



# Tipps zum sicheren Online-Banking

Der finanzielle Schaden bei einem ungenügend gesicherten Online-Konto geht schnell in die Tausende. So sichern Sie Ihre Bankgeschäfte im Internet und schützen sich vor Trickbetrüchern.

Mehr als 24 Millionen Deutsche stehen im Visier krimineller Banden, die sich mit gefälschten Mails, manipulierten Webseiten und ausgefeilten Trojanern auf das Stehlen von Kontodaten und das Fälschen von Überweisungen spezialisiert haben. 24 Millionen Menschen, das sind 38 Prozent aller Bundesbürger zwischen 16 und 74 Jahren, die laut einer Untersuchung des IT-Verbands Bitkom Online-Banking im Jahr 2008 genutzt haben.

Besonders Banking-Trojaner werden immer raffinierter und gefährlicher. Beispielsweise soll der im November

2008 aufgespürte Banking-Trojaner Sinowal rund 2700 Webseiten von Geldinstituten kennen. Besucht ein Anwender eine dieser Seiten auf einem mit Si-

nowal infizierten PC, dann manipuliert der Schädling die Seite heimlich und klaut die Kundendaten des Surfers.


Win32.Banker.ohq geht noch weiter. Der Banking-Trojaner tauscht die Originalseite gegen eine Kopie aus, auf welcher der Surfer seine Transaktion ausführt. Derweil loggt sich Win32.Banker.ohq unsichtbar auf der Originalseite ein und verwendet die eingegebenen Daten, um damit eine eigene Überweisung durchzuführen.

Der Artikel gibt zehn Tipps, mit denen Sie Online-Banking sicher und vor Schädlingen geschützt durchführen.

## Kompakt

- Führen Sie Ihre Online-Geschäfte nur über mit SSL verschlüsselte Verbindungen durch.
- Eine TAN benötigen Sie niemals bereits beim Einloggen.
- Ein PC in einem Internetcafé ist zu unsicher für Online-Banking.

Alle dafür erforderlichen Programme sind kostenlos. Sie finden sie auf Heft-CD und -DVD oder zum Download im Internet.

Neben diesen Tipps benötigen Sie in jedem Fall einen aktuellen Virens scanner – beispielsweise Avast Home Edition 4.8 (kostenlos, [www.avast.com](http://www.avast.com) und auf ) – und eine leistungsfähige Firewall, wie sie in allen aktuellen DSL-Routern enthalten ist.

Aktivieren Sie außerdem unbedingt die automatischen Windows-Updates und aktualisieren Sie regelmäßig alle Anwendungen, die mit dem Internet Kontakt aufnehmen, wie Browser, Mail-Programm und Plug-ins wie Adobe Flash und Adobe Reader.

Eine Übersicht über die verschiedenen TAN-Verfahren, welche die Banken mittlerweile anbieten, finden Sie im Artikel „TAN, eTAN, mTAN – was wirklich sicher ist“ ab Seite 96.

## Die Tricks der Betrüger

Gefälschte Mails und Webseiten sehen zwar täuschend echt aus, enthalten aber doch meist sprachliche Fehler. Bei manchen Fälschungen ist sogar sofort klar, dass es sich um einen Betrugsversuch handelt: Eine Originalseite fordert niemals bereits beim Einloggen eine Transaktionsnummer (TAN) von Ihnen.

### 1. Phishing-Mails


Phishing-Mails lassen sich relativ leicht erkennen: Zum einen schicken die wenigsten Finanzinstitute ihren Kunden schlecht formulierte Mails, in denen diese auf einen Link klicken sollen, um etwa ihre Kontodaten zu überprüfen oder dubiose Formulare auszufüllen.

