

NetBank security guide



Determined to be different

Contents

Page	Section
4	Peace of mind with NetBank
5	What are the common online dangers?
5	Computer viruses
5	Hoax and scam emails
7	Identity theft
7	Social networking
9	How do we protect you?
9	Transactions monitored by dedicated staff
9	NetBank website identity verification
11	Encrypted data
12	Independent security audits
12	Automatic timeout periods and password lockout
13	What can you do to protect yourself?
13	Secure your computer
13	Optimisation check
14	Internet security package
14	Update your operating system
14	Using Microsoft Windows Security Centre
16	Register for NetCode
16	Create an additional login
16	Receive security notifications by email
17	Review your NetBank login and activity log
18	What should you do now?
18	NetBank security checklist
19	Understanding the security features of your browser
19	Internet Explorer 7 (Microsoft Windows)
20	Firefox 3 (Microsoft Windows, Apple Mac OS X)
21	Safari 3.2 (Microsoft Windows, Apple Mac OS X)

Contents

Page	Section
22	Further information
22	NetBank
22	Register for NetBank
22	Learn more about NetCode SMS and register
22	Security Centre
22	Internet security packages
24	Further online security information
24	Protect Your Financial Identity
24	Stay Smart Online
24	NetAlert
24	Scam Watch

Peace of mind with NetBank

The internet has changed the way millions of Australians communicate, share information, shop, and do everyday banking. With 24/7 access from around the world you can view balances, transfer funds and lots more at your convenience using NetBank – Australia’s most popular online banking service.

The Commonwealth Bank is committed to keeping you safe online and uses state of the art fraud prevention and detection technology, monitored around the clock by a dedicated team, to actively protect your finances and confidential information.

You also have an important role to play in security. By taking the simple measures outlined in this guide to protect yourself online you’ll enjoy peace of mind when using the internet and NetBank.



The safety of your money is 100% guaranteed.

This means we’ll cover any loss should someone make an unauthorised transaction on your account using NetBank – provided you protect your Client number and Password, and immediately notify us of the loss, theft or misuse of your password and of any suspicious activity on your account.

What are the common online dangers?

Computer viruses

As the internet has grown in popularity, cyber-criminals have seen an opportunity to prey on unwary users for financial gain.

Using Computer Viruses and Trojans, they target and infect unprotected computers to gain access to logins and passwords as you surf the internet. These Viruses often record key strokes, mouse clicks or take a snapshot of your screen without your knowledge, when you visit secure sites that require your credentials and send this information to the waiting cyber-criminals.

Computer viruses are usually spread through email attachments (including URL links to websites), which might appear to be sent by a friend or trusted source, and files downloaded from the internet.



Tip

Every computer used to access NetBank needs an internet security package installed to protect you from viruses. Learn more about internet security packages on page 13.

