

NSW Department of Community Services Practice Notes on Internet fraud

FOR DoCS' FUNDED SERVICES ON INTERNET BANKING AND INTERNET PURCHASING FRAUD

The Department of Community Services recently published on the DoCS website the *Fraud Risk Assessment for Service Providers*. Since then there has been particular attention in the news about the dangers associated with Internet banking and purchasing. These dangers can be both internal and external to an organisation, and are being addressed in the Fraud Risk Assessment.

DoCS believes that these practice notes will be able to assist you to avoid those dangers.

INTERNAL DANGERS

These relate to potential fraud by any unscrupulous employees or management.

You would normally have in place controls to prevent bogus payments or misuse of funds, including: paperwork requiring two authorisations; cheques requiring two signatures; blank cheques not signed; and segregation of duties, for example between the purchasing officer and the person authorising payment.

Where your payments or funds transfers are done through the Internet banking process, you should also ensure that your organisation:

- Restricts Internet banking access to a limited number of authorised individuals, whose passwords are confidential to them and changed periodically, and deletes access when those people leave the organisation
- Requires any Internet payment or funds transfer to be authorised by two designated individuals. (Your bank can arrange this).

EXTERNAL DANGERS

These are mainly associated with criminals including computer "hackers."

Common methods used by these people to access your confidential online banking logon and password information to defraud your accounts, include:

1. E-mails purporting to be from a bank or another legitimate business and asking for confidential information ('phishing' e-mails)
2. E-mails asking you to be a sales agent for a good or service, with the promise of commissions delivered to your bank account (job scams)
3. E-mails purporting to be from a bank which ask customers to click on a link which sends them to a fake bank website ('ghost' website)
4. Trojan/spy ware - computer programs which conceal hidden programming which infect computers and are used by criminals to record and remit your access keystrokes or to destroy people's data.

Here are some tips to avoid these traps:

- Never provide personal details including customer ID or passwords, in response to any e-mail. A bank will never ask you for any private password and this important information should never be shared with anyone.
- Never click on a link or attachment in an e-mail which purportedly sends you to a bank's website. Access your bank's Internet banking logon page only 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, particularly if they have attachments.

- Avoid opening, running, installing or using programs or files you have obtained from a person or organisation that you do not know you can trust.
- Always scan new programs and files for viruses before opening, running, installing or using them.
- 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.
- Most 'phishing' e-mails do not address you by your proper name because they are sent en masse to thousands of recipients. They sometimes contain typing errors and grammatical mistakes, even if they include the banks' registered logos.
- Install software that will filter spam e-mail or use an Internet Service Provider (ISP) that will filter spam prior to delivery at your inbox. Spam filters are often included in anti-virus software.

If you have responded to a 'phishing' e-mail or you have inadvertently entered your personal information on a 'ghost' website, it is always best to seek guidance from your bank. Do not delay in contacting your bank as staff can assist with advice on your next steps. Keep the bank's customer helpline handy in the office. In addition, you should report the crime to your local police.

The bank may need to do an investigation if there is any suspicion that a fraud has been committed. If the investigation proves that you are an innocent victim and have not contributed to the loss, the bank may refund the loss.

The following steps should be followed for **Internet banking**.

- Always access your bank's website by typing the address into the browser.
- Keep your computer up-to-date with anti-virus, firewall software and the latest patches.
- Use passwords or PINS (Personal Identification Numbers) that are easy to remember but hard to guess. They should not be relevant to your personal or work situation. Passwords with telephone numbers, postcode, your name, or the name of a close relative or work colleague, and dates of birth are simple for criminals to trace. Create passwords with letters and numbers that cannot be easily attributable to you or your organisation.
- Always memorise your password or PIN and do not write it down or store it on your computer, including in any system or on the programmable function keys. You are responsible for keeping this information confidential, even from relatives and friends.
- Change your password regularly and don't use the same password for other services such as your video store.
- Confirm that your data is encrypted between your computer and the bank by looking for the key or padlock symbol on the (usually bottom right hand) corner of the browser window.
- Always log out from the Internet banking menu when you finish all of your banking.
- Close your Internet browser after logging out at the end of each Internet banking session.
- Beware of any windows that 'pop up' during an Internet banking session and be very suspicious if it directs you to another website which then requests your customer identification or password.
- Avoid using shared computers at public places, such as Internet cafes, to conduct your Internet banking.
- Look after your account details if you save or print them after electronically accessing them from the bank's system. Keep this information in a safe and secure place or destroy it once you have finished with it.

You should take the following precautions when conducting **Internet purchasing** for your organisation:

- Deal only with merchants in whom you have a degree of trust - for example, those with a reputable trading name or brand, or from whom you have previously purchased goods in the store or over the telephone.
- Look for the merchant's contact details on their website and call them to help verify their authenticity. Ask friends and colleagues if they have successfully purchased from the merchant previously.
- Look for the key or padlock symbol on the merchant's web browser. This will indicate whether or not the merchant's site offers an encrypted line of communication to protect your details.
- Do not send your credit card details via insecure means such as e-mail that is not encrypted.

Further information can be obtained from your bank directly or from its website.