

## Overview

ING Security Policy aims to assist clients in ensuring that their on-line transactions and personal information is secure at all times. This document outlines:

- Latest key security issues
- ING's standard practices
- Verifying websites
- How to protecting yourself against fraud

May 2007

ING INVESTMENT MANAGEMENT

# Security Policy



ING makes every effort to provide optimal security of your data and of all transactions. For us protecting our clients is just good business. However hard we work there are risks online, and you can take some action to protect yourself. Here we provide some general information to answer any concerns that you may have around the security of online transactions. More specific information should be available from your bank.

## 1. Latest Key Security Issues

From time to time we will provide information on security related news items that we feel you should be aware of. These security updates will be presented on this page.

### Phishing

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; see more on ING's standard email practices.

### Imitation of ING websites

ING monitors the internet to find imitation websites which are often the first step made by phishers. We then work with the appropriate international authority to get the websites closed down as quickly as possible – sometimes on the same day we find the website. To report phishing attacks please email our security team.

email address = [global.cirt@mail.ing.nl](mailto:global.cirt@mail.ing.nl)

## Advanced Fee Fraud

You may already have heard of 'advance fee fraud', where emails offering large sums of money are sent to thousands of email addresses, but a modest 'fee' was required in order to cover legal fees, open an account or pay customs charges.

Sometimes the money offered is as a result of a lottery for which you have never bought a ticket. Sometimes the money is held in an account overseas but the account owner cannot access it, they promise a percentage of the money in return for your help. In both cases various fees have to be paid.

Do not respond to these emails. They are part of a fraud and you will not receive any of the promised money.

We place this warning here because we are aware that the criminals carrying out these frauds do on occasion use the name of ING or an ING subsidiary as part of this scam.

## 2. ING's Standard Practices

ING may communicate with clients by mail on occasion, so how can you tell which mails are from us, and which are fraudulent?

- ING will address you by name in any emails.
- ING will not embed hyperlinks in emails that take you to sites where you must enter your security information.
- ING will never ask for you to confirm your details by email
- ING will use state-of-the-art encryption and authentication mechanisms to secure the transactions; these will vary by bank so check with your bank about the processes used.

If you have any doubt about any email you have received purporting to be from ING you should contact your bank.

### 3. Verifying Websites

Clients must be sure that the site they are entering really belongs to ING or an ING subsidiary and that it is a secure site. Check that your website is secure:

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

If it is a https, the secure lock icon, a small padlock will appear on the lower bar of 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, GlobalSign and Thawte.

If you have any doubts about a website you should contact your bank.

### 4. Protect Yourself

#### Take care of your personal information

Your account numbers, customer Number, PIN, memorable date and customer identification number are the keys to your account. Never write them down, give them to anyone else or include them in an e-mail. Remember that protecting your Customer Number, PIN and security details is your responsibility.

#### Take care of your computer

- Update your computer by installing the latest software and patches, to prevent hackers or viruses exploiting any known weaknesses in your computer
- Install and update virus protection, to protect against viruses corrupting your computer and to prevent hackers installing Trojan viruses on your computer

For additional information please contact:

---

#### INGIM Compliance

Email: [ingim.compliance@ingim.com.au](mailto:ingim.compliance@ingim.com.au)

Website: [www.ingim.com.au](http://www.ingim.com.au)

---

ING Investment Management Limited  
ABN 23 003 731 959  
Level 21, 83 Clarence Street  
Sydney NSW 2000 Australia  
[www.ingim.com.au](http://www.ingim.com.au)

- Install and update anti-spyware tools.
- Install and update personal firewalls
- Use only programmes from a known, trusted supplier.

#### Beware of Spam Emails

- Use a spam filter to avoid even seeing these messages
- NEVER respond to a spam message, your email address is then recorded as live and the spam will increase.
- Should you read a spam message remember: if it sounds too good to be true, it probably is too good to be true.

### 5. More info

The US Federal Trade Commission provides information on how to avoid phishing scams.

<http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm>

The Anti-Phishing Working Group provides statistics on phishing attacks and advice for individuals and companies.

<http://www.antiphishing.org/>

For more information please contact your own bank