Außerdem enthalten Phishing-Mails nie eine persönliche Anrede, weil der Spamversender nur Ihre E-Mail-Adresse kennt (Bild A). Dank des eingebau-

## Inhalt

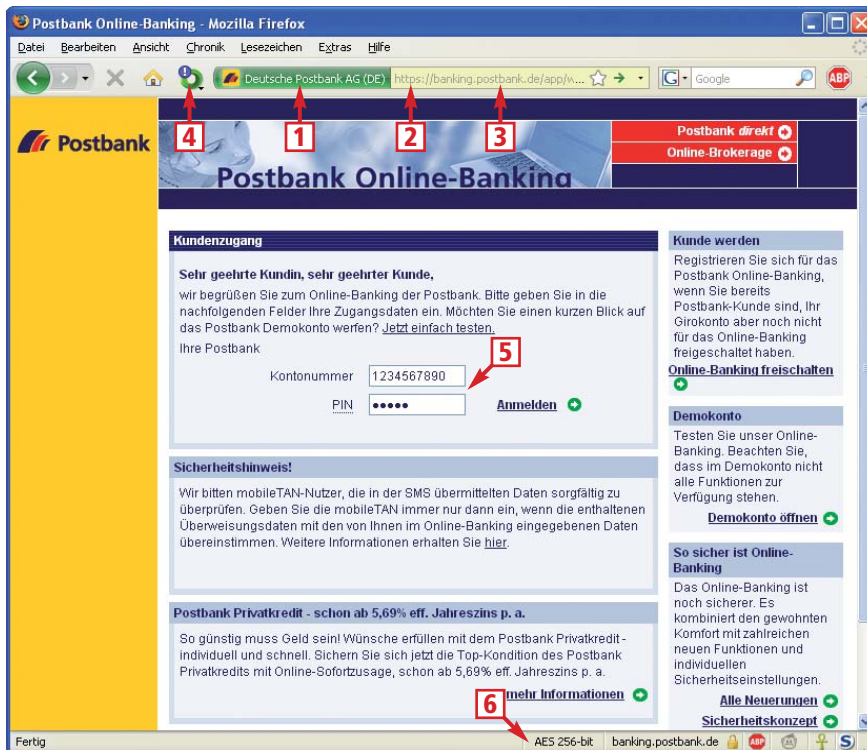
### Tipps zum sicheren Online-Banking

■ <b>Die Tricks der Betrüger</b>	
1. Phishing-Mails	5.89
2. Phishing-Webseiten	5.90
3. Vorsicht bei TANs	5.90
■ <b>Sicheres Online-Banking</b>	
4. Sichere Browserverbindungen	5.90
5. Verschlüsselung checken	5.92
6. SSL-Zertifikat überprüfen	5.92
■ <b>Profi-Tipps</b>	
7. Schutz vor Pharming	5.92
8. Firefox absichern	5.93
9. Online-Banking unterwegs	5.93
10. Online-Banking mit Ubuntu	5.94
Online-Banking: So erkennen Sie die Originalseite Ihrer Bank	5.89
Software-Übersicht	5.90

ten Spamfilters erkennt Thunderbird 2.0.0.21 (kostenlos, [www.mozilla-europe.org/de/products/thunderbird](http://www.mozilla-europe.org/de/products/thunderbird) und auf ) viele Phishing-Mails bereits beim Empfang und sortiert diese aus. ▶

## Online-Banking: So erkennen Sie die Originalseite Ihrer Bank

Nur wenn Sie Ihre Bankgeschäfte verschlüsselt durchführen und zusätzliche Browser-Add-ons einsetzen, sind Sie sicher vor Lausangriffen. An folgenden Merkmalen erkennen Sie in Firefox, ob eine Verbindung sicher ist.



### 1 Zertifikat

Der große grüne Button beweist, dass das SSL-Zertifikat für die Deutsche Postbank AG ausgestellt wurde.

### 2 SSL-Verschlüsselung

Die Internetadressen von verschlüsselten Webseiten beginnen immer mit „https://“.

### 3 Gelbe Adressleiste

Das Add-on Old Location Bar 1.3 färbt bei verschlüsselten Verbindungen die Adressleiste zusätzlich gelb, wie es in Firefox 2 standardmäßig der Fall war.

### 4 Web of Trust

Die Erweiterung blendet einen Button ein, der in Ampelfarben zeigt, ob die Seite vertrauenswürdig ist oder nicht.

