

## WEGE ZUM ONLINE BANKING

Sicher, bequem und rund um die Uhr



Informationen für Online-Banking-Nutzer

Berlin, Mai 2008

# fokus:verbraucher

Eine Information  
der privaten Banken

## Wege zum Online Banking



### Online Banking – bequem und sicher

Die Abwicklung von Bankgeschäften über das Internet ist schnell, einfach und sehr weit verbreitet. Viele Menschen nutzen das Online-Banking-Angebot ihrer Bank, um bequem von zuhause aus „die eigene Bankfiliale zu besuchen“ – und das unabhängig von Öffnungszeiten, Parkplatzangebot und Wetter.

Die Internetseiten der Banken bieten dem Kunden neben Informationen ein umfassendes Angebot an Bankdienstleistungen: angefangen vom Kontoauszug über eine Überweisung bis hin zu Wertpapiergeschäften. Natürlich umfasst das Angebot viele weitere Geschäftsvorfälle. Wer sich beim Online Banking an bestimmte „Spielregeln“ hält, kann seine „persönliche Bankfiliale“ sicher betreiben.

Die Banken führen umfangreiche Maßnahmen zur Absicherung der im Rahmen des Online Banking übermittelten und bankseitig verarbeiteten Daten durch. Diese Sicherheitssysteme gewährleisten beispielsweise, dass Ihre vertraulichen Daten bei der Übertragung über das Internet nicht unberechtigt eingesehen und nicht unautorisiert verändert werden können. Auf die Sicherheit Ihres Computers hat Ihre Bank jedoch keinen Einfluss. Sie selbst wählen Ihre Hard- und Software frei aus. Außerdem setzen Sie in der Regel Ihren Online-Banking-Computer auch für viele weitere Anwendungen ein. Somit ist Ihr Computer potenziellen Gefahren aus dem Internet ausgesetzt, die Ihre Bank nicht kontrollieren kann.

Damit die von Ihrer Bank vorgesehenen Sicherheitsvorkehrungen nicht durch unberechtigte Manipulationen aus dem Internet unterlaufen werden können, müssen Sie als Kunde Ihrerseits Vorkehrungen zum Schutz Ihres Computers treffen.

Selbstverständlich lauern nicht überall im Internet Gefahren. Nicht jeder Kommunikationspartner will Sie schädigen. Schon wenn Sie die hier beschriebenen Hinweise beachten, können Sie die Sicherheit Ihres Computers um ein Vielfaches steigern und die verbleibenden Restrisiken auf ein Minimum reduzieren.

Nachfolgend zeigen wir Ihnen musterhaft, wie eine Online-Banking-Sitzung zur Ausführung einer Überweisung mit Hilfe eines Internetbrowsers sicher vorstattengehen kann. Die Aussagen gelten sinngemäß auch für Online Banking über andere Kanäle wie zum Beispiel FinTS-/HBCI-Banking.



## Wichtig: nur mit sicherem Computer starten

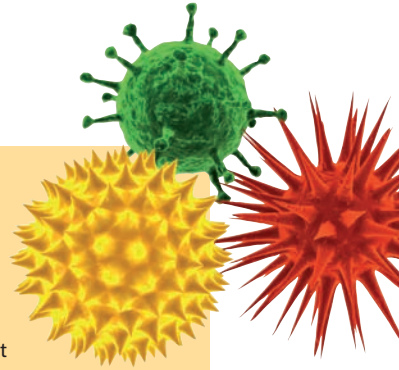
Genauso wie eine Autofahrt nur mit einem fahrtüchtigen und verkehrssicheren Auto stattfinden darf, sollten Sie auch Online Banking nur mit einem funktionierenden und sicheren Computer durchführen. Seien Sie Ihr eigener „PC-TÜV“. Sorgen Sie für Ihre Internetsicherheit. Wenn Sie dann genauso überlegt, ausgeruht und besonnen Online Banking betreiben, wie Sie Auto fahren, kann kaum etwas schiefgehen.

Zuallererst sollten Sie sich fragen, von welchem Rechner aus Sie Bankgeschäfte tätigen wollen. Wenn Sie den Computer nicht kennen, wie in einem Internetcafé oder bei einem Bekannten, dann wissen Sie natürlich auch nicht, welche Gefahren dort lauern. Schadsoftware könnte zum Beispiel alle Ihre Tastatureingaben mitschreiben, manipulieren und an Dritte weiterleiten. Oder umgekehrt: Würden Sie Ihren Wagen einem Unbekannten inklusive Autoschlüssel einfach so übergeben? Mit allen Fahrzeugpapieren?



