bankenverband
BUNDESVERBAND DEUTSCHER BANKEN

ONLINE BANKING SECURITY

Seventh revised edition

Information for online banking users

Berlin, November 2007

fokus:verbraucher

Information for Consumers
from the German Private Banks

Introduction

While the internet offers enormous advantages and opportunities, it also presents various security risks. With this in mind, banks take extensive steps to protect the information transmitted and processed when banking online. This includes, for example, ensuring that confidential data sent over the internet cannot be accessed or modified by unauthorised third parties.

But the banks normally have no influence over the systems used by their customers. The choice is entirely up to them. Moreover, the system selected – a PC connected to the internet, for example – will usually be used for a number of other applications as well.

The systems used by online banking customers are therefore exposed to risks beyond the banks' control. For this reason, the banks cannot assume liability for them.

Typical dangers faced when using the internet

are third parties accessing, deleting or tampering with data while it is being transmitted or obtaining information under false pretences. This may be achieved with the help of

- viruses and worms: programmes that self-replicate or are sent over the internet by e-mail and can damage your PC;
- Trojans: programmes that, unbeknown to the user, compromise computer security by intercepting passwords, for example;
- phishing: using a false name, website or address for fraudulent purposes;
- pharming: redirecting users to a fraudulent server;
- rootkits: malicious software giving unauthorised administrator-level access without the real administrator noticing; they share certain features with trojans;
- hacking: unauthorised access to a PC via the internet.

The banks have a number of measures in place that offer effective protection against attacks when information is sent over the internet or processed by the bank's server.

What can customers do?

To ensure that the banks' security measures cannot be undermined by manipulation, it is essential that customers, too, take steps to protect the system they use. These include being security-conscious when using the internet and checking bank statements regularly.

Naturally, dangers are not lurking everywhere in cyberspace. Not everyone online bankers come into contact with wants to, or will, do them harm. Just by following the ten rules outlined below, customers can significantly improve the security of their PC and reduce the risks of using the internet to an absolute minimum.

Should customers nevertheless suspect that they have come across internet fraudsters, they should ensure that access to their online account is blocked immediately and report any irregularities to their bank without delay. All relevant information should be saved so that the attempt at fraud can be traced. This means that the hard drive should not be formatted immediately.

It is highly important for people who use computers to maintain backup files regardless of whether or not they bank online. It is usually extremely difficult, if not impossible, to salvage data once it has been deleted or corrupted. A convenient way of **making backups** is to save the data on a removable hard drive, a CD or DVD writer. Whatever method is chosen, it is essential to save revised or new data **on a regular basis**.

Security rules

Rule 1 Install security software (including an up-to-date virus scanner)

Install additional security software. Some security problems cannot be solved with your operating system's standard tools alone. An important additional tool is an efficient virus scanner that is continuously updated online and thus able to detect new viruses. New viruses are being discovered almost every day and it is quite possible to become infected while surfing the net.

Remember that, as long as you are online, third parties can build up a picture of what information is on your PC because your computer has its own address on the web and can thus be accessed from outside.

If you do not have adequate security in place, you run the risk of unauthorised persons gaining access to data (e.g. PINs and TANs, which, incidentally, should never be saved) by means of surreptitiously installed **spyware** applications. These can gather sensitive data without your knowledge, such as account information and passwords, or even record your keystrokes. The data is then sent to an unknown e-mail address or server. Spyware programmes may be hidden in internet pages, e-mails or e-mail attachments and are therefore sometimes also called **Trojan horses**. Malicious software which particularly targets core functions of the operating system is also known as rootkit; the dividing line between the two is blurred. As soon as an infected programme is opened, the spyware will install itself on your computer without your knowledge. So delete suspicious e-mails without opening them. Don't

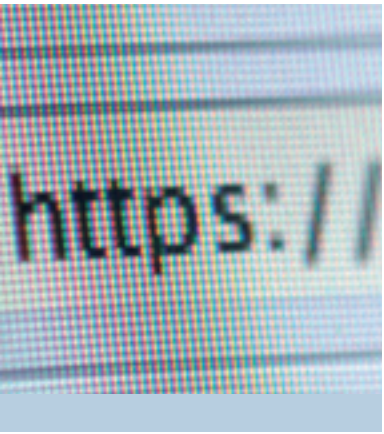
open any suspicious attachments, even if they appear to come from a familiar address. Deactivate your e-mail client's auto-preview function to avoid e-mails being opened automatically.

A **personal firewall** can protect you from such attacks. A firewall is a programme that monitors all incoming and outgoing traffic between your PC and the internet and permits only familiar or authorised connections.

