SwissBanking

September 2009

Secure e-Banking

1 Secure e-banking

E-banking is an established and cost-effective way for private and corporate clients to communicate with their bank. Both sides benefit from this: for example, clients no longer have to go to the bank to make payment transfers or to find out their account balances. They can take advantage of these basic services online at any time, independent of the bank's opening hours. Banks in turn have the ability to communicate with clients 24 hours a day, which also improves the quality of your banking relationship.

But in addition to the advantages of the Internet, applications like e-banking are also associated with various security risks – including data being observed, altered or deleted during transmission, or fraudulently obtained by unauthorised persons.

This information sheet aims to make e-banking clients aware of potential security risks and highlight the means available to combat prevalent Internet threats.

You can help to ensure secure e-banking by becoming aware of the threats posed by the Internet, in order that you can work together with your bank to beat the ever-growing wave of Internet crime.

To protect yourself from manipulation when e-banking, you should cultivate a general level of security awareness when using the Internet and check your account activity regularly. If you think that you may have been the victim of Internet fraud, you should immediately block online access to your bank account and inform your bank promptly about any suspicious account activity.

2 Dangers on the Internet

The dangers and threats on the Internet are changing constantly, and often extremely quickly. The most prevalent dangers include viruses, worms, Trojan horses, phishing, pharming and drive-by downloads. Below you will find definitions of these terms and information on what you can do to fight them.

2.1 Viruses

Computer viruses have similar characteristics to biological viruses: they are capable of spreading themselves and can cause serious harm. Even harmless viruses can alter data on your computer, while the most serious cases can lead to your entire hard disk being erased. Viruses are spread via e-mail or by downloading infected files from the Internet onto your hard disk. Once a virus has been activated, it can spread extremely quickly via e-mail or over the Internet.

2.2 Worms

The damage caused by worms is similar to that of viruses, but worms themselves are standalone programs that do not require a host program for activation. They more often spread themselves independently from computer to computer by exploiting security vulnerabilities or configuration errors in operating systems or applications (e-mail, Internet).

2.3 Trojan horses

Trojan horses (or simply "Trojans") are programs often smuggled onto computers via Internet downloads in order to harm your computer – in ways you may not notice. Most Trojans aim to spy on sensitive data (e.g. passwords) and send it back to their owners, or to manipulate your transactions directly. Trojans allow their owners to gain access to third-party computers and thus take control of them remotely. Trojans are normally disguised as applications that are useful to users of the computers they infect.

2.4 Phishing

"Phishing" – the word Phishing is a contraction of the words "Password", "Harvesting" and "Fishing" - is when unauthorised persons request that you update or re-enter your confidential e-banking access data on your bank's website. The request may come via e-mail or through a manipulated Internet site, with the goal of spying on your confidential data, e.g. e-banking access data or account balances.

2.5 Drive-by downloads

Drive-by downloads are malware infections that happen only because you visited a particular website. These websites often contain legitimate content, but have been contaminated by harmful programs that smuggle malicious code into the site. Simply landing on an affected web page is enough to infect a computer.

2.6 Pharming

Pharming is a type of fraud that involves diverting your Internet connection to a counterfeit website, so that even when you enter the correct address into your browser, you end up on the forged site.

3 Measures to protect your e-banking

Only open e-mail from people and companies known to you, and never open attachments from unknown senders. In case of doubt, check with the sender. Use a current anti-virus software and a personal firewall. It is also important that you always keep the anti-virus software up-to-date by downloading and installing updates from your software provider as soon as they become available, or by using an automatic update service.

Make sure that you always use a current operating system and install the latest version of your web browser (including any plug-ins). You should also install all security updates for your user programs as soon as they become available. Otherwise, criminals may be able to exploit newly discovered weaknesses to gain access to your computer.