## Schadsoftware

Als Schadsoftware (Malware = aus engl. malicious [„böartig“] und software) bezeichnet man Computerprogramme, die vom Benutzer unerwünschte und ggf. schädliche Funktionen ausführen. Da ein Benutzer im Allgemeinen keine schädlichen Programme duldet, sind die Schadfunktionen gewöhnlich getarnt oder die Software läuft gänzlich unbemerkt im Hintergrund. Beispielhafte Ziele von Schadsoftware sind: Ausschaltung der Sicherheitssoftware oder anderer Sicherheitseinrichtungen (wie z. B. von Firewalls und Antivirenprogrammen) eines Computers, Ausspähung sensibler Daten (wie z. B. von Passwörtern) und Weiterleitung per E-Mail/Internet an den „Besitzer“ der Schadsoftware. Auch kann ein Angreifer auf derartig infizierte Rechner zugreifen und dann praktisch die Fernkontrolle über alle Funktionen erlangen. Beispiele für Schadsoftware sind Computerviren, Würmer und Trojanische Pferde.



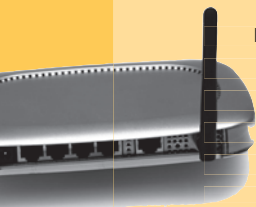
Achten Sie auf anomales Verhalten Ihres Computers:

- Meldungen des Betriebssystems, Ihrer Internet- oder Sicherheitssoftware nicht ignorieren! Einfaches „Wegklicken“ hilft meistens nicht weiter. Wenn Sie eine Meldung nicht verstehen, holen Sie hierzu Informationen beispielsweise über eine Suchmaschine ein oder fragen Sie einen Computerspezialisten.
- Läuft Ihr Rechner plötzlich deutlich langsamer oder unter Volllast, kann das ein Zeichen für unerwünschte „Mitfahrer“ – Schadsoftware – im Speicher oder auf der Festplatte Ihres Computers sein. Suchen Sie nach der Ursache. Einfaches Ignorieren kann die gleichen verheerenden Folgen haben wie das Weiterfahren mit Ihrem Auto bei Fehleranzeige in Ihrem Bordinfo-Display.
- Ist plötzlich das Antivirenprogramm oder eine andere Sicherheitssoftware nicht mehr aktiviert, so ist das ein starkes Anzeichen dafür, dass ein Schadprogramm den jeweiligen Schutz manipuliert hat.

- Das Gleiche gilt auch für nicht funktionierende automatische Updates, zum Beispiel des Betriebssystems oder des Antivirenprogramms. Schadsoftware kann nämlich auch die automatische Updatefähigkeit ausschalten. Als Folge wäre Ihr Computer schutzlos, Angriffsversuche blieben so unerkannt. Deshalb: Augen auf! Lassen Sie sich vom Gegenverkehr nicht blenden.

Wireless Local Area Network (WLAN) ist in aller Lüfte. Es bezeichnet ein lokales, „drahtloses“ Funknetz. Wollen Sie diese Funkstrecke zwischen Ihrem Computer und dem Internetanschluss nutzen, sollten Sie sich entsprechend schützen. Verschlüsseln Sie Ihr WLAN mit einem sicheren Verfahren. Verbinden Sie Ihren Online-Banking-Computer auf keinen Fall mit öffentlichen, ungesicherten Funkstrecken – beispielsweise am Flughafen oder Bahnhof.

#### WLAN



Bei WLAN kommunizieren ein oder mehrere Computer über eine Basisstation (Router) mit dem Internet. WLAN bietet verschiedene Verschlüsselungsverfahren zur Absicherung der Kommunikation zwischen Router und dem Empfänger am Computer (z. B. ausgeführt als USB-Stick) an. Achten Sie darauf, dass Router und PC-Empfänger mindestens mit dem Sicherheitsstandard WPA, besser mit WPA2 kommunizieren. Auf keinen Fall sollten Sie Ihr WLAN nur im WEP-Modus oder ungesichert betreiben. Weitere Informationen zur Sicherheit von Funkverbindungen können Sie unter <http://www.inside-security.de/wlan.html> finden.

