

### Take Care

- Delete without opening emails requesting personal details such as PINs or passwords – legitimate financial institutions and companies will not ask you to provide PINs or passwords.
- Delete suspicious emails with attachments and never open the attachments.
- Check for a secure connection. (Secure website addresses have https at the start. The ‘s’ indicates secure. They will also have a ‘padlock’ icon on the bottom right corner. Double clicking the icon will show who owns the certificate).
- Follow your own path to the site you choose – it is possible to create a link on a web page or in an email and make it look as if it is taking you to a bona fide website when it is sending you elsewhere. Your safest course is to check that you have the correct address (URL) and then type it each time into your address bar.
- Consider whether the message you have received is a message that you would expect to receive – is it one you have received from your financial institution before? (Incorrect grammar or spelling is usually an immediate indicator of a suspect email or website).
- Are there related announcements on the financial institution’s or company’s website?
- Reconcile your account(s) either on-line or by statements frequently and regularly.

### Suspicious? Report It

If you think you may have been taken in by or received a phishing scam, or that you may have received a virus that enables someone to access your account details, report it immediately to your financial institution.

September 2005

## MORE INFORMATION

### REFER TO YOUR BANK’S WEBSITE FOR MORE INFORMATION

[www.anz.co.nz](http://www.anz.co.nz)  
[www.asb.co.nz](http://www.asb.co.nz)  
[www.bnz.co.nz](http://www.bnz.co.nz)  
[www.citibank.co.nz](http://www.citibank.co.nz)  
[www.hsbc.co.nz](http://www.hsbc.co.nz)  
[www.kiwibank.co.nz](http://www.kiwibank.co.nz)  
[www.nationalbank.co.nz](http://www.nationalbank.co.nz)  
[www.superbank.co.nz](http://www.superbank.co.nz)  
[www.tsbbank.co.nz](http://www.tsbbank.co.nz)  
[www.westpac.co.nz](http://www.westpac.co.nz)

### OTHER USEFUL SITES

**New Zealand Securities Commission**  
[www.sec-com.govt.nz](http://www.sec-com.govt.nz)

**New Zealand Commerce Commission**  
[www.comcom.govt.nz](http://www.comcom.govt.nz)

**Microsoft New Zealand Limited**  
[www.microsoft.co.nz/security](http://www.microsoft.co.nz/security)

Copies of this pamphlet can also be obtained online at: [www.nzba.org.nz](http://www.nzba.org.nz)



# INTERNET BANKING

## SECURITY AWARENESS

## INTRODUCTION

This pamphlet is intended to provide an explanation of some of the common forms of Internet fraud and provide some suggestions on how to protect yourself.

## FORMS OF INTERNET FRAUD

### Phishing

Phishing is a technique used to gain personal information for the purposes of identity theft using fraudulent email messages that appear to come from legitimate businesses, most commonly banks. These authentic-looking messages are designed to lure recipients into divulging personal data such as account numbers, passwords and credit card numbers.

Phishing emails often look authentic. They pretend to come from a financial institution or other company and have a believable email address. They often copy that institution's logo and message format. It is common for phishing emails to contain links to a website that is a convincing replica of the company's homepage.

Phishing emails give themselves away by telling you that there is some reason why you must provide personal details such as your Internet banking logon, password, credit card number or PIN by reply email or through a website. Phishing emails may seem plausible when first read and attempt to force the recipient to urgently reply or logon to a website before they have time to think about what they are doing.

### Replica Websites

These are the websites (URLs) you are directed to by phishing emails. These websites appear authentic but are, in fact, the mechanism for capturing your personal details. These sites will often contain incorrect grammar or spelling, which is usually an indication that they are not authentic sites.

### Viruses

Computer viruses are called viruses because they share some of the traits of biological viruses. A computer virus passes from computer to computer like a biological virus passes from person to person. A computer virus must piggyback on top of some other programme or document in order to get executed. Once it is running, it is then able to infect other programmes or documents. Viruses are commonly transferred by email. Most computer fraud programmes are passed on by a virus.

### Worms

A worm is a computer programme that has the ability to copy itself from machine to machine. Worms normally move around and infect other machines through computer networks. Using a network, a worm can expand incredibly quickly from a single copy. A worm usually exploits some sort of security hole in a piece of software or the operating system.

### Trojans

A Trojan is a programme that enters your computer undetected, giving whoever planted the Trojan unrestricted access to the data stored on your computer. Trojans can transmit credit card information and other confidential data even if you are not accessing that data at the time. Catching Trojans requires the use of a Trojan scanner (a.k.a Trojan cleaner, Trojan remover or anti-Trojan). Trojans can be sent either as an email, spam mail, an attachment, or embedded in a web page. It is often preferable when closing down a site to use the 'File Close' instruction rather than click on the 'X' in the upper right corner of the screen.

### Spyware

A technology that assists in gathering information about a person or organisation without their knowledge. On the Internet, "spyware" is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties.

## BANKING SAFELY ON THE INTERNET

### Secure Your System

- Use a personal firewall.
- Always download and install authorised operating system updates.
- Run and maintain an anti-virus product on your home computer and update regularly.
- Do not run or install programmes of unknown origin.
- If using a local area network (LAN) contact your administrator and seek the availability of email gateway filtering for specific file attachments.
- Do not access your bank account from computers in Internet cafes or untrusted PC's as they may not be safe.
- Never leave your PC unattended when logged into Internet banking.
- Always ensure that you log-out properly when you have finished Internet banking.

### Secure Your Passwords

- Do not give your PIN or password to anyone else, including bank staff or Police.
- If you suspect your Internet banking password has been compromised, change it as soon as possible.
- Avoid using your birth date or name as your PIN or password. Passwords should be alpha numeric i.e. pencil37.
- Avoid storing passwords on your computer.
- Do not set up your computer so it 'autocompletes' or saves your password i.e. – do not tick the "remember this password" box.
- Do not use the same password on Internet banking as telephone banking.