

ONLINE BANKING –  
BEQUEM UND SICHER



Informationen für Online-Banking-Nutzer

Berlin, Februar 2011

fokus:verbraucher

Eine Information  
der privaten Banken



ONLINE BANKING –  
BEQUEM UND SICHER

---

Berlin, Februar 2011



## Online Banking – bequem und sicher

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

Die Internetseiten der Banken bieten dem Kunden ein umfassendes Angebot an Bankdienstleistungen, vom Kontoauszug über eine Überweisung bis hin zum Wertpapiergeschäft. Wer sich beim Online Banking an bestimmte „Spielregeln“ hält, kann seine „persönliche Bankfiliale“ sicher betreiben.

Die Banken führen umfangreiche Maßnahmen zur Absicherung des Online Banking durch. Diese Maßnahmen gewährleisten unter anderem, dass Ihre vertraulichen Daten bei der Übertragung über das Internet nicht eingesehen und verändert werden können. Auf die Sicherheit Ihres Computers hat Ihre Bank jedoch keinen Einfluss. Sie selbst wählen Ihren Rechner mit zugehöriger Hard- und Software frei aus. Außerdem setzen Sie in der Regel Ihren Online-Banking-Computer auch für viele andere Anwendungen ein. Somit ist dieser Computer potenziellen Gefahren aus dem Internet ausgesetzt, die Ihre Bank nicht kontrollieren kann.

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

Nachfolgend zeigen wir Ihnen anhand von Beispielen, wie eine Online-Bankingsitzung 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 oder Mobile Banking.

## Wichtig: nur mit sicherem Computer arbeiten

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 besonders Online Banking nutzen, 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 Tastatur- und Mauseingaben mitschneiden, manipulieren und an Dritte weiterleiten. Oder umgekehrt: Würden Sie einen fremden Wagen ohne TÜV fahren? Vielleicht mit defekten Bremsen?

### Typische Gefahren: Phishing und Schadsoftware

Phishing bezeichnet die Vortäuschung von falschen Namen, Internetseiten oder Adressen zum Zweck des Betrugs. Als Schadsoftware (engl. Malware) werden Computerprogramme, wie zum Beispiel Computerviren, Würmer und trojanische Pferde, bezeichnet, die unerwünschte und ggf. schädliche Funktionen unbemerkt ausführen. Hierzu zählen beispielsweise das Ausschalten der Sicherheitssoftware wie einer Personal Firewall oder eines Antivirenprogramms, das Ausspähen sensibler Daten wie Passwörter und das Weiterleiten dieser per E-Mail/Internet an den „Besitzer“ der Schadsoftware. Auch kann ein Angreifer auf derartig infizierte Rechner zugreifen und die Fernkontrolle über alle Funktionen erlangen. Damit übernimmt der Angreifer Ihren Rechner, als säße er direkt davor.

### Achten Sie auf ungewöhnliches Verhalten beim Betrieb Ihres Computers:

- Meldungen des Betriebssystems und Ihrer Sicherheits- und Anwendungssoftware nicht ignorieren! Dies könnte die gleichen verheerenden Folgen wie das Weiterfahren mit Qualm aus der Motorhaube haben. Einfaches „Wegklicken“ hilft meistens nicht weiter. Wenn Sie eine Meldung nicht verstehen, sollten Sie dieser auf den Grund gehen. Holen Sie hierzu Informationen beispielsweise über eine Suchmaschine ein oder fragen Sie einen Computer-Spezialisten.
- Läuft Ihr Rechner plötzlich zum Beispiel deutlich langsamer oder unter Volllast, kann das ein Zeichen für unerwünschte „Mitfahrer“ – etwa Schadsoftware – sein. Suchen Sie nach der Ursache, ggf. mit fachkundiger Unterstützung.
- 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 oder gar ausgeschaltet hat.
- Das Gleiche gilt auch für nicht funktionierende automatische Updates, zum Beispiel des Betriebssystems oder des Antivirenprogramms. Schadsoftware kann auch die automatische Update-Fähigkeit ausschalten. Als Folge wäre Ihr Computer schutzlos, Angriffsversuche blieben so unerkannt. Deshalb: Augen auf!



Arbeiten Sie am Computer nicht mit Administratorrechten – weder direkt unter der Kennung „Administrator“ noch indirekt über eine Administratorgruppe. Erlangt ein Angreifer Zugriff auf Ihren Computer, hat dieser ebenfalls Administratorrechte und kann so mit Ihrem Rechner **ALLES** machen. Insbesondere kann der Internetkriminelle dann Sicherheitssoftware und Sicherheitseinstellungen auf Ihrem Rechner manipulieren und Schadsoftware installieren. Arbeiten Sie deshalb mit minimalen Nutzerrechten.