Oft müssen Sie sich für die Anmeldung zum Online Banking, das „Log-in“, ein Passwort oder eine persönliche Geheimnummer (PIN) überlegen. Bilden Sie sichere Passwörter und wechseln Sie diese regelmäßig, zum Beispiel alle drei Monate. Ein einfaches Passwort oder eine einfache PIN kann leicht erraten werden. Eine Methode, um sichere Passwörter zu bilden, ist zum Beispiel in der Broschüre „Online-Banking-Sicherheit – Informationen für Online-Banking-Nutzer“ des Bankenverbandes beschrieben.

Arbeiten Sie am Computer nicht mit Administrationsrechten – weder direkt unter der Kennung „Administrator“ noch indirekt über eine Administratorgruppe. Erlangt ein Angreifer Zugang zu Ihrem Computer als Administrator, so kann er auf und mit Ihrem Rechner ALLES machen. Insbesondere kann der Internetkriminelle Sicherheitssoftware und Sicherheitseinstellungen auf Ihrem Rechner ganz einfach manipulieren und Schadsoftware installieren.



Um sich sicher im Internet zu bewegen, sollten Sie die folgenden Schritte nacheinander durchführen:

1. Beachten Sie die Sicherheitseinstellungen Ihrer installierten Software – insbesondere vom Betriebssystem und Internetbrowser. Denn: Es gibt Schadsoftware, die Schwachstellen und Fehlkonfigurationen in Softwareprogrammen ausnutzt. Achten Sie darauf!
2. Prüfen Sie, ob es neue Updates für Ihr Betriebssystem gibt. Spielen Sie insbesondere Sicherheitsupdates sofort ein.
3. Prüfen Sie, ob Ihre Sicherheitssoftware, wie Antivirenprogramm und Personal Firewall, aktiviert und auf dem aktuellen Stand ist. Aktualisieren Sie sie ggf.
4. Aktualisieren Sie Ihr Browserprogramm.
5. Lesen Sie die aktuellen Sicherheitsmeldungen Ihrer Bank.

## Starten der Online-Banking-Sitzung

Um Ihre Online-Banking-Sitzung zu beginnen, rufen Sie die Log-in-Seite Ihrer Bank auf. Hierzu tippen Sie am besten die Internetadresse (URL) händisch ein. Auf keinen Fall sollten Sie unbesehen und unkontrolliert Web-Links aus nicht verifizierbaren Quellen verwenden, die Ihnen beispielsweise per E-Mail zugesandt werden. Die drohende Gefahr hinter diesen Internetadressen: Es wird Ihnen eine täuschend ähnliche, aber gefälschte Internetseite „Ihrer“ Bank präsentiert, um Ihre geheimen Online-Banking-Zugangsdaten auszuspähen und damit Missbrauch zu betreiben.

https://



Deshalb sollten Sie sich nach Aufruf Ihrer Bankseite noch einmal vergewissern, ob Sie die URL auch richtig, das heißt ohne Tippfehler etc., eingegeben haben.

Sie betrachten nun Ihre Bankseite. Sieht sie vertraut aus? In allen Ihnen bekannten Einzelheiten des Layouts? Wenn Sie Ihre Bankseite schon oft aufgerufen haben, dann fällt Ihnen

sogar eine minimale Änderung sofort auf. Zögern Sie vor allem nicht, bei Ihrer Bank telefonisch, per E-Mail oder in der Filiale nachzufragen, ob eine Änderung vorgenommen wurde. Vorsicht ist auch hier besser als Nachsicht.

Die Log-in-Seite Ihrer Bank muss mit „https“ beginnen. Falls nicht, kann es sich definitiv nicht um die verschlüsselte Online-Banking-Seite Ihrer Bank handeln. Das „s“ macht den Unterschied! Es steht für eine so genannte SSL-Verbindung, die für die Dauer Ihrer Online-Banking-Sitzung für eine verschlüsselte und damit gesicherte Übertragung zwischen Ihrem Computer und dem Rechner Ihrer Bank sorgt. Das Gleiche gilt auch für das Schlüssel- oder Schlosssymbol in Ihrem Internetbrowser. Es befindet sich bei den meisten Browsern unten rechts. Dieses Symbol muss ebenfalls während der gesamten Online-Banking-Sitzung zu sehen sein.

Ebenfalls prüfen sollten Sie das so genannte Zertifikat Ihrer Bank, das Sie nach einem Doppelklick auf das Schlosssymbol Ihres Internetbrowsers sehen. Das Zertifikat informiert darüber, auf wen (Ihre Bank) und durch wen (anerkannte Zertifizierungsstelle) es ausgestellt wurde und wie lange es gültig ist. Sollte beispielsweise der im Zertifikat genannte Besitzer nicht Ihre Bank sein oder das Zertifikat gar nicht mehr gültig sein, so stimmt irgendetwas nicht. Kontaktieren Sie, wie oben beschrieben, sofort Ihre Bank. Zusätzlich können Sie noch den Fingerabdruck des aktuellen Zertifikats mit dem Fingerabdruck Ihrer Bank vergleichen. Dieser ist auf den Sicherheitsseiten Ihrer Bank zu finden.

