**



Aktuelle Transaktionsverfahren wie mTAN oder smartTAN gelten heutzutage beim Online-Banking als technisch absolut sicher. Dennoch müssen auch einige Regeln beachtet werden, damit der Anwender auf Betrüger und Internetdiebe nicht herein fällt. Um erst gar nicht in solche Situationen zu gelangen, müssen folgende Tipps für ein sicheres Online-Banking beachtet werden.

► **Achtung Phishing: Prüfen Sie stets kritisch E-Mails Ihrer Bank!**

Beim so genannten Phishing versuchen Kriminelle über abgefangene TANs und der zugehörigen PIN sich Zugang zu fremden Konten zu verschaffen. Dazu sendet der Angreifer dem Opfer eine E-Mail im Namen der Bank und täuscht somit einen vertrauenswürdigen Absender vor. Häufig wird in diesen Fällen eine Technische Wartung des Online-Banking-Portals oder die Verbesserung der Sicherheit als Grund genannt. Das Opfer wird dazu verleitet schnell zu reagieren. Klickt es auf den in der E-Mail aufgeführten Link, um die Änderungen vorzunehmen, wird es auf die angebliche Webseite der Bank geleitet und dort aufgefordert, sich mit seiner PIN und ein oder mehreren TANs anzumelden. Hinter diesem Link verbirgt sich jedoch nicht der Online-Auftritt der Bank, sondern oft eine nahezu perfekt nach gebaute Internetpräsenz. Werden PIN und TAN auf dieser Seite eingegeben, gelangen diese Informationen unmittelbar in die Hände des Angreifers und ermöglichen ihm über das Online-Banking des Opfers das gesamte Guthaben auf ein Konto seiner Wahl zu transferieren.

Ihre Bank wird Sie niemals via E-Mail dazu auffordern Ihre PIN und TAN einzugeben. Reagieren Sie nicht auf solche Aufforderungen. Beachten Sie den Kontext und auch die richtige Schreibweise. Oft ist dabei schon absehbar, ob ein Angreifer Sie auf eine präparierte Seite leiten möchte, um dort Ihre PIN und TANs abzufragen. Häufig verbergen sich auf der scheinbar echten Seite der Bank auch Schadprogramme. Diese können sich bei fehlenden Sicherheitsupdates oder bei fehlendem und nicht aktuellem Antivirenschutzprogramm ungehindert auf Ihrem Rechner installieren. Schadprogramme wie Trojaner können dann unbemerkt die Eingaben von PIN und TANs mitlesen und diese an den Angreifer versenden. Geben Sie daher die Internetadresse Ihrer Bank stets manuell in die Adresszeile Ihres Browsers ein und klicken Sie nicht in E-Mails auf vorgegebene Links. Außerdem empfiehlt es sich ein Tageslimit zu definieren, welches nur schriftlich und nicht online geändert werden kann. Sollten TAN und PIN doch in die Hände eines Angreifers gelangen, kann im Schadensfall nur eine bestimmte Summe und nicht das gesamte Kontovermögen gestohlen werden.

► **Tätigen Sie Ihre Bankgeschäfte ausschließlich verschlüsselt!**

Achten Sie darauf, dass bei Bankgeschäften und beim Austausch sensibler Daten stets eine verschlüsselte Verbindung zur Verfügung steht! Sie können Ihre Verbindung dahingehend prüfen, in dem Sie die Adresszeile Ihres Browsers bereits vor dem Eingeben Ihrer Zugangsdaten wie zum Beispiel Kontonummer und PIN betrachten. Bei einer verschlüsselten Verbindung beginnt diese stets mit „https“ statt wie üblich mit „http“. Zudem repräsentiert ein kleines Schlosssymbol in der Statusleiste Ihres Browsers eine verschlüsselte Verbindung. Damit Ihre Daten sicher übertragen werden, benötigt der Betreiber ein Zertifikat von einer vertrauenswürdigen Instanz. Um das Zertifikat Ihrer Bank zu prüfen, klicken Sie vor dem Login zum Online-Banking einfach auf das Schlosssymbol in der Statusleiste Ihres Browsers. Daraufhin werde Ihnen alle Informationen zum Zertifikat angezeigt. Prüfen Sie den Namen Ihrer Bank im Zertifikat auf die richtige Schreibweise und schauen Sie dabei auch, ob das Zertifikat noch nicht abgelaufen ist. Stimmt bei der Betrachtung des Zertifikats der Name mit dem Namen der Bank nicht überein oder ist das Zertifikat abgelaufen, loggen Sie sich nicht ein und informieren umgehend Ihre Bank!

► **Verwenden Sie starke Passwörter!**

Passwörter werden nach Ihrer Stärke gemessen. Je länger ein Passwort ist und umso mehr verschiedene Zeichen es enthält, umso stärker der Schutz. Dabei ist jedoch zu beachten, dass Passwörter sinnfrei zusammengesetzt werden sollten und nicht wie häufig, aus dem Namen oder Geburtsdatum des Partners bestehen. Verwenden Sie zum Schutz sensibler Daten stets ein starkes Passwort.