Führen Sie einen kompletten Suchlauf Ihres Antivirenprogramms über alle Laufwerke Ihres Rechners durch. Wiederholen Sie dieses regelmäßig (z. B. einmal in der Woche).

### Informationsquellen

Informieren Sie sich regelmäßig über Sicherheitsaspekte bei der Nutzung des Internets sowie geeignete Schutzmaßnahmen. Informationen dazu finden Sie auf der Internetseite Ihrer Bank, des Bankenverbandes ([www.bankenverband.de](http://www.bankenverband.de)) oder des Bundesamtes für Sicherheit in der Informationstechnik ([www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)) und zusammen mit dem Verband der deutschen Internetwirtschaft unter [www.botfrei.de](http://www.botfrei.de). Kostenfreie Sicherheitssoftware finden Sie zum Beispiel dort in einer speziellen Rubrik unter [www.bsi-fuer-buerger.de/toolbox/tools.htm](http://www.bsi-fuer-buerger.de/toolbox/tools.htm).

### Starten der Online-Banking-Sitzung

Um Ihre Online-Banking-Sitzung zu beginnen, rufen Sie die Anmeldeseite Ihrer Bank auf. Auf keinen Fall sollten Sie unbesehen und unkontrolliert Web-Links aus Ihnen unbekanntenen 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.

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 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. Beim Auto hätten Sie nun vor Fahrtantritt überprüft, ob Sie alle Fahrzeugpapiere dabei haben.

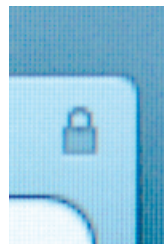
Die Anmeldeseite Ihrer Bank muss mit „https“ beginnen. Falls nicht, handelt es sich definitiv nicht um die verschlüsselte Online-Banking-Seite Ihrer Bank. Das „s“ macht den Unterschied! Es steht für eine so genannte SSL-Verbindung, die für die Dauer Ihrer Online-Banking-Sitzung für eine verschlüsselte 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. Dieses Symbol muss ebenfalls während der gesamten Online-Banking-Sitzung zu sehen sein. Sollte das „s“ oder das Schlüssel- bzw. Schlosssymbol fehlen, melden Sie dies umgehend Ihrer Bank.

Ebenfalls sollten Sie das Zertifikat der Online-Banking-Seite prüfen, das Sie nach einem Doppelklick auf das Schlosssymbol Ihres Internetbrowsers sehen. Das Zertifikat informiert darüber, auf wen und durch wen es ausgestellt wurde und wie lange es gültig ist.

### Schutz der Zugangsdaten

Schützen Sie Ihre Zugangsdaten – PIN und die Liste der Transaktionsnummern (kurz TANs) – bzw. Ihr Zugangsmedium zum Online Banking (z. B. Chipkarte) vor unberechtigtem Zugriff. Verwenden Sie für die Anmeldung zum Online Banking ein sicheres Passwort, das Sie in regelmäßigen Abständen ändern. Geben Sie Ihre geheimen Zugangsdaten niemals auf anderen als den von Ihrer Bank zugelassenen Internetseiten ein oder in sonstiger Weise gegenüber einem Dritten preis. Denn mit der Preisgabe Ihres persönlichen „Schlüssels“ für das Online Banking eröffnen Sie Dritten die Möglichkeit, diesen „Schlüssel“ unberechtigt zu nutzen. Das heißt, der Dritte könnte Einsicht in alle Ihre Kontoumsatzdaten nehmen oder sogar Überweisungen zu Ihren Lasten tätigen. In den Online-Banking-Bedingungen Ihrer Bank sind deshalb Ihre vertraglichen Sorgfaltspflichten zur Nutzung der von der Bank freigegebenen Zugangskanäle und zur Geheimhaltung von PIN und TANs ausführlich geregelt. Diese Pflichten dienen dem Schutz des Online-Banking-Verfahrens im Interesse von Kunde und Bank.



Vergewissern Sie sich bei jeder Eingabe Ihrer persönlichen Zugangsdaten, dass es sich beim Adressaten um Ihre Bank handelt. Ihre Bank wird Sie niemals zum Beispiel per E-Mail oder Telefon kontaktieren, um nach Ihren geheimen Zugangsdaten wie PIN oder TAN zu fragen. Ebenfalls werden Sie niemals nach mehreren TANs gleichzeitig gefragt.



