

Protecting your PC for safe online banking

Help us to help you

Northern Inland takes the security of its Members' funds and information very seriously. We put all reasonable measures in place to secure online facilities, but Members need to take steps to secure their personal computers (PCs) as well. This information sheet provides explanations of computer security terms and guidelines for keeping your online funds secure.

If you are unable to follow these guidelines, do not use NetTeller.

Internet-related fraud is increasing.

Malicious software, spyware and viruses can render your PC inoperable and your information can be copied, making your online transactions a target for fraud.

For more information contact the Privacy Officer at PrivacyOfficer@nicu.com.au or on 1300 65 65 81 or visit www.staysmartonline.com.au.

Northern Inland Credit Union Limited

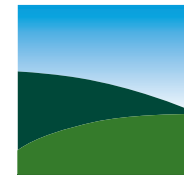
ABN 36 087 650 422

AFSL 235022

481 Peel Street Tamworth
142 Bridge Street Tamworth
252 Conadilly Street Gunnedah
73 Maitland Street Narrabri
Agency: 132 Merton Street Boggabri

Contact us: 1300 65 65 81

www.nicu.com.au




Northern Inland
C R E D I T U N I O N

Internet Security

Effective 05/03/2009

SMART THINKING

Keeping your online banking safe and secure: data encryption is the typical method by which all legitimate online banking, online shopping and other secure websites keep your details private as they get transmitted over the internet. Northern Inland uses this method to encrypt all information sent between your PC, our website and NetTeller. This is done over a secure internet connection using strong 128-bit encryption. The secure connection between your browser and our server uses a technology called Secure Sockets Layer (SSL). This is a well-respected technology developed by Netscape, Microsoft and RSA Inc, and is supported by most browsers.

You can confirm you are connected securely during a NetTeller session by checking for a lock icon  in the bottom (status bar) of your browser. Double-click on the icon to get the security certificate information to verify it came from Northern Inland's secure server by finding the following server information displayed on the certificate: 'secure.nicu.com.au' for our website and 'netteller.tsw.com.au' for a NetTeller session.

A **virus** is a program which can be unknowingly downloaded by visiting a website, received in an infected email, or through the use of an infected USB stick or CD. It attaches to existing programs on your PC and modifies their operations so the virus can propagate. Help prevent viruses by only opening emails and attachments from reliable sources you are expecting to contact you. Avoid opening emails with attachments ending in .exe, .cmd, .bat, scr, .pif. These often indicate the attachment contains a virus or worm. Do not click on links in emails from unknown sources.

Spyware refers to software that collects information about a user without their knowledge and reports that information to a third user. Spyware can copy passwords, credit card numbers and other identifying data as you type them into your computer or copy it from your hard drive.

A **firewall** helps protect your PC from some malicious software. It is a single point between networks where all traffic passes, to filter out suspicious locations. A good firewall means Internet hackers will look elsewhere for an unprotected PC.

Obtain **antivirus, spyware detection and firewall software from your software** distributor or directly from the web. To keep up to date with new threats update your antivirus software at least weekly. Ensure your selected software can run automatic updates when you access the Internet. This saves you the hassle of remembering to update.

Access web pages directly. Don't use a link in an email to get to any web page. Log onto Northern Inland's website by typing the web address in your browser: www.nicu.com.au.

Only download files and programs from reputable sources. For Windows operating systems, see <http://windowsupdate.microsoft.com>. For other software, use the legitimate websites of the company who produces it.

Avoid shareware or freeware unless it has been recommended by a trusted company. Think before you install something, or use other media in your computer. Weigh the risks and benefits, and be aware of the fine print. Does the lengthy licence agreement you don't want to read conceal a warning you are about to install spyware?

Increase the security on your custom settings. Check the following under Tools, Internet options, to ensure the settings are at satisfactory defaults. You may decide to:

- Reset defaults on the Programs, Advanced and Security tabs
- Clear cookies, history and files on the General tab
- Turn off the Autocomplete on the Content Tab. This feature stores passwords that can be cracked by hackers
- Connect Tab: it is safer to disable the autodialing feature and create a desktop shortcut to the Dial up networking properties. This helps to stop 1900 dialler programs and Spyware. Tick "Never dial a connection"
- Security Tab: the default setting is "MEDIUM". Select HIGH if visiting higher-risk sites for freeware and shareware.
- Privacy Tab: the default setting is "MEDIUM".
- Content Tab: enable Content Advisor to help block adult sites. Keep a discreet record of the password you use, as you will need it to change future settings.
- Check AV program settings: increase the protection levels to as high as possible.

Keep your account information, PINs and codes confidential and safe. How careful are you with your secret access codes? Be on your guard: some impostors will say and do anything to make you reveal your account details and codes.

Phishing attacks use email and websites designed to imitate the communications of actual financial institutions. Their objective is to fool recipients into divulging details such as credit card numbers, account usernames and passwords. Under the guise of fake security and maintenance upgrades, phoney investigations, and sham bills and charges, some customers of other financial institutions have been tricked into giving out information.

Be suspicious of any email with urgent requests for personal financial information. Northern Inland will NEVER request this information by email or telephone: we will ask you to contact us instead.

Do not reply to unsolicited email or telephone requests for account numbers, NetTeller passwords, PINs or code information. Telephone Northern Inland on 1300 65 65 81 if you receive any email, purporting to be from us, which you believe to be suspicious.

Take care when giving out personal information. Avoid filling out forms in email messages asking for financial information. Only communicate information such as credit card numbers or account information via a secure website or by telephone when it is unavoidable.

Use Verified by Visa when shopping online. Have peace of mind by registering your password and Personal Assurance Message (PAM). Your password is as easy to use as your PIN at an ATM - and it means you are the only one who can use your VISA card to make purchases over the Internet from participating merchants. For added security, your PAM confirms you are connected to a legitimate website, and your card is being authenticated by NICU. NICU offers this service to all of our VISA credit cardholders. For new and replacement registration numbers, contact Northern Inland on 1300 65 65 81.

What you can do right now to start making your online banking even more secure:

Make sure NICU has your up to date contact details. Include mailing address, email, daytime and after hours telephone numbers. If we see an unusual transaction on your account, this will help us to quickly contact you.

Check your statements. Regular checks of your accounts help you to quickly identify any unauthorised transactions. Contact Northern Inland immediately if you detect any attempted or successful access to your account which was not performed by you or any of your authorised signatories.

Choose secure access codes. Include a mix of capital and lower case letters, numbers and punctuation marks. Select a code that is easy for you to remember, but not easy for anyone else to guess. Avoid using the same code for a number of different services or uses.

Select notification by email. Receive an email when any transaction is performed on your account via NetTeller. Log in to NetTeller. Select 'Personal', then 'Personalise Settings'. Ensure a tick is next to 'Send email confirmations'.

Set transfer limits. Do you regularly use your full daily limit in NetTeller transfers? If not, consider lowering your daily limit. This will reduce the risk to your funds if an unauthorised transaction does occur. Contact Northern Inland via the secure email connection after you have logged into NetTeller, or call us on 1300 65 65 81.

Ask us about NetToken. We offer a second level of authentication in a small security device which fits on your key ring. Your local branch staff would be pleased to give you a demonstration.

Select a Northern Inland password and change it from time to time. This password helps our staff to identify you when you telephone us or visit a NICU branch. Only Northern Inland and you should know your password. Your password is only an identity security measure. It does not give you access to any product or service. It is the only password or code we will ever ask you for. You can change this password at any time by attending at a branch and producing your photo identification.