



Internet Banking Security

Internet Banking Security

Internet Banking is one of the fastest and most convenient methods of conducting your banking. However, it is extremely important that you adhere to the following information to maximise your security whilst banking online.

- Always log into New England Credit Union's website by typing www.necu.com.au directly into the address field in your browser. Avoid using the drop-down or favourites menu to visit our website.
- A locked padlock symbol in your browser whilst logged into Internet Banking indicates that the site is secure.
- Always delete any email that asks for your personal banking information or has a link in it to NECU. These are known as phishing scams and they can take on many forms. A phishing scam aims to lure you into divulging account numbers and passwords.
- Never follow links or redirections from other websites if you intend to log into Internet Banking.
- Register for Verified by Visa. This service is free to NECU members and has added password protection which increases the safety of online transactions.
- Never divulge passwords over the telephone, mobile phone or in any other manner. Remember, NECU will never request this information from you.
- Never use Internet Banking at Internet Cafes or on unfamiliar computers.
- Beware of any windows that 'pop up' or other strange activity on your computer that occurs during an Internet banking session. Be very suspicious if you are directed to another website which then requests your account details or password.
- Never leave your computer unattended while you are performing financial transactions online.
- Always log off when you are finished using Internet Banking to avoid others accessing your account details.
- Make sure you have security programs such as a firewall along with anti-virus and anti-spyware software, including the latest updates, installed and active on your computer. Be sure to scan your computer for viruses and spyware regularly and never access the internet without your security software installed and active.
- Always scan unfamiliar software programs with your anti-virus and anti-spyware software before installation. Use caution before installing a program if you do not know or trust the software provider.
- Always make sure your computer's operating system has the latest updates installed. Updates for operating systems can usually be downloaded for free. If you use a Windows operating system ensure that automatic updates are turned on.

Protecting your Internet Banking Password

- Choose a password that you will remember, but cannot be easily guessed. Ideally your selected password will include some numbers as well as letters.
- For your protection NECU will prompt you to change your password every 3 months. If you ever believe someone may know your password then change it immediately.
- Passwords should be committed to memory. Never record your password on paper, your computer, mobile device or any other manner. Also, do not utilise functionality in your browser that automatically completes a password field.
- Do not share your password with anyone including friends and family. If you do, you may be liable to pay any losses due to fraud. New England Credit Union staff will never ask you to provide your Internet Banking password for any reason.
- Delete immediately any email requests for your password that claim to be from New England Credit Union. New England Credit Union will never request this information from you.

Preventing Hoaxes and Scams

If you become aware of a suspicious email, Internet or telephone hoax or if you think you have received a "scam", please contact NECU immediately on 132 067.

Important Information

New England Credit Union has limits in place for Internet Banking transfers. Please note that if you choose to increase your standard transfer limit your risk in relation to internet fraud will also increase.