Sofern Sie eine Software für das Online-Banking benutzen, sichern Sie diese mit einem starken Passwort ab. Auch Ihre PIN für das Online-Banking sollten Sie dahingehend ändern! Passwörter sollten aus mindestens zehn Zeichen und Ziffern bestehen, Sonderzeichen, sowie Groß- und Kleinschreibung enthalten und nicht aus existierenden Wörtern zusammengesetzt sein. Werden diese Kriterien beachtet, spricht man von einem starken Passwort! Ein Beispiel für ein starkes Passwort ist „Aj1.u3.SiMsiF!“. Um sich ein starkes Passwort zu merken, prägen Sie sich im Vorfeld einen Satz gut ein. Mit Hilfe dessen können Sie jederzeit Ihr Passwort generieren. Zum Beispiel: „An jedem 1. und 3. Samstag im Monat spiele ich Fußball!“. Für das Passwort verwenden Sie nun einfach die Interpunktionszeichen sowie Anfangszeichen eines jeden Wortes. Daraus ergibt sich: „Aj1.u3.SiMsiF!“. Geben Sie Ihr Passwort oder Ihren dazugehörigen Merksatz niemals Dritten preis! Antworten Sie niemals auf scheinbare Anfragen Ihrer Bank nach Ihrem Passwort. Immer wieder tauchen Datenskandale auf, in denen bekannt wird, dass Tausende von Benutzerdaten gestohlen worden und nun im Umlauf sind. Verwenden Sie deshalb nie ein Passwort doppelt. Andernfalls laufen Sie Gefahr, dass von Ihnen gestohlene Benutzerdaten einer Internetplattform für weitere Dienste wie das von Ihnen genutzte Online-Banking verwendet werden können.

► **Behandeln Sie Ihre Zugangsdaten vertraulich!**

Häufig gehen Anwender des Online-Bankings mit Ihren Zugangsdaten zu unvorsichtig um und laufen Gefahr das Kriminelle diese stehlen und so an den Besitz Ihres Kontovermögens gelangen. So ist es nicht selten, dass PIN und TAN-Liste am gleichen Ort aufbewahrt werden. Sie liegen oft unbeaufsichtigt in der Schreibtischschublade oder begleiten den Anwender sogar tagtäglich in der Handtasche. Vermeiden Sie für Ihre Zugangsdaten Aufbewahrungsorte die für Dritte schnell einsehbar sind. Ein Gang auf die Toilette reicht einem Angreifer dabei meistens schon aus, um sich PIN und TANs zu kopieren. Speichern Sie Ihre Zugangsdaten nur verschlüsselt und mit einem starken Passwort auf der Festplatte ab! Verwahren Sie Ihre Zugangsdaten und Transaktionsnummern an einem sicheren Ort auf, sodass Dritte diese nicht finden und einsehen können. Hinterlegen Sie TANs und PIN nicht am selben Ort!

Bei einem fremden Rechner haben Sie keine Kontrolle, welche Programme im Hintergrund laufen. So genannte Keylogger ermöglichen es einem Angreifer im Nachhinein festzustellen, welche Eingaben Sie gemacht haben. Wenn Ihre Überweisung plötzlich, unabhängig von der Stromversorgung und Internetverbindung, unterbrochen wurde oder währenddessen ein Fehler angezeigt wird, versuchen Sie Ihre PIN im Online-Banking-Portal umgehend zu ändern und informieren Sie ihre Bank über den Vorfall, sodass ihr Konto vorübergehend gesperrt werden kann. Damit Angreifer Ihre Daten nicht mitlesen können, sollten Sie das Online-Banking auf fremden Rechnern und in fremden Netzwerken wie Internetcafés vermeiden!

### ► **Verwenden Sie ein Virenschutzprogramm und eine Personal-Firewall!**

Um sich vor Schadprogrammen angemessen zu schützen, ist es stets erforderlich das Sie ein aktuelles Antivirenprogramm verwenden. Achten Sie darauf, dass Sicherheitsupdates regelmäßig durchgeführt werden und sich das Programm immer auf dem neuesten Stand befindet. Verwenden Sie eine aktuelle Personal-Firewall für Ihren Computer. Betriebssysteme wie Windows XP, Vista und 7 haben diese bereits von Haus aus integriert.

### ► **Spielen Sie regelmäßig Sicherheitsupdates ein!**

Nicht nur das Virenschutzprogramm, sondern auch das Betriebssystem sowie alle installierten Anwendungen (Textverarbeitung, Browser, E-Mailprogramm) sollten beim Erscheinen von Sicherheitsupdates umgehend aktualisiert werden. Diese Updates können vom Betriebssystem und den meisten Programmen automatisiert durchgeführt werden. Überprüfen Sie dazu die Sicherheitseinstellungen bei Ihrem Betriebssystem in der Systemsteuerung.

*Autoren: Dipl.-Inform.(FH) Sebastian Spooren, Prof. Dr. Norbert Pohlmann  
Institut für Internet-Sicherheit - if(is), Fachhochschule Gelsenkirchen*

Weiterführende Informationen:

<http://www.internet-sicherheit.de>, <http://www.branchenbuch-it-sicherheit.de>

### **Das Institut für Internet-Sicherheit - if(is)**

Das Institut für Internet-Sicherheit ist eine fachbereichsübergreifende wissenschaftliche Einrichtung der Fachhochschule Gelsenkirchen. Es forscht und entwickelt auf Basis innovativer Konzepte im Bereich der Internet-Sicherheit. 2005 gegründet, hat es sich unter der Leitung von Prof. Norbert Pohlmann und in enger Zusammenarbeit mit der Wirtschaft innerhalb kurzer Zeit einen Ruf als eine der führenden deutschen Forschungsinstitutionen der IT-Sicherheit gemacht. Weitere Informationen finden Sie unter: <http://www.internet-sicherheit.de>.

### **Sichere E-Geschäftsprozesse in KMU und Handwerk**

Der IT-Sicherheitstipp wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: <http://www.ec-net.de/sicherheit>