Folgen Sie keinen Instruktionen, die Ihnen negative Konsequenzen wie beispielsweise eine Kontosperre androhen. Informieren Sie umgehend Ihre Bank über diesen Betrugsversuch.

Bei der Anmeldung 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 oder mehrere TANs. Andernfalls befinden Sie sich auf einer gefälschten Seite oder Ihr Computer ist mit einer Schadsoftware, zum Beispiel einem so genannten trojanischen Pferd, infiziert.

#### **Sicherheit und Status quo überprüfen**

Sie haben jetzt Zugriff auf Ihr Konto erlangt, stoßen allerdings noch keine Kontobewegung an. Beim Auto würden Sie jetzt vor dem Lenkrad sitzen und gleich den Motor anlassen. Halten Sie vor dem Losfahren kurz inne. Prüfen Sie zunächst, ob Sie keinen „blinden Passagier“ mitnehmen, wie es um Ihren Treibstoff aussieht und wie sich der allgemeine Zustand Ihres Fahrzeugs darstellt.

Wenn Ihre Bank es anbietet, prüfen Sie den Zeitpunkt der letzten Anmeldung. Wenn jemand anderes Zugriff auf Ihr 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. Wurden seit Ihrer letzten Anmeldung Überweisungen veranlasst oder stehen aktuell schon Überweisungen in den Vormerkungen? Sind alle plausibel? Andernfalls kontaktieren Sie umgehend Ihre Bank.

Sie sollten regelmäßig die Sicherheitseinstellungen Ihres Online Banking prüfen. Diese Einstellungen sind ebenfalls abhängig vom Angebot Ihrer Bank. So können Sie bei einigen Banken Überweisungsmitel setzen oder ein Referenzkonto

bei online geführten Konten einrichten. Durch ein Limit können Sie 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 online Ihr Geld auf kein anderes Konto schicken. Ferner sollten Sie regelmäßig auch Ihre bei der Bank gespeicherten persönlichen Daten, wie Postanschrift, E-Mail-Adresse oder Handynummer, prüfen. Abhängig vom Angebot Ihrer Bank wird Ihnen an die E-Mail- oder Postadresse eine Änderung des Limits gemeldet oder über Ihre Handynummer die mobile TAN zugesandt.

Durch all diese Prüfungen können Sie feststellen, ob jemand Einsicht in das Konto genommen oder gar eine Überweisung veranlasst hat. 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. Sie fahren mit Ihrem Auto jetzt los.

### **Warnung vor ungewöhnlichen TAN-Abfragen**

Sie sollten immer die Sicherheitshinweise Ihrer Bank bei oder nach der Anmeldung lesen. Vorsicht, wenn die Sicherheitshinweise mit einer oder mehreren TANs quittiert werden sollen – dies wird Ihre Bank niemals verlangen! Lediglich zur Freigabe eines Auftrags oder zur Anpassung Ihrer persönlichen Online-Banking-Einstellungen werden Sie nach einer einzigen – niemals aber nach mehreren – TANs gefragt. Sollten Sie nach einer oder gar mehreren TANs auf eine Weise gefragt werden, die Ihnen ungewöhnlich erscheint, wie zum Beispiel

- wegen einer angeblichen Kontoentsperrung oder Laufzeitbeschränkung Ihrer TAN-Liste,
  - zur Quittierung eines Sicherheitshinweises,
  - wegen Wartungsarbeiten oder
  - vermeintlicher zusätzlicher Sicherheitsmaßnahmen,
- brechen Sie den Vorgang sofort ab und kontaktieren Sie umgehend Ihre Bank.

### Überweisung vornehmen

Füllen Sie nun wie gewohnt die Überweisungsmaske aus. Haben Sie bereits früher Überweisungsvorlagen angelegt, so verwenden Sie diese, natürlich erst nach einer kurzen Prüfung, ob alles richtig eingegeben wurde. Denn ein Angreifer, der Zugriff auf Ihr Konto hätte, könnte auch diese Vorlagen manipuliert haben, indem er zum Beispiel die Kontonummer für Ihre monatliche Mietzahlung ändert. Kontrollieren Sie die Überweisungsdaten und schicken Sie dann den Auftrag an Ihre Bank. Diese fordert Sie nun zur Eingabe einer – nicht zwei oder mehrerer – Transaktionsnummer auf. Bevor Sie diese eintippen und die Transaktion somit bestätigen, überprüfen Sie noch einmal die Überweisungsdaten. Benutzen Sie ein Legitimationsverfahren, das sich eines zusätzlichen Gerätes (z. B. Handy beim mobilen TAN-Verfahren, TAN-Generator etc.) bedient, vergleichen Sie die Überweisungsdaten auf dem Display dieses Gerätes mit den auf dem Computerbildschirm angezeigten Überweisungsdaten. Beim mobilen TAN-Verfahren wird die TAN per SMS auf Ihr Handy geschickt. Aus Sicherheitsgründen gilt, dass der Kunde niemals eine mobile TAN auf dem gleichen Mobiltelefon empfangen darf, das er für das Mobile Banking verwendet.

