Protecting Your Information Online

Customer security is the number one priority for banks regarding online banking. Banks provide advice and guidance; online, over the telephone and in many publications on how to protect against fraud perpetrated by criminals over the Internet.

When you access the Internet through e-mail or the World Wide Web, it's important that you safeguard your personal information. All users of the Internet have a responsibility to protect themselves against Internet crime, in the same way that they buy cars with safety and security features to protect themselves against injury or financial loss. This fact sheet prepared by the Australian Bankers' Association and the Australian High Tech Crime Centre will assist you with some practical tips and guidance on secure Internet practice.

WARNINGS ABOUT CYBERCRIME

Customers who bank online should be aware of the following methods which criminals attempt to convince you to reveal your confidential access information:

1. E-mails purporting to be from a bank or another legitimate business and asking for confidential information ('phishing' e-mails);
2. E-mails asking customers to be a sales agent for a good or service, with the promise of commissions delivered to your bank account (job scams);
3. E-mails purporting to be from a bank which ask customers to click on a link which sends them to a fake bank website ('ghost' website);
4. Trojans/spy ware - computer programs which conceal hidden programming which infect computers and are used by criminals to record and remit your access keystrokes or to destroy people's data.

If successful, through these fraudulent means, criminals can access your confidential online banking logon and password information which is then used to defraud accounts.

SIMPLE STEPS YOU CAN TAKE TO KEEP YOUR INFORMATION SECURE

1. Avoid being caught by fraudulent e-mails

'Phishing' e-mails are those sent to your e-mail address by criminals who want to steal your personal information. These authentic-looking messages appear to come from banks and legitimate businesses, but are designed to lure recipients into divulging personal data such as bank account numbers and passwords by your attempt to logon. Links within these fraudulent e-mails may also take you to fake or 'ghost' websites which are designed to fool consumers. It may look like an authentic website, with logos and homepage, but it is, in fact, another way criminals try to steal your personal information.

Tips:

- Never provide personal details including customer ID or passwords, in response to any e-mail. A bank will never ask you for your private password and this important information should never be shared with anyone.
- Never click on a link or attachment in an e-mail which purportedly sends you to a bank's website. Only access your bank's Internet banking logon page by typing the address into your browser.
- Be wary of any e-mail from someone you do not know or trust – delete without opening any e-mails that you think are suspicious.
- Always check your statements for any transactions that look suspicious. If you see any transactions that you did not undertake, immediately report this to your bank.
- Most 'phishing' e-mails do not address you by your proper name because they are sent out en masse to thousands of recipients. They sometimes contain typing errors and grammatical mistakes, even if they include the banks' registered logos.
- Install software that will filter spam e-mail or use an Internet Service Provider (ISP) that will filter spam prior to delivery at your Inbox. Spam filters are often included in anti-virus software.

If you have responded to a 'phishing' e-mail or if you have inadvertently entered your personal information on a 'ghost' website, it is always best to seek guidance from your bank. Do not delay in contacting your bank as staff can assist with advice on your next steps. Keep the bank's customer helpline handy at home. In addition, you should report the crime to your local police.

The bank will need to do an investigation if there is any suspicion that a fraud has been committed. If the investigation proves you are an innocent victim and have not contributed to the loss, the bank will refund the loss.

2. Tips for protecting your computer

It is important that you take positive steps to protect your computer if you are using e-mail, browsing websites and conducting e-commerce. Criminals try to defraud customers by use of Trojans which monitor keystrokes, enabling the criminal to record confidential information such

as online banking passwords and logon identification, as well as other material which is stored on your personal computer.

It is important to use only a trusted and secure computer to access your Internet banking account. Using publicly shared computers, such as those at Internet cafes, is strongly discouraged. If you use your home computer to access your Internet banking account, we recommend:

- Install reputable anti-virus and firewall protection on your computer because this provides additional layers of protection that you need to reduce your risk of exposure from viruses that can rob your computer of valuable personal information.
- Remember that after you install virus protection you will need to regularly update the software, usually by installing patches (used to update or fix a bug in a computer program), so the protection remains current.
- Install any security patches for your operating system and other software installed on your computer and keep these up-to-date.
- Read your bank's Internet banking security guide which can be found on the bank's website.