Für das Log-in zu Ihrem Konto dürfen auf der Internetseite der Bank nur die üblichen, Ihnen bereits bekannten Zugangsdaten abgefragt und eingegeben werden – keinesfalls weitere wie zum Beispiel eine TAN. Andernfalls befinden Sie sich auf einer gefälschten Seite oder Ihr Computer ist mit einem Spionageprogramm, einem so genannten Trojanischen Pferd, infiziert.

Sie haben jetzt Zugang zu Ihrem Konto erlangt und stoßen noch keine Konto-bewegung an. Beim Auto würden Sie jetzt vor dem Lenkrad sitzen und gleich den Motor anlassen. Halten Sie vor dem Losfahren inne. Prüfen Sie zunächst, ob Sie allein im Auto sind, wie es um Ihren Treibstoff aussieht und wie sich der allgemeine Zustand Ihres Fahrzeugs darstellt.

Wenn Ihre Bank es anbietet, prüfen Sie den Zeitpunkt Ihres letzten Log-ins. Wenn jemand anderes Zugang zu Ihrem Konto hat, wird er sich vielleicht Ihren Kontostand zu einem Zeitpunkt angeschaut haben, an dem Sie selbst gar nicht online waren. Merken oder besser notieren Sie sich immer den Zeitpunkt Ihrer letzten Online-Banking-Sitzung. Abschließend prüfen Sie Ihre Umsätze, Ihren Konto- und Depotstand. Sind diese plausibel? Andernfalls kontaktieren Sie Ihre Bank.



Sie sollten regelmäßig die Sicherheitseinstellungen Ihres Online Banking prüfen. Diese Einstellungen sind ebenfalls abhängig vom Angebot Ihrer Bank. So können Sie selbst bei einigen Banken Überweisungslimits setzen oder ein Referenzkonto bei online geführten Spar- und/oder Anlagekonten einrichten. Durch ein Limit können Sie selbst festlegen, wie viel maximal von Ihrem Konto auf einmal überwiesen werden kann. Wenn Sie Geldfluss nur zu und von einem Referenzkonto erlauben, kann ein Dritter Ihr Geld auf kein anderes Konto schicken. Ferner sollten Sie ggf. auch Ihre bei der Bank gespeicherten persönlichen Daten wie E-Mail-Adresse und Handynummer regelmäßig prüfen. Abhängig vom Angebot Ihrer Bank wird Ihnen an die E-Mail-Adresse eine Änderung des Limits gemeldet oder über Ihre Handynummer die mobile TAN zugesandt werden.

Durch diese Prüfungen können Sie feststellen, ob ein Angreifer Ihre Zugangsdaten zum Konto und Transaktionsdaten (beispielsweise die iTAN) besitzt und bereits verwendet hat. Sie erhalten dadurch Hinweise, ob jemand Einsicht in das Konto nahm oder gar eine Überweisung veranlasste.

Wenn angeboten, sollten Sie auch die Sicherheitshinweise bei und nach der Anmeldung lesen. So benötigen Sie eine Transaktionsnummern (TAN) nur zur Freigabe von Transaktionen – und zwar eine einzige TAN für eine Transaktion – oder zur Änderung von persönlichen Daten. Keinesfalls benötigen Sie TANs beispielsweise zur Bestätigung dieser Sicherheitshinweise. Wird das von Ihnen verlangt, kontaktieren Sie bitte sofort Ihre Bank. Ebenfalls stimmt etwas nicht, wenn Sie auf einmal zur Eingabe von mehr als einer TAN aufgefordert werden.

Hat Ihre Kontoumgebung Ihrem kritischen Blick standgehalten, so können Sie jetzt an Ihre Überweisung gehen. Sie wissen nun, dass seit Ihrer letzten Online-Banking-Sitzung nichts vorgefallen ist.