### 5 Kontonummer und PIN


Wenn bereits beim Einloggen zusätzlich eine TAN verlangt wird, handelt es sich um eine Phishing-Seite.

### 6 AES 256-bit

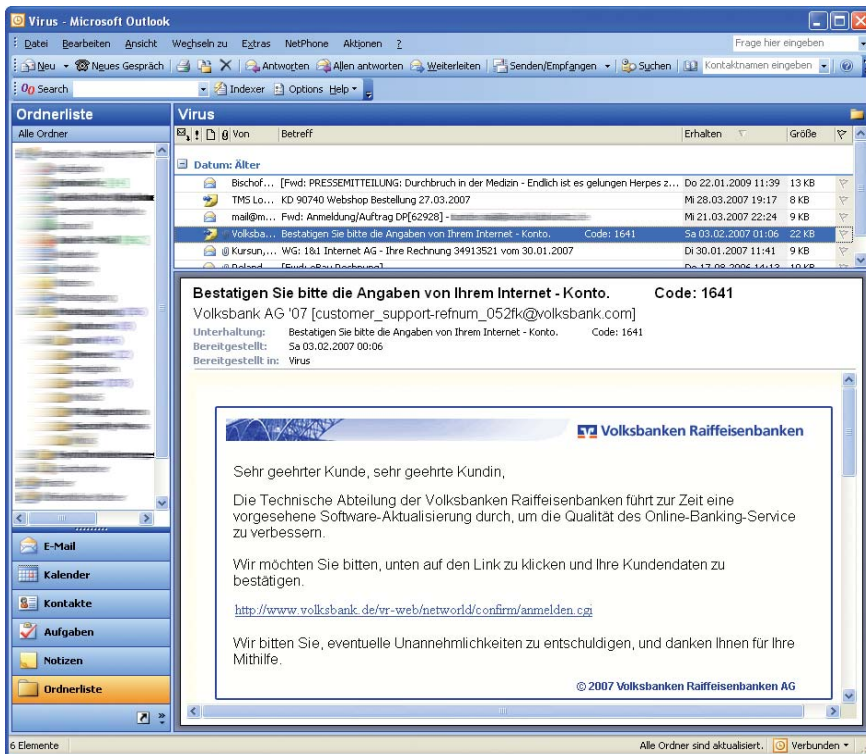
Das Add-on Cipherfox 1.77 zeigt den aktiven Verschlüsselungsstandard an.

## 2. Phishing-Webseiten

Sowohl Firefox als auch der Internet Explorer verfügen über eingebaute Phishing-Filter, die jede besuchte Webseite mit einer Datenbank gefährlicher Adressen vergleichen und gegebenenfalls vor dem Besuch der Seite warnen.






Jede dieser Datenbanken ist jedoch nur so gut wie das darin enthaltene Datenmaterial. Zusätzlichen Schutz bietet das Add-on Web of Trust 20090325 (kostenlos, [www.mywot.com/de](http://www.mywot.com/de) und auf ) , das es in einer Version für Firefox und einer für den Internet Explorer gibt.


Web of Trust basiert auf einem Community-Gedanken: Jeder Nutzer, der eine neue gefährliche Webseite entdeckt, markiert diese mit wenigen Klicks. Spätere Besucher warnt Web of Trust dann, indem sich der Button der Erweiterung rechts neben der Adressleiste rot färbt. Liegen noch zu wenige Bewertungen vor, zeigt dieser Button entweder ein Fragezeichen an oder er ist gelb. Noch wichtiger ist die Farbe Grün: Sie zeigt an, dass Sie sich auf einer seriösen Seite befinden.



