



26 August 2004

TO: All APRA regulated Authorised Deposit-Taking Institutions

## EMERGING THREATS TO INTERNET BANKING

Over the past year or so there has been a marked increase in the number of Internet-based fraudulent attempts to gain access to ADI customers' accounts. A number of Australian ADIs have been targeted. Unsolicited e-mails and/or fraudulent websites are used in order to trick people into disclosing confidential personal details such as user names and PINs/passwords. This is commonly known as "phishing".

The techniques used by perpetrators of these frauds include, but are not limited to:

- sending e-mails to customers asking them to provide their details. These e-mails use the ADI logos and copied graphics to mislead the customer into accepting the validity of e-mails and websites;
- faking domain names to appear as if they represent real ADIs; and
- using "frames" to redirect customers to ADI websites so that, while customers are transacting with the institution, their personal details may be captured via the fake website.

ADIs which provide e-banking services or communicate to their customers via e-mails should already be aware of such possible scams targeting their customers. They should have already implemented appropriate security measures to prevent, detect and respond to such "phishing" frauds and other scams of this nature.

Another trend is the increasing use of key-logger and Trojan attacks to gain confidential information from customers' PCs. APRA would like to remind ADIs that they have a responsibility to advise customers of the steps they need to take to securely operate their Internet banking accounts.

Given the risks to ADIs from these activities, APRA strongly recommends that all ADIs offering services over the Internet take the following actions if they have not already done so:

- introduce procedures to ensure that under no circumstances would a customer be asked to reveal their PIN/password. Customers should be reminded that your institution will not make unsolicited requests for customer information such as PINs and passwords through e-mail and this should be clearly visible on your institution's website and/or in account statements or other print mailings;
- implement strong authentication and control mechanisms to provide reliable safeguards against identity theft;
- actively seek out fake websites or other scams which target your institution;

- ensure appropriate limits are in place for online transactions; and
- ensure fully documented incident response procedures are in place which are communicated to all relevant staff members.

ADIs should, as a minimum, advise customers to do the following:

- change their password frequently and use passwords which are hard to guess;
- ensure they have anti-virus software and a personal firewall. They should update the anti-virus and firewall products with security patches or newer versions on a regular basis, and never install software or run programs of unknown origin;
- do not accept links or redirections from other websites or media for the purpose of logging onto your website;
- always look for the SSL encrypted connection, indicated as https:// and a padlock, as well as check your institution's name in the website's digital certificate; and
- always be on the alert for fake websites and suspicious emails purporting to be from your institution, and report these immediately.
- avoid using computers at public places, such as Internet cafes, to undertake any online banking functions.

In late May 2004, the Australian High Tech Crime Centre (AHTCC) launched the Joint Banking and Finance Sector Investigation Team to assist financial institutions in responding to threats such as phishing. The Australian Bankers Association (ABA) and the Credit Union Services Corporation Australia Limited (CUSCAL) have supported this initiative, which also involves the Australian Computer Emergency Response Team (AusCERT), and allows member entities to notify the team of any incidents targeted at their institution or its customers. In some cases it has been possible to shut down the offending sites within a very short timeframe. APRA strongly encourages those entities not already a member of this initiative to contact the AHTCC or AusCERT.

A number of banks have recently announced their intention to introduce two-factor authentication as a means of overcoming some of the recent threats. On 12 July 2004, the ABA announced the formation of the Online Authentication Taskforce to develop industry standards for enhanced authentication of on-line transactions. APRA supports these initiatives and strongly encourages the adoption of two-factor authentication on an industry-wide basis.

Should you have any questions or comments on this advice, please contact Mr David Pegrem, Manager, IT Operational Risk, on 02 9210 3324 or email [david.pegrem@apra.gov.au](mailto:david.pegrem@apra.gov.au).

Tom Karp  
Executive General Manager  
Supervisory Support Division