ING BANK

ING BANK Security Policy

ING BANK has outlined some important security information to enable you to protect your personal and account details when banking online. This information is updated regularly, so please ensure you read the message as often as possible.

Detecting a Virus

What is a virus

Viruses (and their relative's worms and Trojans) are malicious programs that can harm your computer or use your computer to harm someone else's computer or network. Virus code is usually buried within the code of another program. Once the program is executed the virus is activated and may perform a number of different activities, such as attaching copies of itself to other programs on your computer.

How do you know if your computer has a Virus

When you open and run an infected program, you might not know you've contracted a virus. Your computer may slow down, stop responding, or crash and restart. Sometimes a virus may prevent your computer from starting up.

Note that similar symptoms may appear from software and hardware problems that are unrelated to a virus. If in doubt, you should seek professional assistance.

The best way to protect your computer is by installing anti-virus software and keeping it up to date.

How you can protect your computer from a virus

- You should install and maintain up-to-date anti-virus software on your computer
- You should regularly virus scan all files on your computer
- You should consider regularly scanning your computer for spyware
- ING BANK recommends that you install and enable a personal firewall on your computer to create a security barrier between your computer and the Internet
- It is essential that you have a securely configured computer to protect yourself on the Internet. Operating systems are complex, and vendors regularly release patches to close security holes. You should regularly update your computer's software from the vendor's website. If you are using Windows XP, enable the 'Automatic Updates' Feature.
- You should ensure that you are running the latest version of your web browser.(link to Microsoft and Netscape)

Detecting Hoax e-mails

What is a hoax e-mail and how can it affect you

- A hoax e-mail is an e-mail that usually asks for your personal information and has a link to an authentic looking, but fake website. They might also ask you to install software which may contain viruses.
- If you have clicked on an attachment in a hoax email, you should scan your computer for viruses and then change your ING BANK Access Code. If you are unsure whether you have removed any viruses, you should seek professional assistance.

ING BANK e-mail support

- Genuine e-mails from ING BANK do not contain direct links to the online banking. ING BANK will never ask you to reveal or change your Access Code or any other confidential, personal or account information via e-mail.
- If you receive a hoax email do not click on any links or open any of the attachments. Do not provide any personal information requested in the email. Contact ING BANK immediately on 13 16 88. Then delete the email.
- For further tips on hoax emails and other scams you can visit the Australia Securities & Investments Commissions (ASIC) website at http://www.fido.asic.gov.au

ING BANK Online Banking

Logging on to online banking

- Always access ING BANK online banking by typing www.ingbank.com.au into your browser (or use your favourites menu) and clicking on Online Banking. Never click on a link in an email to log on.
- Avoid using computers at public places, such as Internet cafes, for online banking. If you do access online banking at one of these places, you should change your Access Code as soon as possible afterwards.
- When signing on to online banking, always look for a padlock image (insert picture) on the toolbar of the online banking window
- When you successfully sign in, the welcome screen will display your last sign in time. If this is not correct please contact us immediately by calling 13 16 88.
- After three failed login attempts, your login will be disabled
- Never leave your computer unattended while logged onto online banking
- When you have finished your online banking, ensure you exit correctly by clicking the Log Off button

How to protect your access code

- Choose a secure Access Code that cannot be easily guessed. Avoid using a related number such as your birth date.
- Never disclose your Access Code to anyone else and do not keep a written record of it. Commit it to memory. ING BANK will never ask you for your Access Code except when logging onto Internet banking or via our automated telephone system.
- Change your Access Code regularly
- Report any suspected security breach to us immediately

What else can you do to protect your account information

- You should regularly read our security policy
- Always check your statements for any suspicious transactions
- If you believe your account has been compromised in any way, contact ING BANK immediately on 13 16 88
- For further definitions, please see our glossary

Glossary

Virus Viruses (and their relatives worms and trojans) are malicious programs that can harm your computer or use your computer to harm another's computer or network.

Anti-virus software Anti-virus software is designed to protect you and your computer against known viruses, worms and trojans. Ensure that your software is configured to download updates regularly.

Spyware Also known as "adware", spyware is hidden software that transmits user information via the Internet to third-parties such as advertisers or hackers. Often the user is unaware that spyware is installed.

Firewall A system designed to protect a computer or network from unauthorised access, especially via the Internet.

Patches Type of software used to repair or update existing software, patches are often distributed by operating system vendors such as Microsoft and Apple.

Hoax e-mails A number of customers from Australian financial institutions have been targeted with hoax e-mails which appear to be genuine bank e-mails. These e-mails usually claim to require your information, and link to an authentic-looking, but fake website. They can also ask you to install software which often contains viruses.

Fake websites Also known as "ghost websites", the purpose of fake websites is to obtain your log in details to access your bank accounts. They can also be used to obtain other personal information which could be used in identity theft.

Phishing Phishing is a collective term for the use of hoax e-mails and fake websites to deceptively obtain personal information to be used in identity theft.