**Phishing-Mail:** Diese gefälschte Mail erkennen Sie an kleinen sprachlichen Fehlern und daran, dass Ihr Name in der Anrede fehlt (Bild A)

## Software-Übersicht

Programm	Quelle	Seite
 Adblock Plus 1.0.2 (Werbeblocker)	<a href="https://addons.mozilla.org/de/firefox/addon/1865">https://addons.mozilla.org/de/firefox/addon/1865</a>	93
 Avast Home Edition 4.8 (Virenschanner)	<a href="http://www.avast.com">www.avast.com</a>	89
 Cipherfox 1.77 (Optimiert Verschlüsselung)	<a href="https://addons.mozilla.org/de/firefox/addon/8919">https://addons.mozilla.org/de/firefox/addon/8919</a>	92
 Firefox 3.0.10 (Browser)	<a href="http://www.mozilla-europe.org/de/firefox">www.mozilla-europe.org/de/firefox</a>	93
 Imgburn 2.4.4.0 (Brennprogramm)	<a href="http://www.imgburn.com">www.imgburn.com</a>	94
 Noscript 1.9.2.6 (Javascript-Blocker)	<a href="http://www.noscript.net">www.noscript.net</a>	93
 Old Location Bar 1.3 (Optimiert Verschlüsselung)	<a href="https://addons.mozilla.org/de/firefox/addon/7637">https://addons.mozilla.org/de/firefox/addon/7637</a>	90
 Thunderbird 2.0.0.21 (Mail-Programm)	<a href="http://www.mozilla-europe.org/de/products/thunderbird">www.mozilla-europe.org/de/products/thunderbird</a>	89
 Ubuntu 9.04 Desktop-Edition (ISO-Datei)	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	94
 Web of Trust 20090325 (Anti-Phishing)	<a href="http://www.mywot.com/de">www.mywot.com/de</a>	90

Alle  -Programme finden Sie auf Heft-CD und -DVD in der Rubrik „Internet, Online-Banking“, Ubuntu 9.04 finden Sie nur auf Heft-DVD.

## 3. Vorsicht bei TANs

Wenn Sie bereits beim Einloggen in Ihr Online-Konto nach einer TAN gefragt werden, befinden Sie sich auf einer gefälschten Seite (Bild B). TANs benötigen Sie nur, um etwa Überweisungen freizugeben, aber nie beim Einloggen. Dafür haben Sie Ihre Zugangsdaten, meist die Kontonummer und Ihre PIN.


## Sicheres Online-Banking

Nutzen Sie Online-Banking nur, wenn die Verbindung zwischen Ihrem Computer und Ihrer Bank verschlüsselt ist. Im Zweifelsfall überprüfen Sie das SSL-Zertifikat Ihrer Bank.

## 4. Sichere Browserverbindungen

Normalerweise werden alle Daten beim Surfen im Klartext übertragen. Damit jedoch niemand die Kommunikation zwischen Internetnutzer und Online-Bank belauscht, verschlüsseln alle Finanzinstitute die Verbindung.

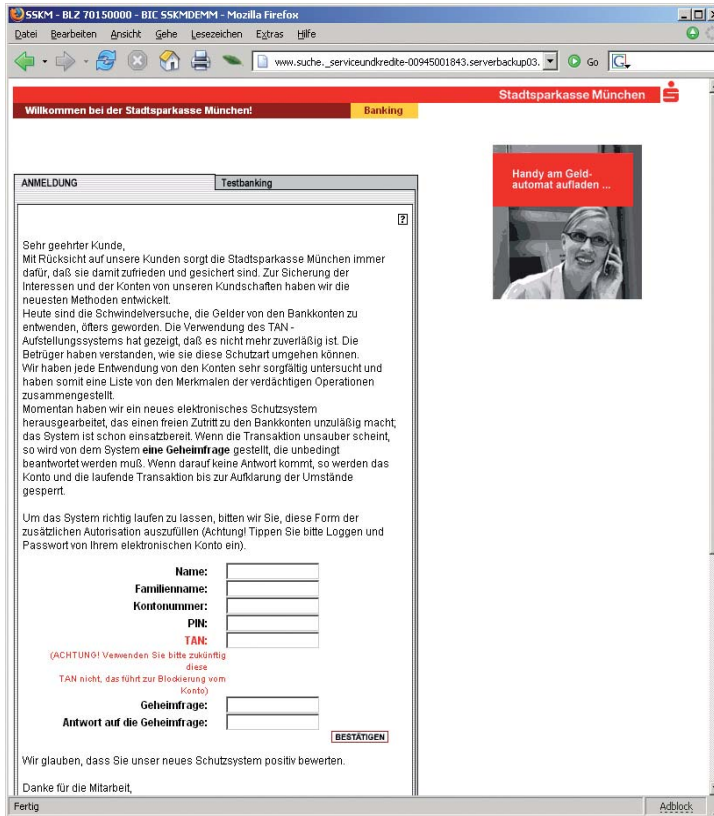
Die Verschlüsselung schützt nicht nur die übertragenen Daten. Durch das dabei verwendete Zertifikat garantiert Ihnen Ihre Bank auch, dass Sie sich auf der richtigen Seite befinden. Wenn Ihnen Ihr Browser keine erfolgreiche Verschlüsselung der Verbindung anzeigt, brechen Sie den Vorgang sofort ab.

