Make sure your online banking is secure

Banking online provides a convenient way for Internet users to manage their accounts.

Internet banking fraud
If you bank online you should be aware of the dangers of attempts to steal your credentials by using fraudulent email messages that appear to come from legitimate businesses.
These authentic-looking messages often create a sense of urgency, and are designed to fool recipients into divulging personal data such as account numbers, passwords and credit card numbers.

Phishing
'Phishing' is a technique used to gain personal information for the purpose of identity theft. 'Phishing' emails give themselves away by telling you that there is a reason why you must provide personal details such as your Internet banking log on, password, credit card number or personal identification number by reply email or through a website. It is common for 'phishing' emails to contain links to a website that is a convincing replica of the financial institution's home page.

Financial institutions do not communicate with customers about account details by email. If you are concerned that you have been affected by a 'phishing' or other email scam, you should contact your financial institution immediately.

What you can do

To make sure that your online banking is secure, there are some things you can do:-
always type the address of your bank website into your browser; never use a link that has been sent to you by email
be suspicious of email that creates a false sense of urgency
ensure that you are aware of the security advice provided by your financial institution.

Extract below is from the Australian Bankers Association website

ADVICE TO BANK CUSTOMERS

ABA and bank advice to customers regarding ghost websites, phishing and trojans is as follows:

- Avoid opening unsolicited emails. Instead, delete them from the menu, then permanently delete them from your 'deleted items' folder;
- Never click on a link in a email which attempts to send you to a bank's website;
- Never log on to Internet banking other than by typing the address into your browser;
- If you do not have anti-virus software, we recommend you obtain anti-virus protection, run it and maintain it or use one of the many free tools available on the Internet;
- Use a personal firewall to prevent viruses from downloading onto your system or launching attacks against other Internet user's systems;
- Do not run any software program unless you are certain of its origin and function;
- If you are concerned you have been affected by an email scam or Trojan, please contact your bank immediately and change your Internet banking password.