Computer stores also offer a wide range of other programmes that can help to improve the security of your PC, such as access protection and encryption devices.

Keep abreast of any new security threats on the internet and of the steps you can take to protect yourself from them. You will find information about banking online safely on your bank's website.

Rule 2 Protect sensitive data when sending it over open networks



Any unsecured transmission of data over the internet may be intercepted or viewed by unauthorised third parties.

The banks have taken steps to ensure that data sent when banking online is encrypted before transmission. Enter your PIN and other access codes only when you are sure that you are on your **bank's secure pages** and have an encrypted connection. One of the ways you can verify this is by checking that the internet address (URL) of your bank starts with "https://".

Don't forget that data transmitted during online banking sessions is not automatically encrypted when it is saved on your PC and should therefore be protected by further security measures.

As a general rule, never send sensitive information over open networks unless it is encrypted. Protect your confidential correspondence by using approved encryption methods, many of which are available free of charge.

Rule 3 Be sure you know who you are dealing with

Not everyone on the internet is who they claim to be. It is comparatively easy for an expert to forge an e-mail address or even fake a whole website – that of the bank you use to bank online, for instance.

Check the URL in the address box of the browser and make sure your bank's internet address is correctly spelled. The tiniest discrepancies may be a sign that the site is fake.

Check, too, the security information provided by the browser, such as the results of **certificate verification**. This allows, among other things, the credentials of the server to which you are connected to be confirmed by an independent authority – the certificate issuer. Make sure the name of the internet site indicated on the security certificate matches the name of the site on your screen.

You should not trust an address if the (apparent) owner is also the issuer of the certificate. The certificate should be from a reputable certificate authority and should be valid. If in doubt, ask your bank for information about trustworthy certification authorities which issue server certificates for the online banking service you use.

You should divulge information only if you are certain who is receiving it and what will happen to it. Be suspicious of any departure from the usual routine, such as a request to enter your PIN or TAN at a time you don't expect.

A favourite trick of hackers is to obtain the information they need by impersonating someone in a position of trust. In a scam known as **phishing** ("password fishing"), for example, you will be asked by the fraudsters to update or re-enter confidential access codes (such as your PIN or TANs) on the website of your bank. You may receive such a request by e-mail or via manipulated internet pages. But the link will take you to a bogus website created by the phisher, who will then be able to capture your confidential codes. So it is very important to verify that you are entering your confidential access codes on your bank's genuine website. One way to make sure of this is to enter your bank's internet address manually in the address bar of your browser. Be sure to look out for anything unusual when you are banking online, such as differences in the appearance of your bank's website.

Pharming is another technique used to steal confidential access codes. It works by redirecting users to a rogue server. Malicious software forges the domain name resolution of the host file on your PC or attempts to manipulate the DNS server responsible for the domain name resolutions. Prevent these attacks by installing up-to-date antivirus software and a personal firewall. In addition, make sure that the site you have called up has a valid certificate.

Rule 4 Be careful with sensitive data and access media

Protect your access codes and **access media** (e.g. PINs, chip cards) from unauthorised use. Never enter confidential access data on a site other than that of your bank or divulge it to a third party in any way. When shopping online, for instance, you shouldn't enter your online banking access data on either the shopping website or the site of an online money transfer service.

Don't store **sensitive data** (passwords, PINs, access codes, credit card numbers) on your hard drive. If the PC is not used by you alone (your computer at work, for instance), this could otherwise enable third parties to view the information. In addition, spyware applications that have managed to access your computer might be able to capture your data and send it on by e-mail, for example. If you use security-enhancing equipment such as a chip card reader with a PIN keypad, make sure you enter your confidential codes only when requested to do so by the device.

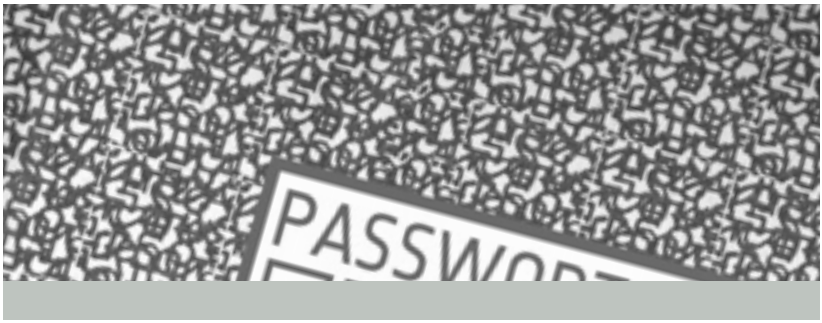
Above all, don't store your password for dialling into the internet. This will help to protect you from unwanted connections.

