



## Internet Banking Security

**We are committed to providing Members with a secure Internet Banking service and as such have placed additional security measures in place. Please see below for our Security Policy, smart browsing tips, a list of common security threats and security software and links to further information.**

NB: The information provided below is to assist Members to better understand Internet Banking Security. Liability for unauthorised transactions will be determined in accordance with the Credit Union's Internet Banking Terms and Conditions and the Electronic Funds Transfer Code of Conduct.

- 1. Our Policy**
- 2. Protect yourself - Smart Browsing Techniques**
- 3. Internet Threats**
- 4. Security Software**
- 5. Further Information**

### 1. Our Policy

#### **Two Factor Authentication**

At Victoria Teachers Credit Union we are committed to providing Members with a secure Internet Banking service. As part of a recent upgrade to our security, a second password known as the 'Funds Transfer Password' will now be required when you add a new Funds Transfer External payee in the 'Transfers' menu. The Funds Transfer Password is entered in an 'on-screen keyboard' using your mouse, which will further enhance the security of our Internet Banking service.

The on-screen keyboard is a simple tool that enables entering small pieces of secret text safely, using your mouse so no hidden Key Logger can find your text. You can use it to enter very secret passwords safely on non-trusted machines.

#### **Transaction Verification**

At Victoria Teachers Credit Union we place the utmost importance in ensuring that your funds are transferred correctly to a third party account. Internet Banking transactions may be put on a hold and reviewed by Victoria Teachers Credit Union if the transaction does not appear to be legitimate.

#### **128 Bit SSL Encryption**

Victoria Teachers Credit Union supports SSL 128-bit encryption, the highest level of protection possible during the Internet Banking session. SSL stands for 'Secure Sockets Layer'. It is a protocol designed to enable applications to transmit information back and forth securely. Applications that use this protocol inherently know how to give and receive encryption keys with other applications, as well as how to encrypt and decrypt data sent between the two. SSL has been universally accepted on the World Wide Web for authenticated and encrypted communication between the customer's computer and servers.

#### **Auto Log Out Feature**

Your Internet Banking session will automatically expire and log you out if there is inactivity for more than five minutes. This is done to reduce the risk of anyone stealing your session. Hence if you login and leave your session inactive for five minutes, the session will be terminated.

### **Monitoring Suspicious Activity**

We regularly monitor online transactions and investigate for any anomalies to ensure that your online security is not compromised. Occasionally, this may involve one of our Staff members contacting you to verify a transaction.

### **Last Login Time Displayed**

With each successful login you will be able to view your last login date and time. Please check these details to ensure that unauthorised parties have not accessed your account. If you have any concerns, please contact us immediately on **1300 654 822**.

### **Account Lockout**

To avoid any breach of Internet Banking security, access to your account will be locked after a third unsuccessful login attempt.

If you have any concerns, please contact us immediately on **1300 654 822**.

### **Audit Trails**

Detailed logs containing information about all Internet Banking transactions are recorded and archived. Such information is retained by Victoria Teachers Credit Union for internal purposes only, and will not be passed on without Members consent.

### **Host System Security**

Victoria Teachers Credit Union continues to provide a solid security framework to ensure Members Internet Banking transactions are processed in a secure environment, using industry standard global technologies.

## **2. Protect yourself - Smart Browsing Techniques**

There has been widespread media attention regarding online security. We recommend that Members take precautions to avoid the possibility of inadvertently getting caught by Internet scams or becoming a casualty of online fraud.

To protect yourself, you should:

### **Browsing Behaviour**

- Never access Internet Banking by clicking a link in an email.
- You should always type [www.victeach.com.au](http://www.victeach.com.au) in the address bar to access our Internet Banking service, alternatively access it via your Favourites/Bookmarks.
- Take extra precautionary measures while accessing Internet Banking from a foreign computer (*e.g. cyber cafes, public libraries*). If you have entered the login details on any shared computer other than that of your own, please change your passwords after such use from your own PC at your workplace or at home.
- Never click on an email that asks for your account details or your passwords. We will never ask for your account details or your passwords by email. If you receive this type of email, it's almost certainly a scam. If you have any doubt about an email that seems as though it has been sent by us, contact us immediately on **1300 654 822** to verify its contents.

