



ING Standard Practice on Anti-Phishing

ING Online is a secure and personalised website. Only the customer can access his account or verify a transaction, using his User Name, unique Password and unique Personal Identification Number (PIN). Every combination of username and password is unique. After log on, data is verified on existence. When a customer signs a transaction a digital signature is put on the transaction to ensure non-repudiation. All transactions processed via ING are recorded for later reference. Independent professional third party companies regularly perform a penetration test for ING Online. All information the customer shares with ING is held in the strictest confidence, in compliance with privacy standards. Please refer to ING's Privacy statement for further information.

If you experience any problem with the Security Certificate, check the browser and third-party application problems that have been recognized by [Thawthe](#) and [VeriSign](#).

In the security section, you can find the following information:

- [What safety measures are in place?](#)
- [How can you contribute to a safe use of the ING Online application?](#)
- [What else can you do?](#)
- [Security glossary](#)

What safety measurements are in place?

Secure connection with ING

When a user logs on to ING Online a secure connection is established between the ING host system and your (desktop) computer. This function is called Secure Socket Layer (SSL). This network security method takes care of the encryption (128 bit) of all the information that is sent to ING or received from ING. As soon as a SSL session starts, a little padlock will appear in the bottom right hand corner of the status bar of your Internet Browser (Microsoft Internet Explorer). By clicking on this padlock you can view the details of the security certificate in use. (See next paragraph: Check the secure connection). SSL is the standard way of securing personal information and transactions on the internet.

Restricted log on time (time out)

When you are logged on to ING Online and you have not performed an action that caused traffic between your computer and the ING server for a period longer than 15 minutes, the connection will automatically be cancelled. Since this will result in a loss of all the data since the last time that you saved your work, be sure that you save the transaction that you are working on before this period expires. After that, you will need to log on again to access the application.

How can you contribute to a safe use of the ING Online application?

Check the secure connection

Click on the 'closed padlock' icon on the status bar in the bottom right hand corner of your browser. Information on the secure connection is shown. Check whether the Secure Socket Layer (SSL) certificate is issued to: www.ingonline.com. Check the URL (address) in the address bar of your browser. This should say: <https://www.ingonline.com/>. If this is not the case, don't key in your log on name, password or any other information; there is no secured connection with ING Online.

Check that your website is secure,

- The URL will begin with https://
- OR
- The application window will specify that SSL (Secure Sockets Layer) Library.



SSL Library

If https, the secure lock icon, a small padlock will appear on the browser



Click on the padlock icon to see the details of the security certificate. The certificate shows who owns the site; it should be your bank. Check that the details and validity are correct. We work with well known certification authorities such as Verisign, Global Sign and Thawte. ING also provides certificates from its own ING Corporate PKI.



Internet Explorer 5 and 6



Netscape 4.7 and above

If you are using the new Internet Explorer 7, you will find the padlock in the top right of the browser window.





Be careful with passwords/PIN codes

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

1. Your password/PIN code is strictly confidential. ING staff will never enquire after your password/PIN code. Not via the internet, via e-mail, by telephone or otherwise. Never give your password/PIN code to anybody!
2. Change your password frequently. From security point of view ING requires that you'll change your password at least ones a month.
3. Use the latest version of your internet browser. Check and update on a regular basis the version of your internet browser. Normally newer versions of internet browsers are more sophisticated with regard to security matters than older versions. To guarantee the use of the latest versions of your browser software, consult the Microsoft website for available updates.
4. Be meticulous with your log on name and your password/PIN code. Be sure that it is not known to others, since they would be able to look into your data.
5. Never write down or leave your log on name and password/PIN code where others may look into them. Have nobody watching when you key in your log on name and password/PIN code.
6. Do not make use of an unsafe password. Passwords that are too obvious must be regarded unsafe. E.g. your wife's or husband's name, the name of your child, pet or car, the names of months etc. are all easily guessed and tried out too easily. Compose your passwords preferably of a mix of non meaningful characters and figures, upper and lower case and change your password often.
7. If you suspect anyone to have any knowledge of your personal codes, immediately contact Customer Services to have your account blocked.

Phishing: be suspicious of emails asking for your information

A phishing attack is an online fraud technique which involves sending official-looking email messages with return addresses, links and branding that all appear to come from legitimate banks, retailers, credit card companies, etc. Such emails typically contain a hyperlink to a spoof website and mislead account holders to enter customer names and security details on the pretence that security details must be updated or changed. Once you give them your information it can be used on legitimate sites to take your money.

