

Community CPS is aware of instances where international cheques received for the purchase of goods by persons overseas have been found to be invalid, stolen or counterfeit.

**10) Contact Community CPS immediately
if you think you have been scammed**

- If you suspect any communication purportedly from us is a hoax, or if you think that your Web-Link security or password has been compromised, then contact us via one of the mediums below:

Phone: (02) 6286 0555 Fax: (02) 6286 0560

Email: cps@cpsact.com.au

For more information about Web-Link security and general information in relation to safe Internet use, firewalls, virus scanners, fake emails & websites and online financial fraud, please visit the Community CPS Website at **www.cpsact.com.au**

Glossary of Terms

PHISHING: The act of sending an e-mail, falsely claiming to be an established legitimate enterprise, in particular a financial institution, in an attempt to scam someone into surrendering private information that will be used to transfer funds from their account.

SPYWARE: Any software which covertly gathers your information through an Internet connection without your knowledge, such as your password.

TROJAN: Trojans are files that appear to be something desirable but are in fact malicious. Generally you will be unaware that a Trojan file is on your computer unless you have software to either prevent it being loaded or detect it when it loads. Trojans contain malicious code that, when triggered, cause loss or theft of data by sending information from your computer, or your keystrokes, without your knowledge, over your Internet link. In order for a Trojan to spread, you must invite the program into your computer. Some Trojans will remain dormant on your computer until triggered by an event, such as visiting a particular website, while others may only activate if they are opened by the user. An example would be opening an infected email attachment or even clicking on a link within an email.

Contact Details:

Mail: CPS Credit Union Co-operative (ACT) Limited
Locked Bag 1000, Mawson ACT 2607

Tel: (02) 6288 0555

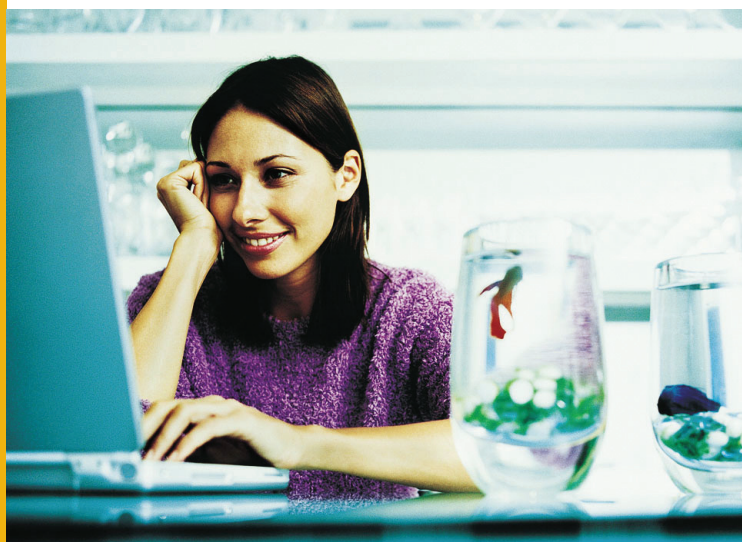
Fax: (02) 6286 0560

Web: www.cpsact.com.au

ABN: 31 087 649 670

AFS Licensed Number: 240672

Internet Banking Safety Tips



Community
CPS
CPS CREDIT UNION CO-OPERATIVE (ACT) LIMITED

Community
CPS
Life without a Bank

CUT 037 10/04

Life without a Bank

Internet Banking Safety Tips

There is an increasing trend for fraudsters to send scam emails relating to the Internet Banking services provided by financial institutions.

These emails appear to be authentic and ask the recipients to update their details and thus reveal login or credit card numbers. This practice is called 'phishing'.

Please disregard and immediately delete these emails from your personal computer, should you ever receive one.

Community CPS will never send you emails which ask for your password or account details to be disclosed via a link within the email message.

You should also never **access any Internet Banking service from a link within an email.**

Safety checks to protect yourself-

1) Keep your computer secure

- Install an effective virus protection program on your computer and take the time to keep it current by regularly downloading the latest updates from the virus protection company's official website. If you have not upgraded your virus protection software within the past month then your protection is most likely inadequate.
- Install 'firewall' software to protect your computer from unauthorised access over the Internet. This is particularly important for broadband users.
- Install 'anti spyware' software to protect your computer from 'spyware software'. Spyware is software that collects your personal information without first letting you know what information it is taking and without letting you decide whether this is OK or not. The information spyware collects can range from a list of all the Web sites you visit, to more sensitive information like usernames and passwords. Spyware can unknowingly be installed on your computer if you download music, free games, or other software from unfamiliar websites and websites you don't trust.

2) Delete suspicious emails and attachments without opening them

- Some fraudsters can lure you into opening an email or attachment that unknowingly installs a 'trojan', which allows someone to monitor your computer and access your accounts.
- Suspect a scam if you are asked for your account details or passwords via email. If you are sent an email asking you to disclose any confidential information such as your Web-Link password, even if the source appears legitimate, delete the email immediately and contact Community CPS.

3) Only enter Web-Link via the Community CPS Website by typing in the URL www.cpsact.com.au in the address bar of your web browser or by clicking on this address from your 'favourites' or 'bookmarks' list

- Never click on any hyperlink in an email. Scam emails often contain a hyperlink to a false webpage that often looks identical to the Internet Banking login page of a legitimate financial institution. This simply provides the fraudsters with another means of obtaining your account information and password, by recording your keystrokes as you attempt to login to the false login screen.

4) Never disclose your password to anyone

- Keep your Web-Link password and account details secure. Avoid recording your Web-Link password anywhere. If you must record your password then keep it separate from your account details and highly disguise it, so that it is not easily identified as your Web-Link password.

5) Change your password regularly

- Changing your password regularly will minimise the time available for intruders to guess your password and gain unauthorised access to your account.

6) Avoid using public computers to access Web-Link

- In some places, fraudsters have loaded software on public computers that record keystrokes. This software enables these fraudsters to obtain and use any account information and passwords entered on computers loaded with this software.

7) Check for the padlock symbol at the bottom right hand corner of your screen

- The padlock symbol appears when information is being transferred over a secure connection. However this is not guaranteed as some scam websites even show the padlock at the bottom of the screen to give a false sense of security.

8) Use the 'LOGOUT' function to quit Web-Link

- Always end your Web-Link session by clicking on the 'LOGOUT' function, rather than just closing down the application. This securely closes the connection to Web-Link and helps prevent fraudsters from accessing your Web-Link account.

9) Overseas Transactions via the Internet

Members should be extremely careful when dealing with persons or organisations in another country to ensure they are not victims of fraudulent activity. This warning applies to members that may consider selling goods through any Internet facility, either a public facility or through their own web site.

In particular members are strongly advised not to:

- Provide their account number and BSB number to anyone for the purpose of an overseas funds credit unless they are absolutely certain of the bona fides of the other party;
- Accept international cheques from any person or organisation in another country for the sale of goods without first verifying the identity of the other party and that the international cheque is valid. Goods should not be despatched until the cheque has been cleared by the drawing bank (there are likely to be considerable delays in obtaining clearance on any international cheque).