AFG SECURITIES - INTERNET BANKING SECURITY

TRANSACT SAFELY ONLINE

Tips on passwords, Internet security and logging on.

We employ various security measures to ensure that your transactions and personal information are protected. However, you as a customer can also play a big part in protecting your banking and personal information. To help you, we have developed a number of tips and hints.

PASSWORD PROTECTION

To access your accounts, you will need your customer number and a personal "password". Your password protects the security of your information. Passwords will only keep outsiders out if they are kept secret!

Here are a few helpful tips to assist you in choosing and using your access code:

- When choosing a **primary password** (used to accesses your internet banking session), select something that you will remember easily but which will not be obvious to others. A password should have a minimum of eight characters and use uppercase letters, lowercase letters, symbols (@#$&) and numbers.

- When choosing a **secondary password** (for transferring and redrawing funds), select something that you will remember easily but differs from your primary password and will not be obvious to others. Your secondary password should have a minimum of six characters (maximum of 14) and use uppercase letters, lowercase letters and numbers. This password is entered via an onscreen virtual keyboard.

- Have a unique password for your internet banking. Avoid using the same password for different online applications. Doing so puts your money at risk should anyone discover your single access code.

- Do not choose a password that is easily identified with you (for example, your date of birth, telephone number or your name or any part of it).

- Keep your password confidential - you should not share or reveal your password to anyone. Do not disclose your password to anyone including a family member, friend or a lender staff member. Be wary of unsolicited calls or emails requesting personal information, password or card numbers.

- As an additional safeguard, it is advised that you regularly change your password; we recommend every 30 days. We will from time to time require a password change.

- Do not write your password down even if it is disguised.

Note: change your password, or notify us as soon as you suspect your existing password has become known or used by someone else.

INTERNET SECURITY

PUBLIC PLACES

- Be wary of your surroundings and ensure no one is observing you when entering in your Customer Number or password.
- Never click the 'save my password/details' option sometimes offered.
- Never change security details such as your password in a public place (i.e. libraries, Internet cafes).
- Do not leave your computer unattended or idle for long periods of time.
- Always log out from your Internet banking session when you have finished and close the browser.
- Try to use computers that have anti-virus software installed.

CLOSED PADLOCK – SECURE SESSION

When logging into or using Internet Banking, look for the closed padlock symbol at the bottom right corner of your web browser or at the right hand side of the web browser address bar. You can click on the padlock symbol to view the server security certificate's details. The certificate informs your browser that the web site you are connected to is in fact ours and not a "fake" site. The closed padlock images appear below.

HTTPS – SECURE SESSION

When using Internet Banking, check to see that you are correctly accessing our secure site by looking at the address bar at the top of your browser. Check to see that the web address begins with "https://". Web addresses that begin with "https://" are secured (unsecured addresses start with "http://").

VIRUSES

A computer virus is a program that attaches itself to another program, but changes the action of that program so that the virus is able to spread. Anti-virus software is designed to protect you and your computer against known viruses, worms and Trojans. A Trojan is a malicious program disguised as something harmless, such as a game or a screen saver, which in fact contains hidden code that allows an intruder to possibly take control of your machine without your knowledge.

New viruses are constantly appearing; viruses range from harmless pranks that merely show an annoying message, to programs that can destroy or disable a computer altogether.

- It's important that everyone who uses a computer is aware of proper security practices. Protect your computer with up-to-date antivirus software. You should regularly update your computer system with the latest anti-virus software.
- Avoid opening, running, installing or using programs/files you have obtained from a person or organisation that you do not know you can trust, especially unsolicited email containing file attachments
- Scan new programs/files/attachments for viruses before opening, running, installing or using them
- Ensure you have the latest available updates and anti-virus definitions for your anti-virus software. Unless your software is kept up to date it will quickly become ineffective at preventing virus infection
- You should regularly scan your computer with current anti-virus software to ensure your system is not infected by a virus

SPYWARE

"Spyware" is the collective name given to software that is installed on your computer to secretly obtain information and send it back to another source. Spyware programs can be installed through a virus or as part of another software installation e.g. a 'freeware' program.

Spyware can be removed from your computer by:

- Running a spyware remover program: special programs can be used to remove spyware that has been installed onto your machine;
- Virus checking: scanning your machine with a virus checker can remove any virus related spyware;
- Deleting cookies: deleting cookies from your browser can help spyware related problems; and
- Installing a personal firewall: a personal firewall will stop unauthorised 'attacks' to your computer from spyware sources. A personal firewall is particularly important if you have a permanent, high-speed connection to the Internet.

HOAX EMAILS

Be very cautious of emails that have a link to a website and/or an Internet Banking site that asks for personal details, your customer number, your Internet Banking password and/or credit card details.

- Only click on a link in an email if you are absolutely certain that it is from a reliable source.
- Do not click on emails where you do not know the sender or source and don't be duped by great offers coming through email.
- Think twice about forwarding an email with a "great offer" to a friend/relative.
- If you receive a suspicious email (especially ones purporting to come from a financial institution), do not act on the instructions contained in the email.
- Avoid opening suspicious or dubious emails or attachments, even if the email is from someone you trust (the email and attachment could have been forwarded automatically without the person's knowledge).
- You should not reply to "spam" emails or emails where you do not know the sender or source. It simply confirms that your email address is valid and you may receive further emails from them. You should simply delete the email.

Email is one of the prime movers for malicious viruses. Regardless of how enticing the "subject" or attachment may look, be cautious. Any unexpected email, especially one with attachments (from someone you may or may not know), could contain a virus and may have been sent without that person's knowledge from an infected computer. Should you receive an email of this kind and you are doubtful of its legitimacy, delete it.