### **Password Protection**

- Your Internet Banking User ID and password are your keys to accessing our Internet Banking service. Only the right combination of these allows you access.
- Always use an alpha-numeric password with a combination of numbers, upper and lower case letters with at least one special character, e.g. Rf3Tg#1.
- Avoid sharing details that you use to access other online services such as email or messengers. Your password should be unique to Internet Banking.
- Avoid obvious answers to the secret questions or passwords that others might guess, like names, birthdays or telephone numbers.
- Change your password regularly. Password(s) can be changed online at your own convenience.

- Do not write your username and password on a piece of paper or save it on your computer.
- Never disclose your login details to anyone, Victoria Teachers Credit Union will never ask for your login details in an email.
- Disable functionality on your computer or browsers that remembers login details.

### **Keeping Your Computer Secure**

You should ensure that your computer is kept safe and secure from unauthorised access. To protect yourself you should:

- Install effective protection on your computer and keep it up to date.
- Ensure that you have the latest security upgrades and patches for your Internet browser.
- Install an effective virus protection program, however most importantly you must regularly download the latest version and upgrades. If you have not upgraded for the past three months, your protection is probably inadequate.
- Install a 'firewall' to protect your computer from unauthorised access over the Internet.
- It is important to regularly review the settings of your security programs to ensure they are still providing an appropriate level of security.
- Delete suspicious emails without opening them. Avoid opening dubious attachments, even if the email seems to come from someone you trust.
- Do not leave a connected session unattended.
- Should you receive a fraudulent email or believe your accounts have been compromised, please contact us immediately on **1300 654 822**.

For more information visit <http://www.staysmartonline.gov.au/>

## **3. Internet Threats**

**Today, entirely new types of high-tech frauds are posing serious threats and challenges. Here is an overview of a few Internet threats we should be aware of.**

### **Adware**

Adware is any software application or program in which advertising banners are displayed or pop-up windows appear while the program is running. Adware is considered 'spyware' and is installed without the user's knowledge. It typically displays targeted ads based on words searched for on the Web or derived from a user's surfing habits that have been periodically sent in the background to a Web server.

### **Hacking**

Hacking means illegally accessing other people's computer systems for destroying, disrupting or carrying out illegal activities on the network or computer systems.

### **Key Logger**

A Key Logger (*Key Logger* or *Keystroke Logger*) is a program that runs invisibly in the background, recording all the keystrokes, usually saving the results to a log file. A Key Logger allows you to find out what other users do on your computer in your absence. It is designed for hidden computer monitoring and monitoring of computer activity.

### **Pharming**

Pharming redirects a user to a spoofed website by 'poisoning' the local domain name server (DNS). Poisoning a DNS server involves changing the specific record for a domain, which results in sending the user to a website different from the one intended unbeknown to the user. This type of attack involves Trojan Horses, worms or other technologies that attack the browser address bar, thus redirecting the user to a fraudulent website when the user types in a legitimate address.

Unlike in phishing, a pharming attacker does not have to rely upon users clicking on hyperlinks in emails. Even if users correctly enter the web address (*instead of clicking on a hyperlink*), the attacker can still redirect them to fake sites.

### **Phishing**

Phishing is a technique used to gain personal information for the purpose of identity theft, using fraudulent email messages that appear to come from legitimate sources, most commonly banks and other financial services providers. Such email messages aim to convince consumers to divulge account numbers, credit card details, and online banking passwords through the use of bogus websites that mimic genuine websites.

The latest being Spear phishing where emails appear to come from a company's human resources and target a single user or a department within an organisation.