Bei IE und Firefox zeigt ein geschlossenes gelbes Schloss unten rechts in der Statusleiste eine erfolgreiche Verschlüsselung an. Firefox ab Version 3 zeigt zusätzlich neben dem Adressfeld den zertifizierten Namen des Betreibers der aktuellen Seite grün hinterlegt an. Die Erweiterung Old Location Bar 1.3 (kostenlos, <https://addons.mozilla.org/de/firefox/addon/7637> und auf ) färbt außerdem die übrige Adressleiste wieder gelb ein wie in Firefox 2. ▶

## 5. Verschlüsselung checken

Einige Banken und Webseiten verwenden den nicht mehr zeitgemäßen Verschlüsselungsstandard RC4. Die Erweiterung Cipherfox 1.77 (kostenlos, <https://addons.mozilla.org/en-US/firefox/addon/8919> und auf deaktiviert RC4 und zwingt die Bank so dazu, einen sichereren Standard wie AES 256 Bit zu verwenden (Bild C). Zudem zeigt das Add-on unten rechts den aktuell verwendeten Verschlüsselungsstandard an.

Rufen Sie eine verschlüsselte Seite auf, beispielsweise die Ihrer Bank, und klicken Sie unten rechts doppelt auf die Angabe zur Verschlüsselung, etwa „AES 256-bit“. Setzen Sie danach je ein Häkchen vor allen angebotenen Optionen. Sie deaktivieren damit RC4 und aktivieren eine Anzeige, die

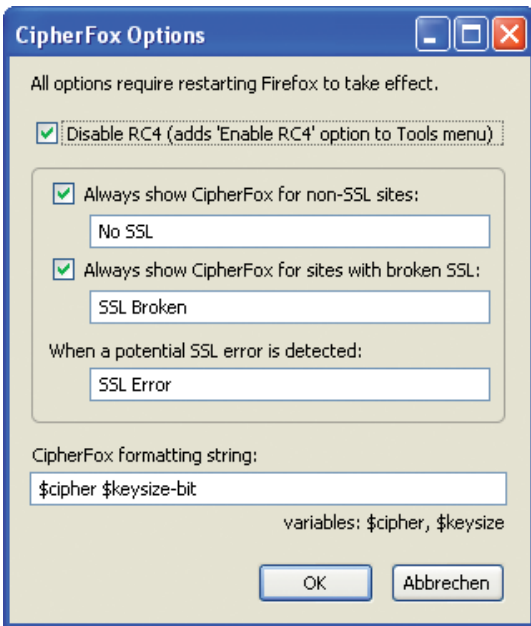


**Vorsicht bei TANs:** Diese Seite fordert gleich beim Einloggen zur Eingabe einer TAN auf. Das ist ein sicheres Indiz dafür, dass hier Fälscher am Werk sind (Bild B)

Sie warnt, wenn eine Seite kein SSL verwendet oder das Zertifikat beschädigt ist.

öffentlich, dann können Sie damit zusätzlich die Echtheit des Zertifikats und damit die Echtheit einer besuchten Webseite prüfen. Postbank-Kunden zum Beispiel finden den SHA1-Wert unter [www.postbank.de/privatkunden/pk\\_banking\\_postbank\\_de.html](http://www.postbank.de/privatkunden/pk_banking_postbank_de.html).