Before entering personal access data such as your PIN, always make sure that the recipient is really your bank. Your bank would never contact you by e-mail or telephone and ask for your PIN or other access codes, for example. Nor would it request several TANs at the same time. Never enter one or more TANs unless you have first issued an instruction to your bank. Don't answer suspicious e-mails or ollow any instructions of this kind, even if you are advised that failure to do so may result in your account being blocked. Inform your bank about the attempted fraud.

Rule 5 Choose a secure password

If you want to use your PC to start an application like online banking, you normally have to begin by entering a password. This enables you to prove who you are and show that you are authorised to work on a particular computer or with a particular application. So it is vitally important not to share this information with anyone. It also means that you shouldn't write it down anywhere and that your password should be unique and difficult to guess.

A good password is usually six to eight characters long and a combination of upper and lower-case letters, numbers and special symbols. When banking online in Germany, the desired level of security is achieved by means of your PIN and a TAN (transaction number, a one-time password used to authorise the transaction). Avoid proper names, familiar terms (i.e. terms which can be found in a dictionary), repetitions of single characters (e.g. AAAAAA) or keyboard patterns (e.g. qwerty). Don't use your own date of birth or that of anyone you know. There are various strategies for selecting a combination that is difficult to guess: a simple method is to create a password from the first letters of a saying or a poem. Adding special symbols or numbers can add further complexity. "2hRbt1" might stand for "two heads are better than one", for example. Change your password if you have reason to suspect someone may have discovered it.



Rule 6 Only use programmes from a trustworthy source

Don't download programmes from the internet onto your hard drive unless you can be sure the source is reliable. Verify the identity of the provider. **Viruses or Trojan** horses may be introduced by downloading programmes or opening an e-mail attachment. Don't open an attachment if you don't know who it is from or what is in it. First save the contents, then check it with a security programme before opening. Think carefully about whether to install audio or 3-D plug-ins on your browser since these can also pose uncontrollable security risks.

Rule 7 Use up-to-date programme versions

Use only an up-to-date version of your preferred internet browser and PC operating system. Only in the most recent versions will all known security holes have been filled.

Software manufacturers also develop small programmes known as **bug fixes or patches** to solve security problems they have discovered. You should install these bug fixes or patches as soon as possible to protect your PC from known vulnerabilities. Keep abreast of the latest developments: most manufacturers operate information services for this purpose.

Rule 8 Run a security check on your PC

Before you use your PC to bank online, take a few minutes to run a personal security check. Activate the security features that protect your computer from unauthorised access. These include, for example, the password that the operating system or screensaver asks you to enter when you start your PC.

In general, you should never surf the internet with administrator privileges. Use only **minimal user rights** when you are online. This makes manipulation and unauthorised access more difficult.

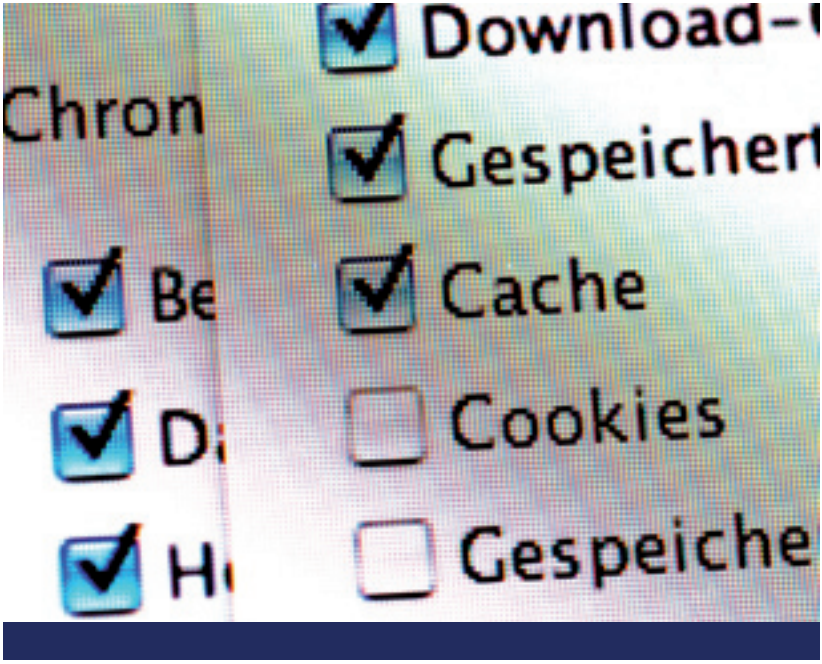
Bear in mind that if a PC is not used by you alone – as is the case in an internet café, for example – you can never know to what extent access is protected by up-to-date security software or exactly what programmes are being run. It is even possible that the keyboard has been tampered with. You cannot expect proper security in this environment. For this reason, it is not a good idea to do your online banking from such places.