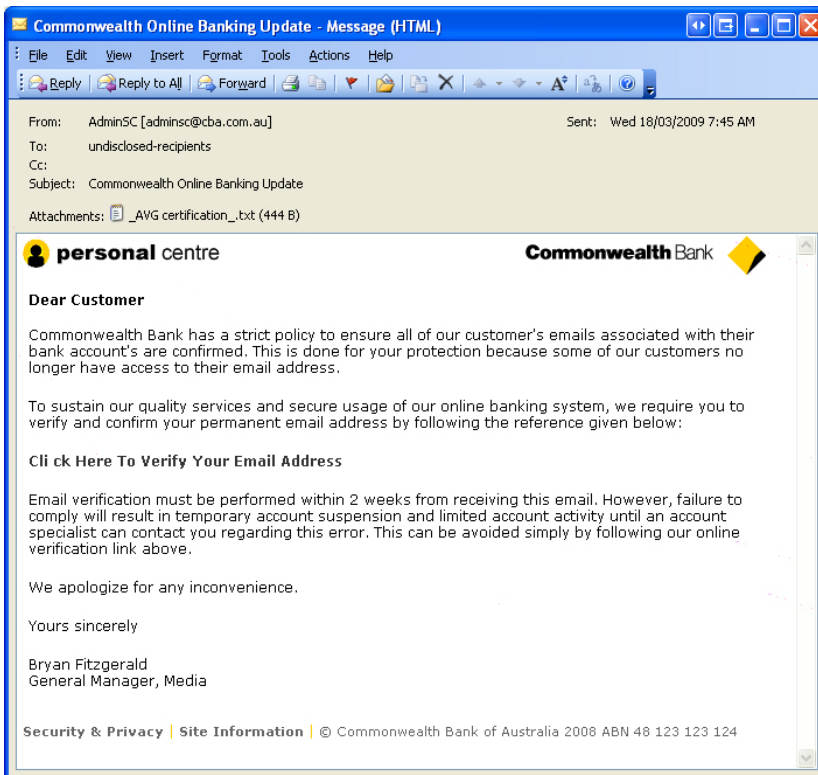
Hoax and scam emails

Emails are a great way to stay in touch with friends and family. Unfortunately, criminals also use the popularity of email to target unsuspecting customers with fake messages asking for their personal details or money.

Hoax emails, commonly referred to as phishing, can appear to be from the Commonwealth Bank and ask you to update or confirm details such as:

- ▶ NetBank client number
- ▶ NetBank password
- ▶ Personal identification questions
- ▶ Contact details
- ▶ Account numbers

The Commonwealth Bank will **never** send you an email asking you to confirm, update or reveal your confidential banking information. You can see an example of a hoax email below:



Please send suspected hoax emails as an attachment to hoax@cba.com.au. If you have responded to a hoax email, call the NetBank Help Desk immediately on **13 2221** and **select option 4** (24 hours a day, 7 days a week).

Scam emails promise a quick and easy way to earn large amounts of money. There's a range of different scam emails, with new ones appearing all the time, but the examples below outline the main types:

'Nigerian 419' scams promise huge financial rewards if you help someone transfer money out of their country by paying fees or giving them your bank account details.

Up-front payment scams ask you to send money upfront for a product or 'reward'. You'll end up with something much less than you expected or more than likely nothing at all.

Transferring money for someone else is basically letting criminals use your bank account to 'launder' their dirty money – this is illegal and you may be prosecuted.



Tip

Scam emails appear too good to be true – and that's because they are!

Identity theft

Identity theft occurs when criminals use your personal information for profit – by applying for credit, running up bills and not paying creditors – while pretending to be you.

These criminals use viruses, hoax emails and social networking sites (described below) to gather information needed to 'steal' your identity like your name, credit card details, address, date of birth, bank account, debit card details and driver's licence, and then commit fraud in your name.

Social networking

Social networking sites, such as Facebook, MySpace and LinkedIn, are online communities of people who share interests and activities and offer a range of ways to connect and communicate with other people. Unfortunately they also offer criminals another way to gather information for identity theft.

To protect yourself while using these social networking sites:

- ▶ Make sure your profile pages can only be accessed by people you trust, and not the general public, by changing the security settings
- ▶ Never publish personal or sensitive information such as your birthday, driver's licence number, tax file number or bank account details
- ▶ Don't publish contact details such as your home address or phone number



Tip

NetCode is a highly effective and convenient authentication system requiring passwords you only use once to authorise certain NetBank activities and transactions. Learn more about this free service and how it can protect you on page 16.

How do we protect you?

The Commonwealth Bank takes the security of your money and personal information very seriously. We're a leader in online banking security and are committed to providing you with the most secure banking environment possible. Our key security measures include:

Transactions monitored by dedicated staff

We have dedicated security staff who use advanced monitoring software to identify potentially fraudulent activity when it occurs and take necessary preventative action until we can establish whether the activity is genuine or not.

Our security staff also work closely with law enforcement agencies including the Australian Federal Police and Australian High Tech Crime Centre (AHTCC) to fight online crime.

Our transaction monitoring, which is industry-leading, is backed up by the NetBank Help Desk, available on **13 2221 option 4** (24 hours a day, 7 days a week).

NetBank website identity verification

When the address bar in your web browser turns green, it means the website you are visiting has an Extended Validation certificate.

NetBank has attained the highest level Extended Validation certificate through an extensive independent audit by VeriSign – the leading internet identity verification organisation based in the United States. The green address bar displaying '**Commonwealth Bank of Australia (AU)**' is a clear visual sign you have reached the genuine NetBank website and your session is protected with encryption.