It is important that you are suspicious of emails asking for your information! Please [read more information](#) regarding this subject.

Protect your pc against computer viruses

Make use of the most recent anti virus software. Check on a regular basis for updates of anti virus software and have these installed immediately. Scan your computer for viruses regularly. Have your anti virus software active at all times.

Do you connect to the internet via cable or a DSL connection?

If you are connected to the internet through a company network, by cable or DSL, then you are typically on line longer and more frequent then would be the case with a dial up connection. It is advisable to have firewall software installed and have the file sharing options with other computers switched off or use very strict settings. Ask your network administrator for more information on this topic.

What else can you do?

1. Update your computer software regularly. From time to time, hackers and/or viruses discover weaknesses in computer software that allows them to illegitimately gain access to computers. Software providers (e.g. Microsoft)



- constantly offer free updates for their software via their websites. To check for updates simply visit the publisher's website, typically in their download section.
2. Store your smart card in a secure environment. In case your smart card is lost or stolen, immediately contact your local Customer Services to block access to ING Online.
 3. If - while operating ING Online - you have opened a report or other kind of downloaded document or attachment, make sure you clear your cache afterwards, because a copy is stored on your hard disk.
 4. Use the "log off" option to close the ING Online application.
 5. Be very cautious when you use a PC to access the internet in an internet café or library, while the security level of this PC is unknown. Always log off and close your browser when you are finished working with ING Online.

Security glossary

Anti-virus software programs

Anti-virus software programs 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. Check the Help function of the software for more information.

Back Door

A hardware or software-based hidden entrance to a computer system that can be used to bypass the system's security policies.

Cookies

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

Encryption

Encryption converts your data into an encoded form before it is sent over the internet, stopping unauthorised users from reading the information. ING Online uses 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 in the right lower corner of your browser.

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 unauthorised traffic to and from your PC.

Keystroke capturing and logging

Keystroke logging is often used by criminals to capture personal details including passwords. Criminals may try to install a hardware device or software to a pc running almost invisibly on the machine. Anything you type on a computer can then be captured and stored.

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.

Phishing

A malicious user or website 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. Please remember that ING staff will never enquire after your password/PIN code. Not via the internet, via e-mail, by telephone or otherwise. Never leave your password/PIN code with anybody!

If you receive suspicious e-mails, please forward them to ING at abuse@ing.com, also if you have other suspicions.

Secure Sessions

When you login to ING Online a 'secure session' is set up. SSL technology is used within your 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. Within ING Online, you will be automatically disconnected if you have not been active for 15 minutes. You will then have to logon again. All ING's internet banking services have this kind of protection.

Spyware

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 a third party. 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.

In order to be effective, Spyware Removal software should be updated on a regular basis. Check the Help function of the software for more information.

Spoof websites and Phishing alerts

Criminals may 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. Criminals are increasingly turning to e-mail to generate traffic to these websites. This is also known as 'Phishing'.

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, read the paragraph Check the secure connection on this webpage. If you find a spoof of our site or have other suspicions, please contact ING at abuse@ing.com.



Trojan Horse

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 a third party from a remote site to take control of the computer. Trojans often sneak in attached to a free game or other utility. Always have Anti-virus software running on your PC and regularly update it.

Virus

A computer program usually hidden within another seemingly innocent program that produces copies of itself and inserts them into other programs and that usually performs a malicious action (as destroying data). Always have Anti-virus software running on your PC and regularly update it.

Vishing

Vishing is an adaptation of phishing attacks that uses telephone or VoIP (Voice over IP tools). An SMS or e-mail is sent asking to call a free phone number to confirm customer details, or they call the customer with a recorded message asking him to enter his account details. If the requested customer details are provided, the customer's account will be attacked.

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. Please remember that ING staff will never enquire after your password/PIN code. Not via the internet, via e-mail, by telephone or otherwise. Never leave your password/PIN code with anybody!

Vulnerability Security holes/bugs

Vulnerability Security holes/bugs are faults, defects or programming errors. These may be exploited by unauthorised third parties 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. Always have the software running on your PC regularly updated.

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. Always have Anti-virus software running on your PC and regularly update it.