



Internet Banking Security

There can be no doubt that the internet has revolutionised all aspects of our lives, however, the increase in internet usage has also exposed computers to the threat of virus attacks. The internet makes computers prone to viruses and other illegal software designed to let outsiders gain access to your details and see the data on your computer.

The Risks

- **Risk 1:** Your computer can be controlled by a remote computer. This means that all the information stored in your computer will be accessed by another unknown remote user (including credit card numbers, passwords, sensitive information from accounting or tax software, etc.).
- **Risk 2:** Your computer can be affected by a virus or worm, which makes your software and hardware act unusually.
- **Risk 3:** Unknown software may be installed on your PC, which can transfer data from your computer to another computer.

Internet Banking is one of the fastest and most convenient methods of conducting your banking. However, it is extremely important that you adhere to the following information to maximise your security whilst banking online.

Browser safety - upgrade to help stay secure:

Fraudsters have rapidly adopted web browsers as a key means of installing malicious software on computers. Criminals can achieve widespread infection of multiple computers by hiding their viruses in a mix of popular and high-traffic websites. Alternatively, they lure users through email spam containing links directing potential victims to web servers hosting their malicious content. This is commonly known as a “drive-by download”, due to the fact that viruses can infect your computer simply by visiting a compromised site.

Since the year 2000, web reports have indicated that more than 90% of attacks on users and vulnerable websites have occurred as a result of drive-by downloads. As popularity of this style of attack has grown, there have been frequent reports of hundreds of thousands of Web sites being affected. In 2007, Google uncovered more than three million malicious Web addresses (URLs) that initiate the spread of viruses. Estimates made in 2007 indicate that more than 600million users are at risk simply from not using the most up-to-date web browser versions. That number is greatly increased today.

NSS Labs, an expert agency that specializes in web security, have tested many of the more recent and popular web browsers for their ability to block or protect the user from such attacks. For the abbreviated report and in depth report, click on the links on our website (www.communitymutual.com.au/net_security.html). It should also be noted that older versions of browsers have such a low catch rate that they did not get rated (eg. Internet Explorer 7 blocked less than 4% of the attacks).

A good virus scan:

It's recommended to have an Antivirus program (such as AVG, McAfee, Norton or Trend Micro) installed and running on your computer. There are several anti-virus programs available and you should select one that provides the maximum number of features such as internet security, spam filtering, email scanning and many more. It's always recommended that you update your installed antivirus program and scan your computer for viruses as regularly as possible (about once a week is recommended).

Protect yourself from dangerous emails:

Emails are now considered one of the major internet threats. Fraudsters are increasingly using e-mails in an attempt to lure consumers into providing personal information or to spread viruses. Some emails may also carry spyware or trojans directly to your computer when opened. To stay safe from such threats we recommend you use an antivirus program that has an email scanning feature. Another very important thing to do is to only open e-mails from sources you trust. Many e-mail providers have an option for screening all e-mails from contacts that are not on your friends list.

Delete all of your spam without reading it:

Never click on a link to “unsubscribe” from a spam email, as it may lead to more spam. Some email services allow you to automatically filter out e-mails that are not on your contacts list, this is a handy service to use.\

Don't give your personal information on the internet:

It is not recommended to give your personal information out over the internet unless you are totally confident that the organisation you are dealing with is legitimate. For example credit card number, full name, address and phone number,

should never be provided unless there is evidence that you are providing them to a legitimate company and some form of structured security system is being used to capture your information. Always read the terms and conditions agreement carefully when you are creating a new profile or account in any website.

Back up all of your important files on a regular basis:

Make two copies of all your important files. Keep one of the copies at work and another at home for added security, and be sure to destroy the old backup copies as you make new ones so no unauthorised person can have access to them. Additionally try not to leave them in a place where they are connected to the internet.

Download protection:

Do not download any software (games, programs), images, videos or music that are available for free on websites if you don't know the website source. Any files that you download should be scanned for viruses before you open them and any programs should also be scanned to be sure no malicious code has accompanied the download.

What can you do:

- Upgrade your web browser so that you are using the most up to date version. According to the NSS Labs reports Internet Explorer 8 and Mozilla Firefox are the two most secure web browsers for stopping viruses downloaded by visiting infected websites.
- Always log into The Community Mutual Group's website by typing www.communitymutual.com.au directly into the address field in your browser.
- A locked padlock symbol in your browser window whilst logging into Internet Banking indicates that the site is secure.
- Ensure your internet connection has a password, ESPECIALLY if you have a wireless network as this type of network can be easily accessed by a third party if no password is in place.
- Always delete any email that asks for your personal banking information or has a link in it to CMG. These are known as phishing scams and they can take on many forms. A phishing scam aims to lure you into divulging account numbers and passwords. The Community Mutual Group staff will never ask for your internet banking login or password details.
- Never follow links or redirections from other websites if you intend to log into internet banking.
- Register for Verified by Visa. This service is free to CMG members and has added password protection which increases the safety of online transactions.
- Never use internet banking at internet cafes or on unfamiliar computers.
- Beware of any windows that 'pop up' or other strange activity on your computer that occurs during an internet banking session. Be very suspicious if you are directed to another website which then requests your account details or password.
- Never leave your computer unattended while you are performing financial transactions online.
- Always log off when you are finished using internet banking to avoid others accessing your account details.
- Make sure all the programs that are involved with the internet are fully updated. This includes your browsers, antivirus software, windows (or other) firewall software and your operating system. This should be done as often as possible. Most of these programs can be set to automatically detect updates on a set timer (daily is best).
- Always scan unfamiliar software programs with your anti-virus and anti-spyware software before installation, especially if you do not know or trust the provider.

Password Tips:

- Your password should be one you can remember, but one that cannot be easily guessed. Eg: don't use your birthday, a friend or family members name, a pets name etc.
- It should contain both letters and numerals; capitals and lower case letters. Ideally a password would be a random sequence of letters and numbers and, as long as you can remember them this is a strong solution.
- For your protection, The Community Mutual Group will annually prompt you to change your password. If you ever believe someone may know your password then change it immediately.
- Passwords should be committed to memory. Never record your password on paper, your computer, mobile device or any other manner. Also, do not utilise functionality in your browser that automatically completes a password field.
- Do not share your password with anyone including friends and family. If you do, you may be liable to pay any losses due to fraud. The Community Mutual Group staff will never ask you to provide your internet banking password for any reason.
- Delete immediately any email requests for your password that claim to be from The Community Mutual Group. Our staff will never request this information from you.

Preventing Hoaxes and Scams

If you become aware of a suspicious email, internet or telephone hoax, or if you think you have received a "scam", please contact us immediately on 132 067.

Important Information

The Community Mutual Group has limits in place for internet banking transfers. Please note that if you choose to increase your standard transfer limit, your risk in relation to internet fraud will also increase.