Rule 9 Activate the browser's security settings

Activate the security settings of your internet browser. You can enhance your security on the internet considerably just by making intelligent use of your browser's security options.

It is especially important for you to **block ActiveX Controls** and allow Java applets to be run only after confirmation. These are small, independent, active content programmes that are run on your PC and can, in certain circumstances, trigger undesired actions (such as e-mailing your password to a third party). Don't use your browser's auto-completion function, which saves any user names and passwords you enter and suggests matches.

Cookies store information in a special file on your hard drive, but do not search for any other data. If in doubt, decide against permitting a website to write information onto your hard drive because this can later be used to create a user profile. Yet rejecting cookies as a matter of course is not always the best strategy. If you reject a cookie, you may be unable to use some websites. If you accept it, the web server will recognise you every time you return to the site. This enables the server to build up a "file" and create a user profile. It records details such as which search terms you use and which pages you visit. Once your preferences and interests are known, targeted advertising banners can be placed. Special security software can prevent user profiles from being compiled, however. This allows you to enjoy the benefits of cookies while preventing unauthorised third parties from tracking your behaviour for unwanted purposes.



Rule 10 Don't make your current account available for fraudulent financial transactions

Fraudsters are currently using websites and e-mails to try to recruit bank account holders in Germany as "financial agents". The financial agents are required to accept incoming payments from third parties, withdraw the amounts and then send them as soon as possible to an account outside Germany in the form of cash remittances. They are promised a commission on the payments. The fraudsters justify these arrangements by claiming cost savings compared to cross-border credit transfers or say that sensitive client information needs to be protected. If you take up an offer of this kind you will be committing an offence and **may be liable to prosecution**. You will also be putting your own safety at risk because the perpetrators of these scams operate in the world of organised crime and will stop at nothing.

Be very suspicious of any offers asking you to make your current account available for payments for unknown firms and individuals, especially if they are located abroad. If you receive unexpected incoming payments which you are requested to return a short time later, contact your bank or the local police. Any returned payments should be sent only to the original account from which they came. All account holders who have either been unknowingly misused as financial agents or have been the victim of any kind of fraud are recommended to report the offence to the police.

Glossary

ActiveX Control	An ActiveX Control is a small Windows programme that can run with the help of a web browser, for example. ActiveX Controls may already be present on your computer or can be automatically downloaded when you call up a website.
Cookie	A cookie is a small text file stored on your PC by a web browser on the instructions of a web server containing details such as your web preferences. Cookies mainly act as a kind of electronic note-taker for the server, recording user-specific browser habits such as which websites have been visited how often and for how long or whether a website should be sent to the user in a personalised form.
Firewall	Firewalls are computers which monitor data traffic between a local network or a single computer and other networks, such as the internet. The firewall's function is to protect the local network or computer from unauthorised access. A personal firewall is a programme fulfilling the function of a firewall on your PC, meaning that it protects you from unwanted access without the need for an additional computer.
Java applet	Java is a programme language developed in the early 1990s. A Java applet is a small programme that is interpreted and executed in a browser after being downloaded from the internet. The Java commands are integrated into HTML pages and executed when these pages are loaded.
Patch	Small programme developed to solve security problems detected in an existing programme version as quickly as possible.
Pharming	Pharming or DNS spoofing is an attack in which the pharmer substitutes a false IP address for that of a well-known domain name. The URL looks legitimate although the user is on a spoof website.