## Überweisung vornehmen

Füllen Sie nun wie gewohnt die Überweisungsmaske aus. Haben Sie bereits früher Überweisungsvorlagen/Dauerauftragsvorlagen angelegt, so verwenden Sie diese, natürlich erst nach einer kurzen Prüfung deren Richtigkeit. Denn ein Angreifer, der Zugang zu Ihrem Konto hätte, könnte auch diese Vorlagen manipuliert haben, indem er zum Beispiel die Zielkontonummer ändert. Kontrollieren Sie die Überweisungsdaten und schicken Sie dann den Auftrag an Ihre Bank. Diese fordert Sie nun zur Eingabe einer Transaktionsnummer (nicht zwei und mehrerer) auf. Wenn Ihre Bank bereits das iTAN-Verfahren einsetzt, müssen Sie die TAN mit dem angeforderten Index eingeben. Bevor Sie diese eintippen und die Transaktion somit bestätigen, überprüfen Sie noch einmal die Überweisungsdaten. Benutzen Sie eine Authen-



tifizierungsmethode, die sich eines so genannten Hardwaretokens (z. B. Handy beim Mobile-TAN-Verfahren, TAN-Generator etc.) bedient, prüfen Sie die auf dem Display dieses Gerätes angezeigten Überweisungsdaten.

Sie können die Überweisung nun durch Bestätigung freigeben. Wird „TAN ungültig“ angezeigt, überprüfen Sie Ihre eingegebene TAN auf Tippfehler. Auf keinen Fall einer Aufforderung wie „Bitte x weitere TANs eintippen“ Folge leisten und sofort über die bekannten Wege Ihre Bank kontaktieren. Prüfen Sie nach Abschluss der Überweisung noch die Auftragsbestätigung. Je nach Ausführung erhalten Sie von Ihrer Bank noch eine Bestätigungsnummer (meistens eine dreistellige Nummer, die zu Ihrer zuvor eingetippten TAN passen muss).

Nach Abschluss der Überweisung sollten Sie Ihren Kontostand (inklusive der Vormerkungen) online nochmals prüfen: Stimmen Umsatzübersicht und Kontostand? Sehen Sie sich die zuletzt vorgenommene Überweisung an. Stimmen Details wie Betrag, Kontonummer, BLZ, ggf. BIC und IBAN?

Kontrollieren Sie auch die vorgemerkten Überweisungen, denn diese könnten ebenso durch einen Angreifer mit Kenntnis Ihrer geheimen Zugangsdaten manipuliert worden sein.

Nach Abschluss der Aktivitäten beenden Sie die Online-Banking-Sitzung korrekt, indem Sie auf den „Log-out“- oder auch „Abmelden“-Link in der Online-Banking-Anwendung klicken. Sie sollten nicht einfach den Internetbrowser schließen, ohne sich vorher ordnungsgemäß abzumelden.

Zu guter Letzt: Überprüfen Sie regelmäßig Ihren beleghaften oder elektronischen Kontoauszug.



## Bei Verdacht

Stimmt mit Ihrem Computer oder mit Ihrer Einsatzumgebung etwas nicht, so bringen Sie das in Ordnung. Bei Problemen mit Ihrer Hard- oder Software wenden Sie sich bitte an den jeweiligen Hersteller. Funktioniert alles wieder so, wie Sie es gewohnt sind, ändern Sie die Zugangsdaten zu Ihrem Online Banking. Vielleicht war ja etwas nicht in Ordnung, weil ein Schadprogramm Ihre Zugangsdaten ausspähen wollte.

Stellen Sie fest, dass die Online-Banking-Seite Ihrer Bank gefälscht ist, so befinden Sie sich gar nicht auf der Seite Ihrer Bank, sondern auf der eines Betrügers. Kontaktieren Sie umgehend Ihre Bank: Rufen Sie die Hotline an. Alternativ schicken Sie eine E-Mail (mit Screenshot) an Ihre Bank. Führen Sie auf keinen Fall weitere Online-Banking-Transaktionen aus, sondern besprechen Sie die weitere Vorgehensweise mit Ihrem Kreditinstitut.

Ist erkennbar, dass ein Dritter Zugriff zu Ihrem Konto hat, wenden Sie sich sofort an Ihre Bank und machen Sie keine weiteren Transaktionen. Sperren Sie umgehend den Onlinezugang zu Ihrem Konto, indem Sie drei Mal eine falsche PIN eintippen.