### **Spoofing**

Email spoofing describes fraudulent alteration of an email 'header' to make it appear that the message has originated from someone or somewhere other than the actual source. The distributors of spam commonly use spoofing to hide or modify the origin of an email message, so as to entice the recipients to open and respond to their solicitations.

### **Spyware**

Spyware is software that is installed on a computing device and takes information from it without the consent or knowledge of the user and gives that information to a third party. Spyware is an intelligence gathering tool that targets sensitive information including banking and credit card details.

### **Trojan Horse**

A Trojan Horse is a program that installs malicious software while under the guise of doing something else. A Trojan Horse differs from a virus in that a Trojan Horse does not insert its code into other computer files and appears harmless until executed. The term is derived from the classical myth of the Trojan Horse. Trojan Horses may appear to be useful or interesting programs (*or at the very least, harmless*) to an unsuspecting user, but are actually harmful when executed.

### **Virus**

A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus can spread from one computer to many others through computer worms and Trojan Horses.

### **Worms**

A worm is a self-replicating computer program, similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program. A worm is self-contained and does not need to be part of another program to propagate itself.

## **4. Security Software**

Most home PC users are often not aware of the 'bots', 'tracking cookies', 'spyware', and other cyber pests that can exist on their systems. Some are harmless whilst some variants can cause unexpected behaviour, and at worst defraud the user of hard earned dollars. So what are the counter measures to combat such threats?

- Patch your system with the latest patches.
- Install a personal firewall.
- Install and keep current anti-virus software and malicious program detectors.
- Safe email practices.

Below is a list of websites<sup>1</sup> that offer software that may help you combat threats:

### **Anti-Spyware Scanner**

Lavasoft Ad-Aware SE Personal  
Spybot Search & Destroy  
PC Tools Spyware Doctor

### **Antivirus Scanner**

Trend Micro Antivirus (Special Credit Union Member offer)  
AVG Anti Virus Free

### **Software Firewall**

Microsoft Windows Firewall  
PC Tools Firewall

Furthermore, you could visit your local PC dealer or electrical superstore, which sell a large range of security solutions. Other excellent resources are The Green Guide in Thursday's 'The Age' newspaper and [www.cnet.com](http://www.cnet.com).

1. Victoria Teachers Credit Union does not endorse any of these services and shall not be responsible for the content of any other site accessed via Victoria Teachers Credit Union's website. These sites are listed for information purposes only. Victoria Teachers Credit Union will not accept any responsibility or liability for any loss or damage incurred by using any service, product or solution provided by these companies.

Any questions or issues you have about the software should be directed to the vendor. It is your responsibility to ascertain the suitability of the software and you will need to read the software and licensing terms and conditions before purchasing and/or downloading the software. Any information provided on the vendor's website will be subject to the vendor's privacy policy which Victoria Teachers Credit Union are not liable to you for any loss or damage you suffer as a result of you using the vendor's website and/or any other third party or disclosure of your information to the vendor or any other third party. We do not receive any commissions or fees from the sale of this product.

WARNING: Not all PCs have the capacity to run some of these software solutions. You should have a minimum of 256MB of memory, and be running WindowsXP operating system. If you have any doubts, many of the software solutions stated can easily be uninstalled if they have a detrimental impact on the performance of your PC. No software can protect you and your computer from all forms of threats, contamination, viruses, frauds and Trojans. It is also your responsibility to ensure your software is up-to-date.

## **5. Further Information**

For further information about Internet and email security, visit the following websites:

Australian Government Initiative  
<http://www.staysmartonline.gov.au/>

International Complaints  
<http://www.econsumer.gov>

Australian Securities and Investment Commission  
<http://www.fido.asic.gov.au>

Australian High Tech Crime Centre  
<http://www.ahtcc.gov.au>

Little Black Book of Scams Online  
<http://www.scamwatch.gov.au>

Australian Competition and Consumer Commission  
<http://www.accc.gov.au> or call 1300 302 502.

Protect your Financial Identity  
<http://www.protectfinancialid.org.au>