EMAIL POLICY

We will never ask for your password or account details to be disclosed via a link within an email message. If you receive an email of this nature, please disregard the email, delete it from your computer and contact our Client Services team immediately on **1800 629 948**.

Our Internet Security Measures

Our website provides you with a range of security practices to ensure that your transactions and personal information are protected.

1. Firewalls
2. Encryption
3. Virtual Keyboard
4. Primary and secondary passwords
5. Incorrect Password Account Lock
6. Automatic Time-Outs
7. Last Login Time Check
8. Email Receipts

Firewalls

Our Internet Banking service is protected by sophisticated firewalls which maintain the secure perimeters between the Internet Banking site and the Internet. This provides full firewall protection that conceals the architecture of the internal networks from the outside world including protection against attacks.

Encryption

Whenever you use our Internet Banking service your information is protected by banking industry standard SSL (Secure Socket Layer) encryption. Encryption is a process of scrambling information using random mathematical algorithms ensuring that only we can receive this information in an understandable format. Security is provided in two different ways:

- authenticating the web server to the client using a digital certificate; and
- encrypting all information sent.

You can identify whether the Internet Banking session is secure or encrypted when you see a padlock in the bottom right corner of your web browser or at the right hand side of the web browser address bar. Clicking on the padlock will also provide you with details on the Security Certificate pertaining to the encrypted session.

Virtual Keyboard

Virtual keyboards are used to reduce the risk of keystroke logging (the action of logging the keys struck on a keyboard). Our Internet Banking site uses a virtual keyboard for secondary password entry when transferring or redrawing funds. It is more difficult for keystroke loggers & spyware to monitor the display and mouse to obtain the data entered via the virtual keyboard, than it is to monitor real keystrokes.

Incorrect Password Account Lock

With our Internet Banking site, after 3 incorrect attempts, access will be locked. This is to ensure that there is no unauthorised access to your account details.

If your account becomes locked, it will then be necessary to contact Client Services on **1800 629 948** to request that your Internet Banking access be reinstated.

To avoid incorrect password attempts, we strongly recommend that you have a password of your own choosing which will be easy for you to remember, and that you should also be aware that the passwords are case sensitive so you need to check your Caps Lock key.

Automatic Time-Outs

For your further protection, our Internet Banking system has been set to automatically "log out" after 10 minutes if your banking session remains unattended. This means that should you leave your computer for any

reason for longer than 10 minutes whilst conducting an Internet Banking session, the system will end your session to ensure that no-one else can access your personal information in your absence.

Last Login Time Check

Our Internet Banking system also provides you with information on the date and time of your last session. This allows you to check the most recent session each time you use Internet Banking to ensure that nothing is out of the ordinary.

Email Receipts

This security feature allows you to define which transfer and payment functions will send an email confirmation to your nominated email address when successfully performed. You can enable or disable this functionality through the Preferences options under Tools. For added security, any changes made to the Preferences will be emailed to the original email address.

Online Security Risks

As a customer you may be seen as a potential target for fraudulent activities. However by arming yourself with information and tools you can protect yourself from becoming a victim of fraud.

Email Scams and Fake Websites

A number of customers from Australian financial institutions have been targeted with hoax emails. These emails appear to be genuine bank emails.

Some emails inform the customer that their security details and passwords need to be updated by logging into an authentic looking, but fake website. The purpose of these websites is to obtain your log on details to access your Internet Banking accounts.

Others communicate security messages and advise you to install software from the email that checks and removes viruses. By downloading the software you are in fact tricked into downloading a virus.

Having used these or similar techniques to capture login and password details, fraud perpetrators are then able to illegally access accounts and withdraw funds.

Please note, we will:

- **never** ask for your Internet Banking login details via phone or email
- **never** use email to send you a link to an Internet Banking login page
- **never** ask you to communicate your passwords to us in any form

JOB SCAMS

We warn our customers and members of the public to be wary of various job scams advertised via the Internet.

Bogus overseas companies have been targeting Australian consumers to act as 'money transfer agents' in the sale of goods and services via methods such as fake job advertisements, unsolicited emails and online chat rooms.

'Employees' are asked to use their own bank accounts to transfer money overseas made from 'sales' in Australia. In fact, they will be transferring stolen money. In most cases, employees are instructed to send these funds to Eastern European countries. Employees are promised a percentage of the transfer as their commission.

The fake job advertisement websites look very professional and convincing. Please note some job advertisements contain Trojan Horses that allow the job advertiser to access the person's computer and collect their personal details, including bank account details. Exercise extreme caution if you receive an email from any person or company asking for your personal and banking details.

Finally, if it sounds too good to be true it probably is.

IDENTITY THEFT

Identity theft is where a dishonest individual or syndicate will gather your personal details in order to gain some sort of financial or other benefit, leaving you, the owner of that identity often in large debt with a negative credit history and in some cases with legal implications.

Identity theft can occur when a fraudster gets access to your personal information such as your date of birth, your address, your driver's licence number and information from utilities, phone and bank account records.

This can be obtained through:

- theft, including theft of mail from your mailbox at home
- by going through your garbage bins
- telephone scams
- Internet

Customers should:

- keep responsible care of all personal information to minimise the risk of loss/theft (e.g. by keeping tax records and other financial documents in a safe place);
- minimise the risk of mail theft by securing your mailbox (e.g. with a padlock);
- cancel unused credit union/bank/utility/phone accounts;
- securely dispose of any documents that may contain personal details (such as account statements, credit card transaction slips, bills, etc);
- regularly obtain a copy of your personal Credit File to make sure there is no unusual activity on your file; and
- promptly report to the police any loss or theft of personal documents.