Rufen Sie eine verschlüsselte Seite Ihrer Bank auf und klicken Sie doppelt auf das gelbe Schloss-Icon, um das Infofenster über das Zertifikat zu öffnen. Firefox wechselt daraufhin zum Reiter „Sicherheit“. Klicken Sie dort auf „Zertifikat anzeigen“. Sie sehen in der vorletzten Zeile den „SHA1-Fingerabdruck“ (Bild D). Beim Internet Explorer findet sich der SHA1-Wert hinter „Fingerabdruck“ auf dem Reiter „Details“.



**Cipherfox 1.77:** „Disable RC4“ zwingt Webseiten, auf RC4 zu verzichten und den sichereren Standard AES 256 Bit zu nutzen (Bild C)

## 6. SSL-Zertifikat überprüfen

Firefox ab Version 3 und der Internet Explorer ab Version 7 unterstützen die neuen Extended-Validation-Zertifikate, die Zertifikate mit erweiterter Überprüfung. Bei diesen Zertifikaten hebt Firefox den Namen des Antragstellers, also den Ihrer Online-Bank, deutlich in Grün hervor. Beim Internet Explorer erhalten Sie mit einem Klick auf das gelbe Schlosszeichen mehr Informationen über das Zertifikat.

Wenn Ihre Bank auf ihren Support-Seiten im Internet den SHA1-Fingerabdruck (Secure Hash Algorithm) ver-

## Profi-Tipps

Ein Restrisiko besteht unter Windows immer, wenn Sie Online-Banking nutzen wollen. So kann ein eingeschleuster Banking-Trojaner beispielsweise die lokale Hosts-Datei manipulieren und Sie beim Besuch der Webseite Ihrer Bank auf eine gefälschte Seite locken. Wem dieses Restrisiko zu hoch ist, der bootet seinen PC von einer Ubuntu-Live-CD und gibt Windows-Schädlingen so keine Chance (siehe Tipp 10).

## 7. Schutz vor Pharming

Pharming ist eine Betrugsmethode, bei der die Betrüger die Aufschlüsselung der Internetadresse auf Ihrem PC manipulieren.

Jedes Mal, wenn Sie eine URL eintippen, sieht das Betriebssystem zuerst in der Hosts-Datei auf Ihrem lokalen PC nach, ob für diese URL eine IP-Adresse hinterlegt ist. Falls ja, steuert



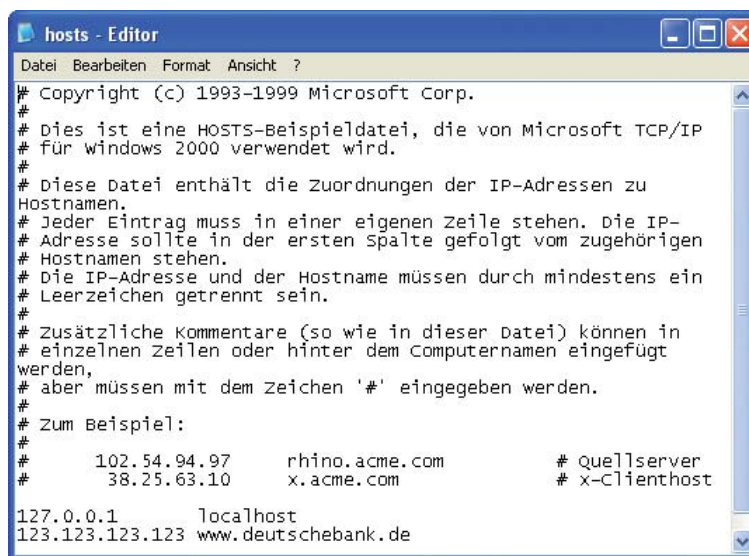
**Zertifikate-Ansicht:** Wenn der SHA1-Fingerabdruck in der vorletzten Zeile des Infofensters zum Zertifikat mit den offiziellen Angaben Ihrer Bank übereinstimmt, ist die besuchte Seite echt (Bild D)

der Browser diese IP-Adresse an. Wenn nicht, fragt er beim DNS-Server (Domain Name System) Ihres Providers nach der richtigen IP-Adresse.

