



AUSTRALIAN BANKERS' ASSOCIATION



JOINT MEDIA RELEASE

IMPORTANT MESSAGE FOR INTERNET BANKING CUSTOMERS

27 October, 2005: The Australian Bankers' Association (ABA) and the Australian High Tech Crime Centre (AHTCC) are warning customers of an ICQ message which has been sent to users of ICQ¹ – an Internet-wide instant messaging service.

The spam ICQ message reads:

"The Australian Bankers Association (ABA), in partnership with the Australian High Tech Crime Centre (AHTCC).

has launched an important information campaign in relation to cyber crime....

*Need more information Go to
[www\(dot\)BNKINGFORAU\(dot\)com/traffic](http://www(dot)BNKINGFORAU(dot)com/traffic)"*

The ICQ message directed consumers to a website which installed malicious software to vulnerable computers. That website has since been removed from access by the general public.

In a bid to increase authenticity, the criminals have included in their ICQ message reference to the co-operative activities of the ABA and AHTCC including an education campaign designed to inform consumers about the methods used by criminals to commit online fraud.

Federal Agent Kevin Zuccato, Director of the AHTCC, said: "Consumers who have received this ICQ message should not reply to it and instead delete it. It is another example of a phishing attempt, where criminals try to lure consumers into providing their confidential banking details which can be used for illegal purposes."

David Bell, Chief Executive of the ABA, said: "Bank customers who have visited the website, contained in the ICQ message, should immediately contact their bank, so it can take protective measures on the customer's behalf."

Tips for Protecting Your Information Online

- Never provide personal details including bank account numbers or confidential passwords, in response to any e-mail. Neither the ABA nor a

¹ICQ (short for 'I Seek You') is an Internet-wide instant messaging service to which Internet users subscribe to communicate online.

bank will ask you for your private password and this important information should never be shared with anyone.

- Anti-virus and firewall protection should be installed and kept up-to-date on the home and business computer.
- Never click on a link or attachment in an e-mail which purportedly sends you to a bank's website. Only access your bank's Internet banking logon page by typing the address into your browser.
- Be wary of any e-mail from someone you do not know or trust – delete without opening any e-mails that you think are suspicious.
- Always check your statements for any transactions that look suspicious. If you see any transactions that you did not undertake, immediately report this to your bank.
- It is important to use only a trusted and secure computer to access your Internet banking account. Do not use publicly shared computers, such as those at Internet cafes, to complete Internet banking.

If you would like to read more about protecting your information online – visit the ABA website: www.bankers.asn.au or the AHTCC website: www.ahtcc.gov.au to obtain fact sheets:

- 1) Protecting Your Information Online
- 2) Protect Your Financial Identity
- 3) Small Business – Protect Your Business Information Online

For further information:

<p>AFP Media Emma Diffen Phone 02 6275 7100 Mobile 0407 245 786</p>	<p>Australian Bankers' Association Heather Wellard, Director Public Relations Phone: 02 8298 0411 Mobile: 0409 830 439</p>
---	---

ENDS