
Introduction

Welcome to the security section of our website. This area has been designed to answer any concerns that you may have around the security of doing your banking online. This includes information on the following:

- Latest security guidelines
- Confirming it is ING Online
- Updating your computer
- Anti-virus software
- Personal firewalls
- Security glossary

You can do your internet banking with ING Online with confidence in knowing that ING Online uses the most up-to-date encryption technology available. To ensure you benefit from this is to use the latest version of a recommended internet browser. Currently, the latest version of Microsoft Internet Explorer offers encryption technology.

All information you share with us is held in the strictest confidence, in compliance with privacy standards. You are the only one who can access your account or verify a transaction, using your User Name, unique Password and unique Personal Identification Number (PIN). When you make a transaction by internet, all transactions are recorded for later reference.

[Notification in case of security improvements:

We'll soon be improving the security of our online login process. We're doing this because we take internet security very seriously. In fact, apart from maintaining our simple, straightforward and hassle free promise to you, it's our top priority.]

Latest security guidelines

Personal information

Your password and PIN are the keys to your account. Remember that protecting your security details is your responsibility:

- Store your smart card in a secure environment.
- Do not write down your personal access codes, give them to anyone else or include them in an e-mail.
- Prevent someone can see your personal access codes during log on.
- Do not use simple, easy to guess passwords.
- Change your password frequently. From security point of view ING requires that you'll change your password at least ones a month.
- In case your smart card is lost or stolen, contact immediately ING to block access to ING Online.
- Use the "log off" option to log off.
- Be very cautions when you do internet banking in an internetcafé, while the security level of this PC is unknown.

ING Online internet banking

- Every combination of username and password is unique. When you log on, data is verified on existence. When you are logged on to ING Online and you did not connected to the ING systems for more than 15 minutes you session is cancelled. To continue you have to log on again.
- When you sign a transaction a digital signature is put on the transaction to ensure non-repudiation.

- A penetration test by independent professional third party companies for ING Online is executed on a regular basis. Possible security gaps are immediately solved.

E-mail communication and security alerts

ING Online will never send you e-mails asking for your confidential or personal security information. If you receive any such request do not act on the instructions given in the e-mail, but contact our Client Service desk immediately on +420 257 474 666.

If you ever get an e-mail containing an embedded link, and a request for you to enter personal details, treat it as suspicious. Do not input any sensitive information that might help provide access to your accounts, even if the page appears legitimate.

Vishing

Vishing is an adaptation of phishing attacks that uses telephone or VoIP (Voice over IP tools). You may receive an email or SMS asking you to call a free phone number to confirm your details, or you may receive a phone call with a recorded message asking you to input your account details. Once you have done this the attacker is free to use your personal information to attack your account.

To protect yourself use only the published official call centre numbers for your financial services company and be cautious in giving out your personal information over the telephone. Remember ING will never ask you for your password over the phone.

Imitation of ING Online website

Security is of the utmost importance to ING Online and we would like to reassure all our customers that swift and appropriate action is being taken. For more information on precautions that can be taken, please read our "*Confirming it is ING Online*" section.

Please forward a copy to: abuse@ing.com and we will investigate further.

Revealing your full PIN

We will never ask you for your PIN, so if you are ever asked for, please stop using the site or service and contact us immediately via telephone on +420 257 474 666 or by e-mailing us at abuse@ing.com

Spoof websites and Phishing alerts

Fraudsters create authentic looking, but false or "spoof" websites. Their purpose is to tempt customers to enter personal information. This information will be re-used to try and access your bank accounts. Fraudsters are increasingly turning to e-mail to generate traffic to these websites. This is also known as 'Phishing'.

Recently customers of several financial institutions have received such e-mails and this activity is only likely to increase. Such e-mails typically contain a link to a spoof website and mislead account holders to enter customer names and security details on the pretence that security details can be updated or changed. For more information visit our "*Confirming it is ING Online*" section.