Haben Betrüger erst einmal einen Trojaner auf einem PC eingeschleust, ist es für sie ein Leichtes, die lokale Hosts-Datei zu verändern. Indem sie gefälschte IP-Adressen für die wichtigsten Online-Banken eintragen, leiten sie die Surfer so auf gefälschte Seiten (Bild E). Das Fatale daran ist: Der Browser zeigt weiterhin die scheinbar korrekte Adresse an, allerdings verfügt die gefälschte Seite über kein SSL-Zertifikat wie die Originalseite. Wie Sie die Verschlüsselung und das Zertifikat überprüfen, le-

sen Sie in den Tipps „5. Verschlüsselung checken“ und „6. SSL-Zertifikat überprüfen“.

Versehen Sie die Hosts-Datei mit einem Schreibschutz, so dass Kriminelle



**Hosts-Datei überprüfen:** Der unterste Eintrag bedeutet, dass der Browser beim Besuch von www.deutschebank.de auf die IP-Adresse 123.123.123.123 umgeleitet wird (Bild E)

sie nicht mehr manipulieren können. Rufen Sie dazu unter Windows XP den Windows-Explorer auf, wechseln Sie in das Verzeichnis „C:\WINDOWS\system32\drivers\etc“ und klicken Sie mit der rechten Maustaste auf „hosts“. Wählen Sie im Kontextmenü „Eigenschaften“ und setzen Sie einen Haken vor „Schreibgeschützt“. Unter Vista wird die Datei bereits vom Betriebssystem geschützt und lässt sich nur mit Administratorrechten ändern.

### 8. Firefox absichern

Neben verseuchten Mails ist der Browser eine der wichtigsten Eintrittspforten für Schädlinge. Sicherheitsexperten nennen diese Gefahr Drive-by-Downloads. Dabei genügt teilweise sogar der Besuch einer seriösen Seite, um den eigenen PC mit einem Trojaner zu infizieren.

Die Kriminellen verwenden dazu manipulierte Banner, die gezielt Sicherheitslücken im Browser und in Flash auszunutzen versuchen. Halten Sie diese Anwendungen deswegen immer auf dem aktuellen Stand. Installieren Sie außerdem die beiden Firefox-Erweiterungen Adblock Plus 1.0.2 (kostenlos, <https://addons.mozilla.org/de/firefox/addon/1865> und auf ) sowie Noscript 1.9.2.6 (kostenlos, [www.noscript.net](http://www.noscript.net) und auf ). Das erstgenannte Add-on entfernt sämtliche Werbe-Banner, während letzteres Javascript nur noch auf ausgewählten Seiten zulässt (Bild F).


### 9. Online-Banking unterwegs

Verzichten Sie auf Online-Banking an einem öffentlichen Computer, beispielsweise in einem Internetcafé. Selbst wenn die Verbindung verschlüsselt ist, so kann trotzdem ein verborgener Keylogger auf dem ▶

Computer installiert sein. Dieser schneidet sämtliche Tastatureingaben inklusive Ihrer Kontonummer und Ihrer PIN mit.