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. Bei einigen Banken erhalten Sie zusätzlich noch eine Bestätigungsnummer.

Nach Abschluss der Überweisung sollten Sie den aktuellen Kontostand sowie Ihre Vormerkungen online nochmals prüfen: Stimmen Umsatzübersicht und Kontostand? Sehen Sie sich die zuletzt vorgenommene Überweisung an. Stimmen Details wie Empfänger, Betrag, Empfängerkonto und Empfängerbank? Kontrollieren Sie auch die vorgemerkten Überweisungen, denn diese könnten ebenso durch einen Angreifer mit Kenntnis Ihrer geheimen Zugangsdaten manipuliert worden sein.



Nach Abschluss aller Aktivitäten beenden Sie die Online-Banking-Sitzung korrekt, indem Sie auf „Logout“– oder auch „Abmelden“ in der Online-Banking-Anwendung klicken. Sie sollten nicht einfach den Internetbrowser schließen, ohne sich vorher ordnungsgemäß abzumelden. Merken Sie sich, wann Sie das letzte Mal Online Banking gemacht haben.

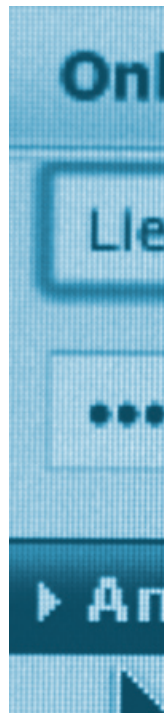
Zu guter Letzt: Überprüfen Sie regelmäßig Ihren beleghaften und/oder elektronischen Kontoauszug.

### 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 Ihre Zugangsdaten. Vielleicht war ja etwas nicht in Ordnung, weil eine Schadsoftware Ihre Zugangsdaten ausspähen wollte. Wenn Sie an Ihrem Fahrzeug ungewöhnliche Geräusche wahrnehmen, gehen Sie diesen ja auch auf den Grund.

Stellen Sie fest, dass die Online-Banking-Seite Ihrer Bank gefälscht ist oder erkennbar ist, dass ein Dritter Zugriff zu Ihrem Konto hat oder haben könnte, so kontaktieren Sie umgehend Ihre Bank: Rufen Sie die Hotline an! Alternativ können Sie eine E-Mail schicken – am besten mit einer Bildschirmkopie (engl. Screenshot) – an Ihre Bank. Führen Sie auf keinen Fall weiter Online-Banking-Transaktionen aus, sondern besprechen Sie die weitere Vorgehensweise mit Ihrer Bank. Sperren Sie umgehend den Online-Zugang zu Ihrem Konto, indem Sie zum Beispiel mehrmals 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. Machen Sie Ihren Computer wieder sicher. Dazu gehört die Aktualisierung und ggf. sogar Neuinstallation des Betriebssystems, des Antivirenprogramms und der Personal Firewall. Zur



weiteren Schadensabwehr prüfen Sie bitte, ob der Angreifer auch die Daten für Ihre Kreditkarten und zum Beispiel Ihre E-Mail-Konten missbraucht haben könnte. Ändern Sie daher sofort all Ihre Zugangsdaten – sowohl die für Ihren eigenen Rechner als auch die anderer Internetdienste, zum Beispiel Online-Shops, soziale Netzwerke und andere Kreditinstitute. Zudem sollten Sie Personen warnen, die Ihren Computer mit nutzen – denn vielleicht hat der Angreifer auch versucht, deren persönliche Zugangsdaten auszususpionieren.



### Ja zum Online Banking – aber nicht im Namen Dritter

Stellen Sie Ihr Bankkonto Dritten – bewusst oder unbewusst – nicht für betrügerische Finanztransaktionen zur Verfügung. Auf Internetseiten und per E-Mail sprechen Kriminelle immer wieder Inhaber von Bankkonten an, um sie für eine Tätigkeit als so genannter „Finanzagent“, „Warenagent“ oder auch „Kontovermieter“ zu gewinnen. Oft werden Ihnen auch stimmige Geschichten – zum Beispiel Kauf von Waren sowie Liebesbekanntschaften im Internet – präsentiert, um Sie unwissend zum Finanzagenten zu machen. Über das inländische Bankkonto sollen diese „Finanzagenten“ Zahlungen Dritter entgegennehmen und möglichst umgehend auf ein anderes Konto im In- oder Ausland weiterleiten oder per Bargeldversand an eine im Ausland befindliche Person überweisen. Als Entgelt werben die Internetkriminellen mit einer stattlichen Provision, die vom Überweisungsbetrag abgezogen wird. Wenn Sie auf ein solches Angebot eingehen, können Sie sich nicht nur schadensersatzpflichtig, sondern auch strafbar machen. Über diese Betrugsarten informiert Sie ausführlich die Broschüre „Tätigkeit als Finanzagent“ des Bankenverbandes.