3.1 Do not use third-party Internet addresses for e-banking

Only enter your e-banking access information when you are certain that you are actually accessing the protected and authorised Internet site of your bank via an encrypted connection. You can recognise an encrypted connection because the "http" in the URL address has an "s" (for "secure") added to the end of it. This indicates that the website has a security certificate (e.g. https://www.sba.ch). You can verify the authenticity of the security certificate by double-clicking on the closed lock symbol that appears in the status bar at the bottom of the browser window. This will open a certificate dialog box, where the name of your bank should appear. Most banks also hold Extended Validation SSL certificates, indicated by the green background behind the section of the URL that contains the bank's name. When you click on this green bar, a dialog box appears showing the name of the bank on the security certificate together with the certifying authority. Once this has been established, you can assume that the site is trustworthy. Unfortunately, Extended Validation SSL is not yet supported by all browsers.

When shopping online, you should never enter your e-banking access data on the shopping site or on the site of an online payment service provider. You should only ever enter your secret access data on your bank's website, and never reveal it to any third parties. Sharing your e-banking access data with other companies represents a breach of the duty of due diligence stipulated in the e-banking agreement between you and your bank.

3.2 Protect your sensitive data

Protect your e-banking access data from unauthorised access and theft. Do not save sensitive data (passwords, e-banking access data, credit card numbers etc.) on your computer. Saving data on computers where you are not the only user, e.g. at your workplace, could allow third parties to see it.

Special spying programs (spyware) that may end up on your computer can also seek out such data and transmit it, e.g. via e-mail. If you use additional tools to improve your Internet security, such as a chip card reader with a PIN entry keypad, enter designated confidential data only when you have been prompted to do so by the device. Above all, never store your password.

You bank will never contact you to ask about your secret access data, whether over the telephone or by e-mail. You should never respond to such e-mails, nor should you follow any instructions they may contain, even if you are threatened with negative consequences such as your account being blocked. Inform your bank about any cases that may arise.

On the other hand, when you are the one making contact with your bank, it can well be the case that you will be asked for your secret access data as a way to identify you for the purposes of telephone banking. Always be sure that you have dialled the correct number and that correct procedure is being followed before you comply with such requests.

Make sure that you only enter your confidential access data on the genuine website of your bank. Be aware of any changes to the appearance of your bank's normal e-banking access page. You will notice small changes immediately if you have accessed the bank's Internet site often – for example, slight shifts in the position of the bank's logo or headlines.

3.3 Create a secure password

Use a good, secure password for e-banking. A good password has at least eight characters and includes a combination of capital and lowercase letters as well as numbers. Do not use your name or numbers such as your birth date, nor those of someone you know. Change your password regularly, especially if you think someone could have discovered it. You can find examples on the Internet, and perhaps on your bank's website, showing how to create a secure password.

4 General precautions

Whenever possible, access your e-banking using a computer to which you have exclusive access. When using a public computer, e.g. in an Internet café, you cannot be sure to what extent access is protected through effective security software or which programs are already installed on the computer. The keyboards of public computers may also be manipulated. You cannot assume that these computers are secure, and thus should not engage in e-banking activities on them.

When doing e-banking, be careful not to open any additional browser windows/tabs or e-mail programs.

Always end your e-banking session by logging out (using the "log out" or "end" function), and then deleting the temporary Internet files and cookies from your web browser. Your bank's website should provide advice on how to do this.

Links to further information:

- www.swissbanking.org > Dossier: Information for bank clients
  http://www.swissbanking.org/en/home/dossier-bankkunden.htm

- Reporting and Analysis Centre for Information Assurance MELANI
  http://www.melani.admin.ch/themen/00103/index.html?lang=en

- German Federal IT Security Office (in German only)
  http://www.bsi-fuer-buerger.de/

This brochure is also available in French, Italian and German and can be ordered online from the Swiss Bankers Association at http://www.swissbanking.org/home/shop.htm.

It can also be downloaded as a PDF from http://www.swissbanking.org/home/en/dossier-bankkunden.htm.

Swiss Bankers Association
Aeschenplatz 7
PO Box 4182
4002 Basel
Switzerland
T +41 61 295 93 93
F +41 61 272 53 82
office@sba.ch
www.swissbanking.org