Browsers that support Extended Validation certificates include:


- ▶ Internet Explorer 7
- ▶ Firefox 3
- ▶ Safari 3.2
- ▶ Google Chrome

The green Site Identity Button tells you that the site has fully verified identity information about the owner (in this case the Commonwealth Bank of Australia) and that the connection is encrypted.

The 'https' in the web address tells you that you are using SSL encryption (SSL is short for Secure Sockets Layer and was developed to transmit private data via the internet). The 'commbank.com.au' before the forward slash tells you that you are using a Commonwealth Bank website.

NetBank - Logon - Mozilla Firefox

Commonwealth Bank of Australia (AU) <https://www3.netbank.commbank.com.au/netbank/bankmain>

CommonwealthBank  [Close](#)

* = Required

Log on to NetBank

*Client number


*Password

LOG ON

Need help?

- ▶ [Forgotten client number](#)
- ▶ [Forgotten password](#)
- ▶ [NetBank centre](#)

Register online now


 **Is your computer performing at its best?**
Check your browser version and settings with our simple test to see if your NetBank experience can be improved.

- ▶ [Run the optimisation check](#)

Current highlights

- ▶ [Money Magazine's Website of the Year 2008.](#)
- ▶ [BPAY virtually anything.](#)

[Terms of use](#) | [Security](#) © Commonwealth Bank of Australia 2009 ABN 48 123 123 124

www3.netbank.commbank.com.au 

The yellow lock means that there is an encrypted connection.

Encrypted data

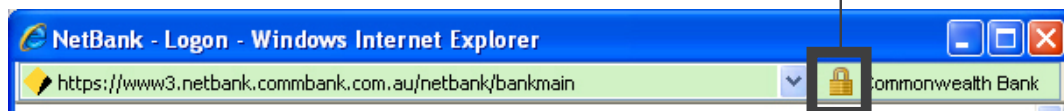
All information sent between NetBank and your computer is encrypted which means the information is unreadable to anyone but you. The encryption technology ensures confidentiality and gives you peace of mind. A padlock symbol is displayed on your web browser to let you know you are viewing a secure web page.

Where is the security padlock?

Internet Explorer 6 - at the bottom right of the screen



Internet Explorer 7 - at the top right of the address bar



Firefox 3 - at the bottom left of the screen



Safari 3 - at the top right hand corner of the screen



You can also tell if you are viewing a secure web page by looking at the text before the website name at the top of your browser, in the address bar. When you see '**https**' you can be assured the page is secure.



Independent security audits

Commonwealth Bank regularly employs independent security consultants to confirm the security of our systems. The work undertaken includes reviews of areas such as architecture, firewall configurations (a firewall prevents unauthorised access to computer networks), the security of our web server and the security of the different applications on our site.

Automatic timeout periods and password lockout

If you're logged in to NetBank but haven't been using it for a certain period of time, NetBank will automatically log you out to reduce the risk of anyone else accessing your banking details if you leave your computer unattended.

If someone does try to guess your password, your account will be locked after a set number of unsuccessful attempts. This protects you against criminals trying to guess your password.

What can you do to protect yourself?

While we take every available security precaution to protect your money and confidential information, there are also a number of important steps you should take to protect yourself from online threats such as viruses and identity theft. Below are five key steps to using NetBank and the internet safely:

1. Secure your computer

To use the internet safely first you need to make sure your computer is secure. Taking the steps below to protect your computer not only saves you time and trouble if something goes wrong but also ensures that you are getting the best online experience.

Optimisation Check

To ensure you get the best out of NetBank, the Commonwealth Bank offers a simple check to see which web browser, operating system and browser settings you have. If your computer isn't optimised for NetBank, we'll provide some recommendations on how you can improve your NetBank experience.

NetBank optimisation check

To ensure you get the best out of NetBank, we've run a simple check to see which web browser, operating system and browser settings you have.

If your computer isn't optimised for NetBank, we'll give you some recommendations on how you can improve your NetBank experience.