Targeting personal data

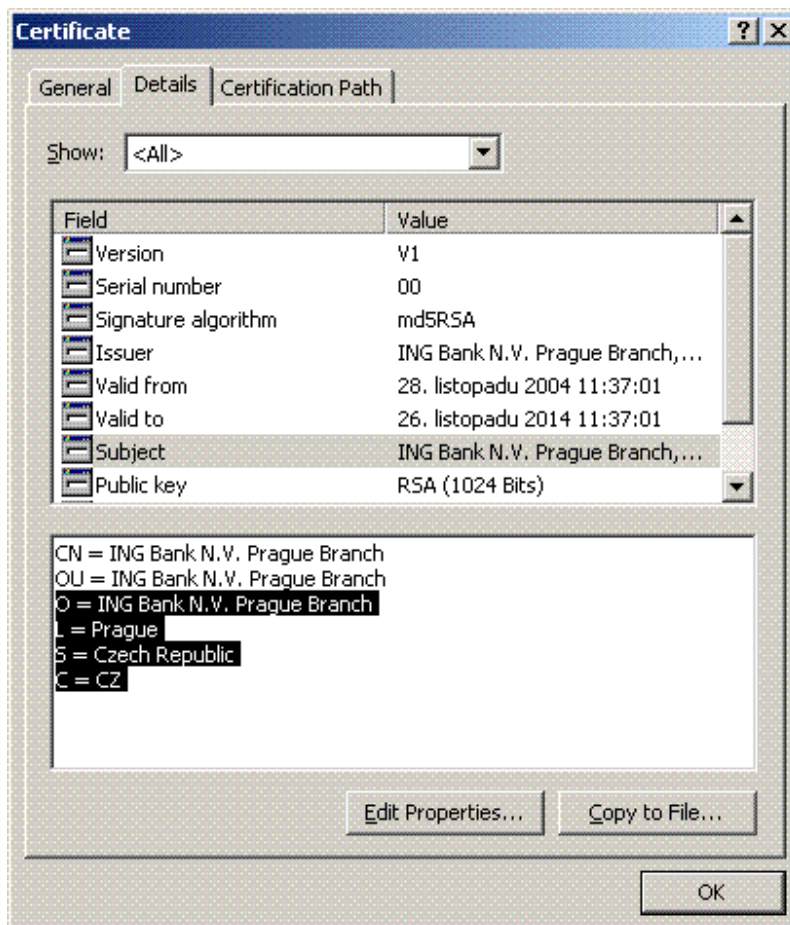
People should be aware that there are malicious ways that their computer can be targeted in an attempt to install bogus software, which has the potential to capture personal data and redirect you to fake sites. Microsoft is aware of some issues and latest information and advice can be obtained by clicking [here](#).

As always we encourage you to keep your antivirus and computer software up-to-date. Keep your computer software up to date. Make sure you keep your computer up to date with the latest security and anti-virus software. Please read our "*Updating your computer*" section and also our "*Anti-virus software*" section.

Confirming it is ING Online

Always check the following before providing personal information:

- Whenever entering personal information onto any website, for example bank details, make sure that the website encrypts the information you send to, and receive from, the site. Always ensure the spelling of the domain name is correct.
- Make sure the URL begins with "https" rather than "http" (as shown below);
- Look for a padlock icon on the bottom of your browser (as shown below);
- Make sure the domain is owned by the company you expect to interact with by double-clicking on the lock icon in your browser. The key to look for is that the domain ingonline in the following example is present:



EG: secure.ingonline.cz = (subdomain=secure).(domain=ingonline).(top-level domain=cz)

If you find a spoof of our site, please contact us at abuse@ing.com

Updating your computer

From time to time, hackers and/or viruses discover weaknesses in software that allows them to illegitimately gain access to your computer. In order to prevent such attacks and protect your computer, software developers offer free updates for their software via their websites.

To check for updates simply visit the publishers website, typically in their Download section, for example: for Microsoft Windows users visit Microsoft Windows Update site.

If you have an earlier version of a browser, it's easy to download an updated version:

- For Internet Explorer: Click on the free Downloads link on the Microsoft site at: www.microsoft.com/ie

What are the known browser problems with the Security Certificate and how do I resolve them? Click [here](#) to view browser and third-party application problems that have been recognized by VeriSign.

Anti-virus software

You may already be using anti-virus software but to be effective the software should be updated on a regular basis with the latest virus definition files. If you are unsure how to do this, you should refer to the program's Help function.

There are many effective programs to choose from, but the most common commercial products include* (in alphabetical order):

- AVAST
- AVG
- Kaspersky Labs
- Norman
- McAfee
- Panda
- Symantec
- Sophos
- Trend Micro

** The list of product suppliers is given for information only and should not be taken as recommendations by ING Online. If unsure on suitability, customers should seek expert advice. Further information can be found by searching for 'Anti-Virus software' and 'Spyware' on internet search engines.*

Spyware Removal Software

You may already be using Spyware Removal software but to be effective the software should be updated on a regular basis. If you are unsure how to do this, you should refer to the program's Help function.

There are many effective programs to choose from, but the most common commercial products include* (in alphabetical order):

- McAfee
- Lavasoft Ad-aware
- Spybot-Search & Destroy
- Spy Sweeper
- Symantec

** The list of product suppliers is given for information only and should not be taken as recommendations by ING Direct. If unsure on suitability, customers should seek expert advice. Further information can be found by searching for 'Anti-Virus software' and 'Spyware' on internet search engines.*

Personal firewalls

A firewall is another small program that helps protect your computer and its contents from outsiders on the internet. When installed it stops unauthorized traffic to and from your PC.

There are many effective programs to choose from, but the most common commercial products include* (in alphabetical order):

- BlackICE Defender
- Kerio Personal Firewall

- McAfee Personal Firewall
- Sygate Personal Firewall
- Norton Personal Firewall
- Tiny Personal Firewall
- Zone Alarm

** The list of product suppliers is given for information only and should not be taken as recommendations by ING Online. If unsure on suitability, customers should seek expert advice. Further information can be found by using Internet search engines on firewalls.*

Security Glossary

Anti-Virus Software

It is a program to detect and remove computer viruses. The simplest software scans executable files and blocks a list of known viruses. Others are constantly active, attempting to detect the actions of viruses. Anti-virus software should always include a regular update service allowing it to keep up with the latest viruses as they are released. For more information visit our "*Anti-virus software*" section.

