



## LYSAGHT CREDIT UNION LTD.

13 AUBURN STREET, WOLLONGONG NSW 2500

ABN 79 087 650 226

AFSL No. 244520

PO BOX 77

Port Kembla NSW 2505

Fax: (02) 4229 6099

Phone: (02) **4226 5900**

Springhill: (02) **4275 6988**

11 February 2009

### **SECURITY WARNING FOR INTERNET BANKING USERS**

Please be advised there has been an increase in fraud attacks on members utilising internet banking. The new method is being referred to as "In Session" Phishing. This works by tricking the user into entering personal details or Internet Banking login details by injecting a false webpage purporting to be from the financial institution while the user is online.

This webpage appears as a pop-up box and often comes in the form of a "Personal Details Update Request" or "Security Validation Request". The pop-up form can be convincingly branded and feature a seemingly genuine form which has the look and feel of a genuine banking communication. The fact that the phishing operates from the users PC when the user is in a session with the genuine institution website gives the impression that the pop-up is originating from the genuine website and must therefore be authentic.

PLEASE NOTE THAT LYSAGHT CREDIT UNION WILL NEVER:

- ASK YOU FOR PERSONAL DETAILS BY EMAIL, OR
- REQUEST THAT YOU RE-CONFIRM YOUR LOGIN DETAILS ONCE LOGGED IN.

We recommend all internet banking members take the following steps to keep themselves and their PC's secure:

- Make sure your computer has up-to-date Internet Security software installed and that it is working correctly.
- Preferably type your financial institution's website address into your browser. Never use a link to your financial institution that has been sent to you in an unsolicited email or that is on a website: These may lead to fraudulent websites.
- Always ensure the link to your financial institution is secure by looking for the https:// at the top of the screen in the address bar and check for the locked padlock symbol in the browser window. Click on the padlock to make sure it's current.
- Always log out from your Internet banking session when you have finished.
- Always close your Internet browser after logging out at the end of each Internet banking session.
- Ensure that you are aware of the security advice provided by your financial institution.
- If any windows 'pop up' during an Internet banking session, be suspicious, especially if it directs you to another website which then requests you to enter personal details of login details.
- Don't send your financial information via email to anyone.

If you have any further questions please contact the Credit Union.