What we tested	What we found	Optimised?	Details
Web browser	Internet Explorer 6		Your browser is compatible with NetBank, but a more recent version is available. If you're experiencing difficulties viewing NetBank, please refer to our technical FAQs or upgrade your browser .
Operating system	Windows XP		Your operating system is compatible with NetBank. Please ensure that you install all available updates.
JavaScript	Enabled		JavaScript is enabled.
Cookies	Enabled		Cookies are enabled.
Screen resolution	1024 x 768		Your screen resolution is optimised for using NetBank.

You can also find out more about [using the internet safely](#) and even take advantage of our [discounted anti virus software offer](#).

You can access the Optimisation Check directly from the NetBank login page.

Internet security package

Every computer used to access NetBank needs an internet security package installed which will protect you from viruses and keep your online identity safe. The package from a reputable retailer should include:

- ▶ Anti-virus – stops viruses from damaging your computer
- ▶ Anti-spyware – protects your computer from viruses that try to monitor what you're doing online
- ▶ Firewall – monitors information going in and out of your computer to stop unauthorised access

It's important to make sure the internet security package is set to automatically download the daily antivirus updates so you're protected against the latest threats. For your convenience, a list of popular internet security packages can be found in the '**Further Information**' section on page 22.

Update your operating system

The operating system is the program that controls the normal functions of your computer. Ensuring your operating system stays up-to-date is an important step in keeping your computer secure. Both Microsoft and Apple regularly release updates, or patches, that provide new features, improve performance and protect against new types of viruses.

- ▶ Microsoft Windows – use Windows Update (<http://windowsupdate.microsoft.com/>)
- ▶ Apple Mac OS X – use Software Update within Finder

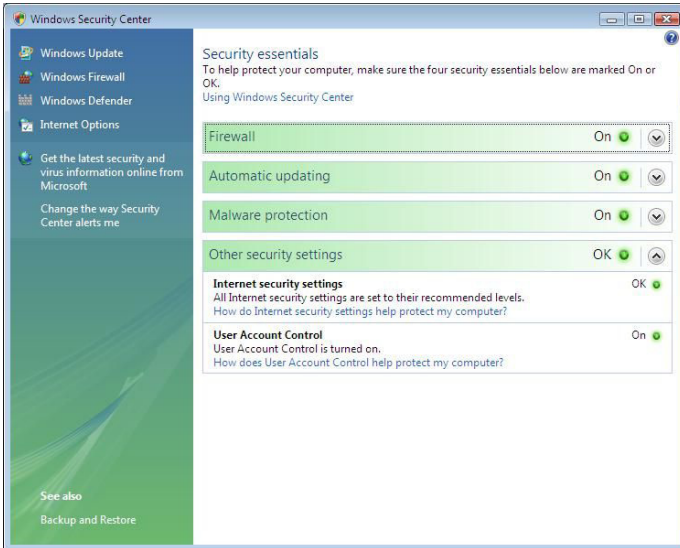
Updates are normally released every month but there may be urgent security patches during the month. You can set your computer to automatically download and install updates.

Using Microsoft Windows Security Centre

For users of the Microsoft Windows operating system, the Security Center can help you take control of security on your computer by showing you all the security related settings on one convenient screen.

It will alert you when security software is out of date or when security settings need to be strengthened, ensuring your computer is set up for you to use NetBank and the internet

safely. The example below shows an antivirus program is not installed and provides a **'Find a program'** link to fix this security problem.



You can access the Windows Security Center by clicking on **Start > Control Panel > Security Center.**

2. Register for NetCode

NetCode SMS offers you another layer of protection against fraud and identity theft. It's a highly effective and convenient system requiring passwords you only use once to authorise certain NetBank activities and transactions. The single-use password is sent to your mobile phone via an SMS message and only remains valid for 30 seconds.

Gaining access to most secure sites relies on 'something you know' such as a password or security questions. By adding a second layer of security requiring 'something you have' such as a mobile phone, you're protected from online threats like viruses and identity theft. With the NetCode SMS single-use password sent straight to your mobile phone, criminals can't authorise any fraudulent transactions.

3. Create an additional login

By creating an additional login you can tailor your level of NetBank access for those times you are using a computer that is not your own.