Phishing	Phishing attacks use e-mail addresses or web pages pretending to be from familiar sources such as internet service providers, retailers or banks with the aim of inducing customers to divulge their account details, PINs and passwords on a fake website.
PIN	Personal identification number, a confidential access code.
Rootkit	A rootkit is a software tool which subverts the core functionality of the operating system with the aim of concealing activities such as stealing confidential access codes or copying files. The rootkit enables the hacker to operate with administrator rights.
Spyware	Spyware is the name given to a hidden software programme which sends user information to a third party without the user's knowledge, let alone approval. This information may include data stored on your PC, your surfing habits or personal information such as confidential access codes for online banking.
TAN	Transaction number; a one-time password used to authorise a transaction.
Trojan horse	Trojan horses are programmes that, unbeknown to the user, carry out operations compromising the security of a PC. The objective of most trojans is to capture sensitive information such as passwords and send them by e-mail or via the internet to the trojan's "owner". So-called backdoor trojans give hackers remote access to computers, which they can then control.
Viruses	Computer viruses are programmes that replicate themselves and spread over the internet by e-mail, for example. Viruses can sometimes inflict considerable damage on infected PCs.
Worms	Worms are self-replicating programmes that spread from computer to computer across a network. The aim of a worm is to infect as many computers as possible within a network and inflict damage.

Emergency checklist

What to do if you think your online banking data is no longer secure

Fraudsters are always trying to access customers' confidential online banking data by means of e-mails (phishing), for example, or malicious software (e.g. Trojan horses). What should you do if you think you may be the victim of fraud after responding to a phishing e-mail or noticing unusual requests or suspicious interruptions when banking online?

☑ Here is a brief checklist:

Step 1 ☐	**Block access to your online bank account** If you think someone has found out your PIN and/or TANs, block access to your online account immediately. You can do this, for example, by repeatedly inputting inaccurate PINs and/or TANs or sending a request to cancel access to a dedicated address at your bank. Contact your bank as soon as possible.
Step 2 ☐	**Check your account and investment portfolio** Check all movements on your account and in your investment portfolio by examining your bank statement or, if available, list of pending instructions. If anything seems suspicious, contact your bank immediately.
Step 3 ☐	**Install and/or update a virus scanner** Update your anti-virus software and operating system.
Step 4 ☐	**Activate your virus scanner** Scan all the drives on your PC thoroughly for viruses or Trojan horses and eliminate them.
Step 5 ☐	**Document the results of the scan** Save or print out the results of the anti-virus scan so that you can show them later on to your bank and/or the investigating authorities.
Step 6 ☐	**Rule out any further risks** Have you entered any other online services data into your PC? If so, cancel these as well. If anyone else uses your computer, inform them about what has happened.

General tips on security in the internet

Always up to date	Make sure your operating system and anti-virus software is always up to date. Manufactures offer regular service and security updates.
Check regularly	Carry out a thorough scan of all drives on your computer at regular intervals (e.g. once a week).
Be suspicious	Don't open any e-mail attachments from an unfamiliar source. If in doubt, contact the sender before opening an attachment.
Keep data confidential	Don't give your personal access code to anyone else. Remember that your bank will never ask you for any of your access codes either personally, on the telephone or by e-mail.
Don't save PINs or TANs	On no account save your PIN or TANs on your computer. Don't make things too easy for Trojan horses.

Further information about security can be found by visiting the websites of your bank and the Association of German Banks (**www.germanbanks.org**).

The “fokus:verbraucher” series

The Association of German Banks compiles information specifically targeting consumers in a series of publications of its own entitled “fokus:verbraucher – Eine Information der privaten Banken” [fokus:verbraucher – information for consumers from the German private banks]. All publications addressed to this target group are specially tailored to consumers’ needs. Consumers thus receive reliable and easy-to-understand information in the same recongnisable format free of charge.

The following publications in the “fokus:verbraucher” series are already available:

Ombudsmann der privaten Banken
Tätigkeitsbericht 2006 [The Private Commercial Banks’ Ombudsman | Ombudsman’s Report 2006] Berlin, July 2007

Banks and Consumers
The Comprehensive Consumer Policy Scheme of the German Private Commercial Banks | Berlin, January 2007

Credit Scoring
Part of modern lending
Berlin, October 2006

Copies of the above can be ordered at **www.germanbanks.org**.
For a complete list of our publications, please visit our German website **www.bankenverband.de**.

As at November 2007.

ONLINE BANKING SECURITY

Berlin, November 2007

PUBLISHED BY Bundesverband deutscher Banken
Postfach 040307, 10062 Berlin
Telephone +49 (0)30 16630
Fax +49 (0)30 16631399

DESIGN Manfred Makowski, Berlin

The Association of German Banks represents the interrests of the private commercial banks in Germany.

www.germanbanks.org

The Association of German Banks can be contacted:

by post:

Bundesverband deutscher Banken
Postfach 040307
10062 Berlin
Germany

by fax:

+49 (0)30 16631399

by telephone:

+49 (0)30 16630

by e-mail:

bankenverband@bdb.de

by internet:

www.bankenverband.de
www.germanbanks.org