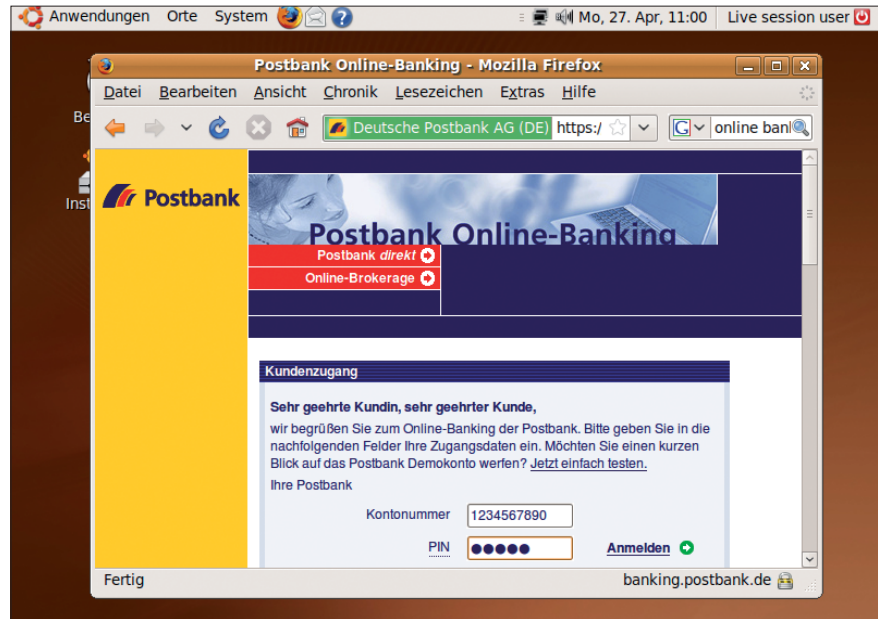
Sofern Sie jedoch mit Ihrem eigenen Notebook unterwegs sind, spricht nichts gegen Online-Banking zum Beispiel über ein öffentliches WLAN. Dank der Verschlüsselung der Verbindung durch Ihre Bank kann Ihre Transaktion selbst über eine unverschlüsselte Funkverbindung nicht geknackt werden.

### 10. Online-Banking mit Ubuntu

Die neue Ubuntu 9.4 Desktop-Edition (kostenlos, [www.ubuntu.com](http://www.ubuntu.com) und auf ) ist ideal, um Ihre Bankgeschäfte in einer vor Windows-Trojanern gesicherten Linux-Umgebung zu erledigen (Bild G).

Brennen Sie die ISO-Datei von der Heft-DVD als bootfähige CD. Wenn Sie über kein geeignetes Brennprogramm verfügen, installieren Sie dazu Imgburn 2.4.4.0 (kostenlos, [www.imgburn.com](http://www.imgburn.com) und auf )

Booten Sie nach dem Brennen von der neuen Ubuntu-CD. Eventuell müssen Sie im BIOS Ihres Computers die Boot-Reihenfolge ändern. Meist öffnen Sie das BIOS, indem Sie direkt nach



**Online-Banking unter Ubuntu:** Booten Sie Ihren PC von einer Live-CD, um Ihre Bankgeschäfte vor Windows-Trojanern zu schützen (Bild G)

dem Einschalten des Computers eine der Tasten [Entf], [F1] oder [F2] drücken.

Wählen Sie zuerst die Sprache aus, in der Ubuntu starten soll. Belassen Sie danach die Auswahl auf „Ubuntu ausprobieren (Rechner bleibt unverändert)“ und drücken Sie zur Bestätigung die Eingabetaste. Nachdem Ubuntu gebootet ist, klicken Sie auf das Firefox-

Icon in der oberen Statusleiste, um den Browser zu starten. Sofern Sie über einen DSL-Router mit aktiviertem DHCP-Server verfügen, sollte das Linux-System automatisch sofort mit dem Internet verbunden sein.

Führen Sie jetzt Ihre Bankgeschäfte durch. Achten Sie aber auch hier darauf, dass die Seite Ihrer Bank eine verschlüsselte Übertragung verwendet und das korrekte SSL-Zertifikat anzeigt. Sobald Sie alle Transaktionen erledigt haben, fahren Sie das System herunter, indem Sie oben rechts auf den roten Button klicken und „Ausschalten ...“ auswählen. Entfernen Sie nun die Ubuntu-CD, bevor Sie Ihren Computer wieder neu starten. Ihr PC würde sonst jedes Mal von der Live-CD booten. ■

Andreas Th. Fischer  
internet@com-magazin.de



**NoScript 1.9.2.6:** Das Add-on erlaubt Javascript nur auf ausgewählten Webseiten (Bild F)

#### Weitere Infos

- <http://de.wikipedia.org/wiki/Transaktionsnummer>
- Hintergrundinfos zu TANs
- [www.com-magazin.de/tipps/1349](http://www.com-magazin.de/tipps/1349)
- Wie man ein sicheres Passwort erstellt