Back Door

It is a hardware or software-based hidden entrance to a computer system that can be used to bypass the system's security policies. For more information visit our "*Anti-virus software*" section.

Cookies

Cookies are small files stored on a computer's hard drive. Cookies are generally harmless and are used to recognize a customer so that they can receive a more consistent experience of a website. Cookies can contain information about your preferences that allows customization of a site for your use.

Encryption

Encryption converts your data into an encoded form before it's sent over the Internet, stopping unauthorized users from reading the information. At ING Online, we use 128-bit Secure Socket Layer (SSL) Encryption, which is accepted as the industry standard level. You know that your session is in a secure 'encrypted' environment when you see https:// in the web address, and/or when you see the locked 'padlock' symbol.

Browsers

IE5 and above

Firewall

A firewall is a small program that helps protect your computer and its contents from outsiders on the Internet or network. When properly installed, it prevents unauthorized traffic to and from your PC. There are many effective programs to choose from. Common commercial examples are from Zone Labs, Symantec (Norton), McAfee and Computer Associates. In many cases there is a version of commercial software that is free of charge for personal users. For more information visit our "*Personal firewalls*" section.

Keystroke Capturing and Logging

Anything you type on a computer can be captured and stored. Such covert activity can be via a hardware device attached to the PC or by software running almost invisibly on the machine. Keystroke logging is often used by fraudsters to capture personal details including passwords. Some recent viruses are capable of installing such software without the user's knowledge.

The risk of encountering such keystroke logging is greater on PCs shared by a number of users, such as those in internet cafés and libraries. Running anti-spyware software would reveal the presence of any such software on your PC. Customers can download free anti-spyware, for more information visit our "*Anti-virus software*" section.

We'll shortly be introducing an online Key Pad which will minimize the risk of anything you type into your computer using your keyboard being captured and stored by others.

Phishing

A malicious user or Web site that deceives people into revealing personal information, such as account passwords and credit card numbers. A phisher typically uses deceptive e-mail messages or online advertisements as bait to lure unsuspecting users to fraudulent websites, where the users are then tricked into providing personal information. For more information visit our "*Confirming it is ING Online*" section.

Secure Sessions

When you login to Internet Banking you are said to be in a "secure session". SSL technology is used within your Internet Banking session to encrypt information before it leaves your computer, in order to ensure that no one else can read it. Depending on your browser settings, a pop-up window may appear to notify you that you will be entering a secure page. You will know that you are on a 'secure' page when you see the 'https://' before the web address. You will also see a closed padlock symbol in the lower right hand corner of your browser window.

Secure Sockets Layer (SSL)

Secure Socket Layer (SSL) protocol provides a high level of security for Internet communications. SSL provides an encrypted communications session between your web browser and a web server. SSL helps to ensure that sensitive information (e.g. credit card numbers, account balances and other proprietary financial and personal data) sent over the Internet between your browser and a web server remains confidential during online transactions.

Session Time-outs

These are automatic disconnections, for security reasons, from any secure session after a period of server inactivity. It may occur even if you are typing something into a page or data field, the event being triggered by no communications to our servers, rather than by keyboard or mouse inactivity. All our internet banking services have this protection.

Spyware

It is any software that covertly gathers customer information through their Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of programs that can be downloaded from the Internet; however, it should be noted that the majority of applications do not come with spyware. Once installed, the spyware monitors customer activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Spyware is similar to a Trojan horse in that customers unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today. For more information visit our "*Anti-virus software*" section.

Trojan Horse

It is a program that appears legitimate, but performs some illicit activity when it is run. It may be used to locate password information or make the system more vulnerable to future entry or simply destroy programs or data on the hard disk. A Trojan is similar to a virus, except that it does not replicate itself. It stays in the computer doing its damage or allowing somebody from a remote site to take control of the

computer. Trojans often sneak in attached to a free game or other utility. For more information visit our "*Anti-virus software*" section.

Virus

A computer program usually hidden within another seemingly innocuous program that produces copies of itself and inserts them into other programs and that usually performs a malicious action (as destroying data). For more information visit our "*Anti-virus software*" section.

Vulnerability

Security holes/bugs are faults, defects or programming errors. These may be exploited by unauthorized users to access computer networks or web servers from the Internet. As these vulnerabilities become known, software publishers develop 'patches,' 'fixes' or 'updates' that you can download to fix the problems. For more information visit our "*Updating your computer*" section.

Worm

A worm is a program that is designed to replicate and spread throughout a computer system. It will usually hide within files and distribute those files through any available network connections. In addition, worms can spread rapidly via e-mail. For more information visit our "*Anti-virus software*" section.