USING INTERNET BANKING

When banking on the Internet follow these steps:

- Always access your bank's website by typing the address into the browser.
- Keep your computer up–to-date with anti-virus, firewall software and the latest patches.
- Avoid using passwords or PINs (Personal Identification Numbers) that are relevant to your personal situation. Passwords with telephone numbers, postcode, your name, or the name of a close relative and dates of birth are simple for criminals to trace. Create passwords with letters and numbers that cannot be easily attributable to you.
- Always memorise your password or PIN and do not write it down or store it on your computer. You are responsible for keeping this information confidential.
- Change your password regularly and don't use the same password for other services such as your video store.
- Confirm that your data is encrypted between your computer and the bank by looking for the padlock symbol on the bottom right hand corner of the browser window.
- Always log out from the Internet banking menu when you finish all your banking.
- Close your Internet browser after logging out at the end of each Internet banking session.
- Beware of any windows that 'pop up' during an Internet banking session and be very suspicious if it directs you to another website which then requests your customer

identification or password.

HOW DO BANKS PROTECT MY PERSONAL INFORMATION?

Banks use a combination of safeguards to protect your information such as employee training, strict privacy policies, rigorous security and encryption systems. Banks have systems in place to constantly monitor online transactions. If banks come across a suspicious transaction, they will investigate it to ensure there is no breach of security. Occasionally, this may involve a bank staff member contacting you to verify a transaction. Banks will communicate with their customers regarding Internet security issues, often by publishing important information on their websites.

Some banks are working on the next step in security - two factor authentication systems. That means customers will identify themselves twice: first with something they know and then with something that they have. For example, using a password to logon to Internet banking and the bank might send an SMS message with a unique number to enter and authenticate the transaction. This unique number could also be generated by a device known as a security token.

The Australian Bankers' Association (ABA), its member banks, State and Federal police are working closely to tackle the problem of cybercrime. Bank staff have been seconded to the Australian High Tech Crime Centre (AHTCC) as part of a new team to continue the fight against fraud that occurs online. They are providing analytical assistance to police who will use this information to identify and prosecute criminals.

Banks work closely with State, Territory and Federal police to prosecute criminals who misuse customers' personal information or commit cybercrime. Each State and Territory jurisdiction has a range of offences which cover identity crime, including the unlawful possession of documents, operating accounts in false names and obtaining monies by deception. The penalties vary across each State and Territory but include large fines and incarceration, in some circumstances for up to ten years. Banks also work closely with other organisations such as the Australian Crime Commission and the anti-money laundering regulator, AUSTRAC.

WOULD YOU LIKE TO READ MORE?

Most banks have detailed information on their websites on how bank customers can protect themselves from Internet fraud attempts perpetrated by criminals. Take a look at your bank's website or give them a call for more information.

For further information from other organisations:

Organisation	Website Address
The Australian High Tech Crime Centre investigates crimes, which involve a computer or other piece of technology. It plays a significant role in reducing crimes such as hacking, denial of service (viruses, worms, Trojans), terrorism and money laundering.	www.ahtcc.gov.au
The Australian Securities and Investments Commission's consumer website FIDO has information on scams a swindles.	http://www.fido.asic.gov.au/fido/fido.nsf
The Australian Competition and Consumer Commission has a consumer protection role and their website publishe information about consumer rights.	www.accc.gov.au
State and Territory Consumer Affairs and Fair Trading - the role of these offices is to safeguard consumer rights and to advise businesses and traders on fair ethical practice.	
Australian Capital Territory	www.fairtrading.act.gov.au
New South Wales	www.fairtrading.nsw.gov.au
Northern Territory	www.nt.gov.au/caft/
Queensland	www.fairtrading.qld.gov.au
South Australia	www.ocba.sa.gov.au
Tasmania	www.tas.gov.au
Victoria	www.consumer.vic.gov.au
Western Australia	www.docep.wa.gov.au
Commonwealth Attorney-General's Department Identity Fraud Prevention Kit	http://www.crimeprevention.gov.au/agd/WWW/ncpHome.nsf/Page/Publications_All_Publications_Public_Safety_ID_Theft_-_A_kit_to_prevent_and_respond_to_identity_theft

Created: February 2005

Australian Bankers' Association: Free-call 1800 009 180 www.bankers.asn.au
Australian High Tech Crime Centre: Telephone 02 6246 2101 www.ahtcc.gov.au