Before you access NetBank from public or shared computers you can create an additional login with '**view only**' access – this means you can view balances and your transaction history but you can't perform new transactions. This gives you peace of mind if you have to use unsecured computers at places like internet cafes or public libraries.

Visit NetBank to view our demo to see how quick and easy it is to create an additional login.

4. Receive security notifications by email

Security notifications are sent out as a secure bank message in NetBank.

You can also elect to receive these messages as an email.

If you didn't perform the activity, immediately call the NetBank Help Desk on **13 2221 and select option 4** (24 hours a day, 7 days a week).

Make sure you receive these important messages and keep your email address up-to-date. If you need to update your email address, login to NetBank, then click on the **'My contact details'** option under the **'Profile and preferences'** tab.

5. Review your NetBank login and activity log

NetBank keeps a record of your access and activity on your account for your peace of mind. The first screen you'll see after a successful login shows the date and time of your last login.

Also, you can view the full history of your activity by going to the **'Security'** tab, then selecting **'Online history'**.

If you notice any unusual activity, immediately let the NetBank Help Desk know on **13 2221 and select option 4** (24 hours a day, 7 days a week).

What should you do now?

NetBank security checklist

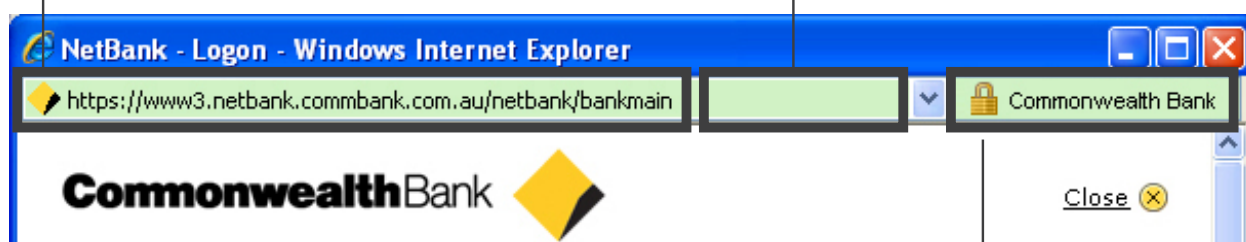
- ✔ Run an internet security package (anti-virus, anti-spyware, firewall). See page 13 for more information.
- ✔ Enable automatic updates for your operating system. See page 14 for more information.
- ✔ Register for NetCode – FREE security enhancement. See page 16 for more information.
- ✔ Login to NetBank directly from commbank.com.au Do not access NetBank via links from other sites.
- ✔ Confirm the authenticity of Bank emails via the '**Bank Messages**' inbox in NetBank.
- ✔ Regularly change your NetBank password and personal identification questions.
- ✔ Keep your contact details up-to-date.
- ✔ Report any suspicious activity on your account immediately to the NetBank Help Desk on **13 2221 and select option 4** (24 hours a day, 7 days a week).
- ✔ Always logout of NetBank using the **LOG OFF** button located at the top right of the screen.
- ✔ Run our optimisation check to ensure you are getting the best NetBank experience.

Understanding the security features of your browser

Internet Explorer 7 (Microsoft Windows)

The 'https' in the web address tells you that you are using SSL (SSL is short for Secure Sockets Layer and was developed to transmit private data via the internet) encryption. The 'commbank.com.au' before the forward slash tells you that you are using a Commonwealth Bank website.

The green shade means that the certificate uses extended validation. This means that the communication between your browser and the website is encrypted and that the certification authority has confirmed that the website is owned or operated by a business that is legally organised under the jurisdiction shown in the certificate and on this status bar.



The yellow lock indicates that you are using an encrypted connection. The name of the organisation that owns the SSL certificate (in this case, the Commonwealth Bank of Australia) is also displayed. If you click on the lock and select 'View Certificate' you will see information about the certifying authority and the contents of the certificate.