Ist erkennbar, dass von Ihrem Konto bereits Geld abgeflossen ist, informieren Sie sofort Ihre Bank und erstatten Sie Anzeige bei der Polizei. In Absprache mit Ihrer Bank machen Sie dann Ihren Computer wieder sicher. Dazu gehört die Aktualisierung und ggf. sogar Neuinstallation des Betriebssystems, des Antivirenprogramms und der Personal Firewall. Zur weiteren Schadenabwehr prüfen Sie bitte, ob der Angreifer auch die Daten für Ihre Bank- oder Kreditkarten sowie Ihre E-Business-Partner und E-Mail-Konten erlangt haben könnte. Das können Sie zum Beispiel durch Einsicht in Ihre Kreditkartenabrechnung erreichen.

Zudem sollten Sie Personen, die Ihren Computer mitnutzen, warnen, denn vielleicht hat der Angreifer auch versucht, deren persönliche Zugangsdaten auszuspähen.



Weitere technische Details inklusive Checkliste zum sicheren PC schlagen Sie bitte in der Broschüre des Bankenverbandes „Online-Banking-Sicherheit – Informationen für Online-Banking-Nutzer“ nach. Informationen rund um das Thema Sicherheit finden Sie im Internet auf den Seiten Ihrer Bank, des Bankenverbandes (<http://www.bankenverband.de/online-banking>) sowie auf den Seiten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter <http://www.bsi-fuer-buerger.de>.



## Ergänzende Sicherheitshinweise

Zum Schluss folgen einige Hinweise, die Sie unbedingt befolgen sollten.

- Öffnen Sie keine E-Mails von unbekanntem Absendern.
- Öffnen Sie keine Anhänge, bevor Sie die E-Mail nicht auf Plausibilität geprüft haben. Beispielsweise werden in letzter Zeit immer öfter als „Rechnungen“ getarnte Trojanische Pferde per E-Mail versendet. Fragen Sie sich, ob Sie Kunde der im Absender genannten Firma sind und damit gemeint sein könnten.
- Verwenden Sie nur legal erworbene Software aus vertrauenswürdigen Quellen.
- Vor dem Öffnen sollten Sie eine heruntergeladene Datei erst lokal speichern und auf Schadsoftware prüfen.
- Erscheint Ihnen irgendetwas unseriös, werden Sie misstrauisch!
- Bevor Sie sich mit dem Internet verbinden, prüfen Sie, ob Ihre Sicherheitssoftware aktiviert ist, und aktualisieren Sie diese, bevor Sie sich im Internet bewegen.
- Schalten Sie die Autorun-Funktion aus, wenn Sie mit mobilen Speichermedien, wie USB-Sticks, DVDs oder CD-ROMs, arbeiten. Vor der Ausführung und dem Öffnen von Inhalten dieser Medien sollten Sie USB-Sticks, DVDs oder CD-ROMs

erst mit einem Antivirenprogramm sorgfältig überprüfen.










- Wenn WLAN, dann sicher!
- Installieren Sie nur Software, die Sie wirklich brauchen. Im Umkehrschluss sollten Sie deshalb nicht jedes „Powertool“ und jede „Toolbar“ installieren, die man Ihnen unterjubeln will.



## 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:

- |   |  |
|---|--|
|    | <b>Kundeninformation zum Kreditverkauf</b><br>Fragen und Antworten<br>Berlin, März 2008              |
|    | <b>Die Abgeltungsteuer</b><br>Informationen für Privatkunden<br>Berlin, Februar 2008                 |
|    | <b>SEPA</b><br>Einfach bezahlen in Europa<br>Berlin, Januar 2008                                     |
|    | <b>Private Altersvorsorge</b><br>Informationen für Privatkunden<br>Berlin, Dezember 2007             |
|    | <b>Elektronische Kontoauszüge</b><br>Informationen für Privatkunden<br>Berlin, Dezember 2007         |
|   | <b>Online-Banking-Sicherheit</b><br>Informationen für Online-Banking-Nutzer<br>Berlin, November 2007 |
|  | <b>Sicher mit Karte</b><br>10 Sicherheitstipps zur Bankkarte<br>Berlin, November 2007                |
|  | <b>Tätigkeit als Finanzagent</b><br>Finger weg von dubiosen Angeboten!<br>Berlin, Juli 2007          |
|  | <b>15 Jahre Ombudsmann der privaten Banken</b><br>Tätigkeitsbericht 2006<br>Berlin, Juli 2007        |

Alle Publikationen können unter [www.bankenverband.de](http://www.bankenverband.de) kostenfrei bestellt werden oder als pdf-Datei heruntergeladen werden.

## WEGE ZUM ONLINE BANKING

---

Berlin, Mai 2008

**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](http://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](mailto:bankenverband@bdb.de)



#### Im Internet

[www.bankenverband.de](http://www.bankenverband.de)