### Die wichtigsten Sicherheitshinweise im Überblick

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

- Prüfen Sie, ob es neue Updates für Ihr Betriebssystem oder Ihre Softwareprogramme gibt. Spielen Sie insbesondere Sicherheitsupdates sofort ein. Aktivieren Sie die automatische Installation von Updates auch von Ihrer Anwendungssoftware.
- Setzen Sie zusätzliche Sicherheitssoftware ein. Denn manche Sicherheitsprobleme lassen sich nicht allein mit „Bordmitteln“ des Betriebssystems lösen. Wichtige Zusatzwerkzeuge sind eine Antivirensoftware und eine Personal Firewall. Beide müssen permanent aktualisiert werden und damit in die Lage versetzt werden, aktuelle Gefahren zu erkennen.
- Verwenden Sie immer die aktuellste Version Ihres Internetbrowsers.
- Öffnen Sie keine E-Mails und Anhänge von unbekanntem Absendern. Beispielsweise werden als „Rechnungen“ getarnte trojanische Pferde per E-Mail versendet. Prüfen Sie Ihre E-Mails auf Plausibilität. Fragen Sie sich, ob Sie Kunde der im Absender genannten Firma sind und damit überhaupt gemeint sein können. Verwenden Sie Ihren gesunden Menschenverstand.
- Nutzen Sie ein Programm, mit dem Sie die Aktualität Ihrer installierten Software überprüfen können (Update-Check). Diese Programme gibt es auch kostenlos.



## Die Reihe „fokus:verbraucher“

Informationen, die sich gezielt an Verbraucher wenden, fasst der Bankenverband in einer eigenen Reihe „fokus:verbraucher – eine Information der privaten Banken“ zusammen. Hier erhalten Verbraucher kostenfrei fundierte Informationen in leicht verständlicher Form.

Folgende Publikationen sind in der Reihe zuletzt erschienen:

	<b>Geldanlage in Wertpapieren</b> Informationen für Privatkunden	Berlin, Dezember 2010
	<b>IBAN</b> Einfach bezahlen mit IBAN und BIC	Berlin, November 2010
	<b>Was Banken leisten</b> Kapitalgeber und Dienstleister für Wirtschaft und Gesellschaft	Berlin, Oktober 2010
	<b>Private Immobilienfinanzierung</b> Informationen für Privatkunden	Berlin, Oktober 2010
	<b>Ombudsmann der privaten Banken</b> Tätigkeitsbericht 2009	Berlin, August 2010
	<b>Neue Regeln für Verbraucherkredite</b> Was ändert sich für Bankkunden?	Berlin, Juni 2010
	<b>Einlagensicherung der privaten Banken</b> Informationen für Privatkunden	Berlin, Mai 2010
	<b>Ombudsmann der privaten Banken</b> Fragen und Antworten	Berlin, April 2010
	<b>SEPA</b> Einfach bezahlen in Europa	Berlin, April 2010
	<b>Vorsorgevollmacht – frühzeitig für Notfälle Bankangelegenheiten regeln</b> Fragen und Antworten	Berlin, Februar 2010
	<b>Das Girokonto für Privatkunden</b> Der Schlüssel zu Bankdienstleistungen	Berlin, Dezember 2009

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

Die wichtigsten Tipps für Sie zum Mitnehmen:

## Online Banking – bequem und sicher

- Geben Sie immer nur eine TAN zur Freigabe eines Auftrags ein.
- Prüfen Sie regelmäßig Ihre Kontoumsätze.
- Halten Sie Ihren Rechner stets sauber und aktuell.

fokus:verbraucher



## ONLINE BANKING – BEQUEM UND SICHER

---

Berlin, Februar 2011

**HERAUSGEBER** Bundesverband deutscher Banken  
Postfach 040307, 10062 Berlin  
Telefon (030) 1663-0  
Telefax (030) 1663-1399

**GESTALTUNG** Manfred Makowski

**Foto** fotolia

© 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)