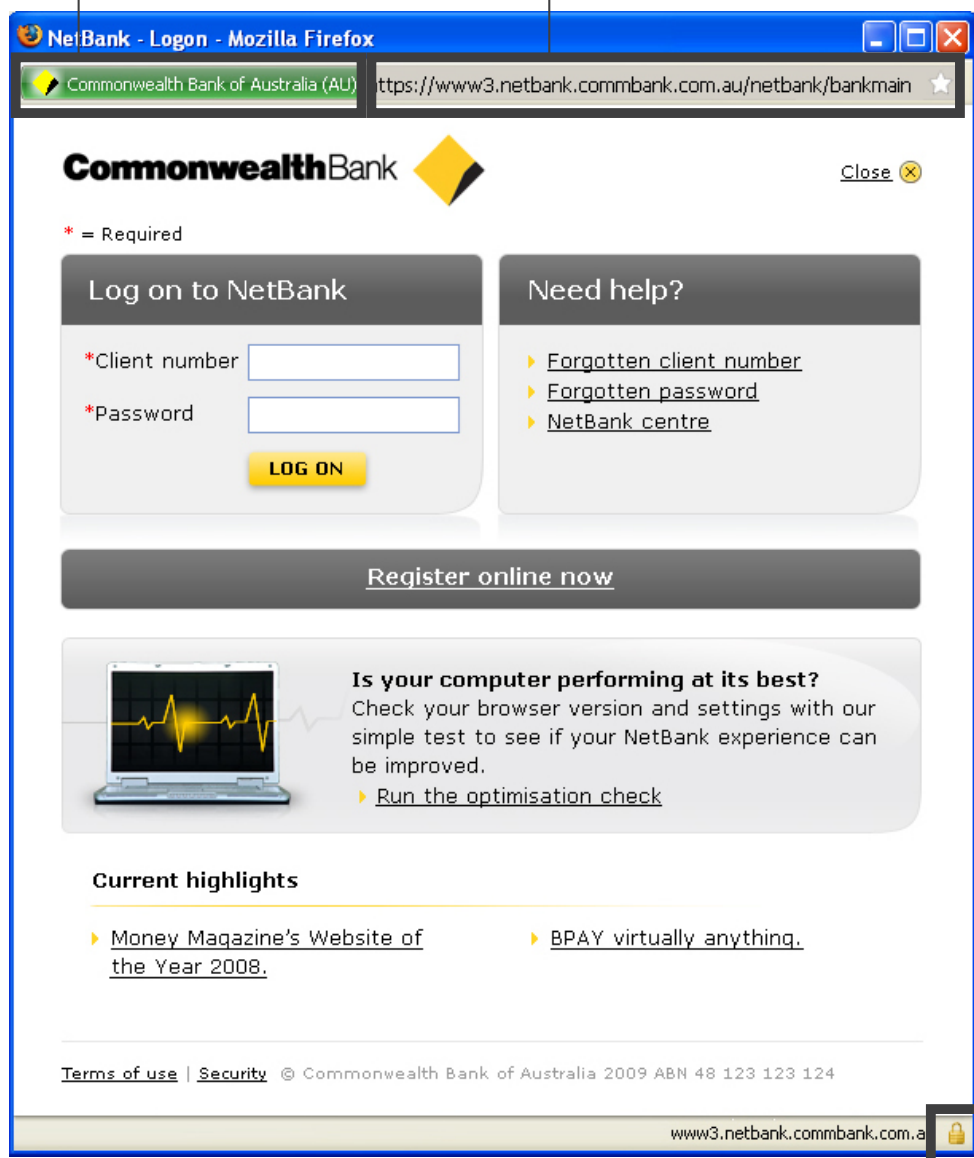
If you are using IE7 on Windows XP, the phishing filter (a filter for hoax emails) and/or certificate revocation is needed to enable the address bar to turn green when on a site that uses extended validation certificates (this means you can be sure a site is genuine):

- ▶ To turn on the phishing filter (this would be turned on by default) click on **Tools > Phishing Filter > Turn On Automatic Website Checking**
- ▶ To turn on certificate revocation (this would be turned off by default), click on **Tools > Internet Options > Advanced**. Scroll down to '**Security**' and tick Check for Server Certificate Revocation. Note that this requires a restart of the browser to take effect.

Firefox 3 (Microsoft Windows, Apple Mac OS X)

The green Site Identity Button tells you that the site has fully verified identity information about the owner (in this case the Commonwealth Bank of Australia) and that the connection is encrypted.

The 'https' in the web address tells you that you are using SSL (SSL is short for Secure Sockets Layer and was developed to transmit private data via the internet) encryption. The 'commbank.com.au' before the forward slash tells you that you are using a Commonwealth Bank website.



The yellow lock means that there is an encrypted connection.

Safari 3.2 (Microsoft Windows, Apple Mac OS X)

The lock symbol and the green identity indicator tells you that the website's ownership has been verified with a certificate and that any information entered will be encrypted.

NetBank - Logon

Commonwealth Bank of Australia

CommonwealthBank

Close

* = Required

Log on to NetBank

*Client number

*Password

LOG ON

Need help?

- ▶ [Forgotten client number](#)
- ▶ [Forgotten password](#)
- ▶ [NetBank centre](#)

[Register online now](#)

Is your computer performing at its best?
Check your browser version and settings with our simple test to see if your NetBank experience can be improved.

- ▶ [Run the optimisation check](#)

Current highlights

- ▶ [Money Magazine's Website of the Year 2008.](#)
- ▶ [BPAY virtually anything.](#)

[Terms of use](#) | [Security](#) © Commonwealth Bank of Australia 2009 ABN 48 123 123 124

Further information

NetBank

Register for NetBank:

<http://www.commbank.com.au/personal/netbank/default.aspx>

NetCode SMS demo:

http://www.commbank.com.au/personal/netbank/learn-about-netbank/demos/security/netcodesms_step1.aspx

Security Centre:

<http://www.commbank.com.au/security-privacy/>

Internet security packages:

Popular internet security packages for Windows include:

- ▶ CA: <http://www.ca-store.com.au>
- ▶ Checkpoint: http://www.checkpoint.com/products/za_iss/index.html
- ▶ F-Secure: <http://www.f-secure.com/estore/aus/>
- ▶ McAfee (Internet Security): <http://au.mcafee.com/>
- ▶ Symantec: <http://shop.symantecstore.com/store/symnahho/DisplayHomePage>
- ▶ Trend Micro: <http://www.trendmicro.com.au/au/products/personal/index.html>

The commercial market for internet security packages for Macintosh systems is less mature, however some packages are available:

- ▶ ClamXav: <http://www.clamxav.com>
- ▶ McAfee (Virex): http://www.mcafee.com/au/small/products/virusscan_for_mac/virusscan_for_mac.html
- ▶ SecureMac: <http://securemac.macscan.com>
- ▶ Virus Barrier: <http://www.intego.com/virusbarrier/>

These sites are listed for your general information only. The Commonwealth Bank does not endorse any of the services, products or solutions provided by these companies and does not accept any liability for any loss or damage you may suffer arising out of or associated with your choice of any service, product or solution provided by these companies. You should seek independent expert advice if you have any concerns regarding what services, products or solutions may be suitable for you.

Configure your package so that it automatically scans (at a minimum):

- ▶ Incoming and outgoing email and attachments
- ▶ Files as they are opened
- ▶ Your entire disk, at least monthly
- ▶ Preferably other services, if possible, such as web traffic and instant messaging

Most high quality commercial software packages, like those listed above, provide easy-to-use, intuitive “consoles” for the home user. They are generally preconfigured to provide an optimum level of security, and options are easily selected using ‘tick boxes’ or ‘radio buttons’.

Maintain your internet security package by:

- ▶ Updating the software every year or two
- ▶ Updating the signatures* often (e.g. every few days) — this should happen automatically with most packages

* Most anti-virus or internet security software packages are updated on an hourly or daily basis by the vendor. This ensures that the software package is able to identify the latest threats. This update process usually occurs automatically but it is configurable by the user. Note that this is not the same as updating the version of your software (e.g. changing from a 2006 version to a 2008 version).

Further online security information

Protect Your Financial Identity

A joint initiative between the Australian Bankers Association, Australian High Tech Crime Centre and Australian Securities & Investments Commission

<http://www.protectfinancialid.org.au/>

Stay Smart Online

An Australian Government initiative

www.staysmartonline.gov.au

NetAlert

An Australian Government initiative

www.netalert.gov.au

Scam Watch

An Australian Competition & Consumer Commission initiative

www.scamwatch.gov.au