Investec

Information Security

Protecting you home PC and your documents

General Advice for home computers

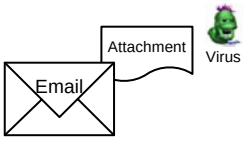
Home computers are increasingly being used to store store addresses, track finances, perform on-line Banking, store digital photos and music and even complete complete tax returns! All of this information should be given the same level of protection as you would valuable physicals documents. And computers have the added problem of being connected to te Internet and open to attack from cyber-criminals.

There are many methods criminals use, some to steal your identity distrupt your computer or remotely control of it so it can be used to attack others. Fortunately there are some simple tools and techniques to protect yourself…

Protection from email virus

Most viruses are transmitted via attachments to emails, so always be very cautious when your receive any emails, especially from unknown people.

Attachment may appear to be word documents, spreadsheet, pictures, etc but often contain malicious viruses.



If the sender of an email is known to you, but the email is unexpected - ask the sender if they meant to send it before you open any attachments (their computer might be infected with a virus that has automatically sent itself to you and they don't know!).

If an email "appears" to come from your Internet provider, Microsoft or even your Bank, be very very cautious. It's easy to "spoof" an email to make it look like it comes from somebody else when in fact they come from Hackers.

Microsoft never send updates via email and Banks never ask for personal information via email.

There are many Anti-Virus products around; some are available for home users free of charge.

www.mcafee.com	US$39
www.symantec.com	US$49
http://www.free-av.com	**Free!**
http://www.grisoft.com	Free!
http://www.bitdefender.com	Free!

The biggest issue with any Anti-Virus product is keeping it up to date as new viruses are released. **At the moment the hacking community releases one new virus every** day as viruses are often written to impress other hackers and gain cudos within the hacking community.

Most commercial products (McAfee, Symantec, etc) provide a mechanism to automatically update themselves. The free products need to be manually updated.

Viruses (or Virii) can also be transmitted via MSN-Messenger, Yahoo-Chat, Kazaa, etc. Do not trust **any** files sent to you!

Spam

The internet is plagued by spam.Nearly 80% of email is unsolicited or “Spam”. Most is send completely randomly.

Never use your main email account to sign up for anything on the internet.

Never ever buy anything from, click on any link in, or reply to any spam. **Not even the “unsubscribe link”**. This proves your email is genuine and you’ll recevie more Spam.

Don't give permission for companies or Web sites to share your e-mail address with partners or affiliates.

Use a good anti spam program and filter system on your computer.
http://www.mailwasher.net/ costs $37 but has a free trial or try http://www.spambully.com/

Passwords

A technique often used is to guess password or try to get you to disclose it by pretending to be from your Bank or IT Helpdesk.

Change your passwords (and please do not use your pet's name, your partner/children's name, your hobby, etc - they are too easy to guess).

Never reveal your password if somebody telephones you. Always verify who they are before disclosing personal information.

Install a Firewall

Another way Hackers infect home computers is by connecting to them while you are surfing the Internet ("pop ups" advertising products are often an indication that they can do even worse things!).

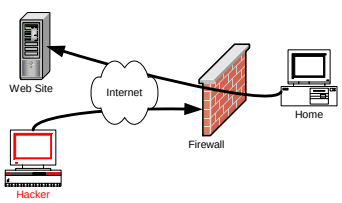
The best way to protect your computers from unauthorised connections from the Internet is to install a personal firewall.

There are several on the market, again some free, some commercial. And commercial does not always mean better!

www.mcafee.com	US$39
www.symantec.com	US$49
www.blackice.iss.net	US$39
www.zonelabs.com	**Free**
www.sygate.com	Free

The firewall sits between your computer and the Internet and acts as a security guard, restricting what can come in and go out.

To start with the firewall may ask you what you want to allow in or out, but soon it learns enough to make the decisions on it's own.



The main point is never allow any body from the Internet to connect to your computer!

Update and clean up your machine

Keep your computer updated (Microsoft Windows has hundreds of Bugs, which Microsoft issue fixes or patches for). Go to to http://windowsupdate.microsoft.com

Once you have installed an anti-virus and a firewall, you can then use some products to clean your computer and remove any spy programs that have already been installed

A lot of web sites use small programs to track your activity, and use the information to target you with adverts. Ad-aware (from http://www.lavasoft.de/) or SpyBot (from http://www.safer-networking.org/) removes the tracking programs and cookies, giving you your privacy back.

If your computer has been infected in the past, hackers often install backdoors (or Trojans) to allow them to take over your machine again. The Cleaner (from www.moosoft.com) detects and removes all known Trojans. This is a commercial product (US$30), but they do allow you to download a trial (and hence clean your PC for free!).

Finally check on http://www.grc.com and follow the "shields up" links to see how your machine looks from the Internet. This site scans your computer (don't try this at work - it doesn't work through our firewalls!) to show you how the hackers see you! Very scary if you don't have a firewall installed.

In summary

- Install an anti-virus programme
- Install a firewall
- Clean up and remove all the spy-ware that any hackers have already installed
- Kept your PC up to date with security patches by visiting windowsupdate.microsoft.com or www.apple.com/support
- Never trust third parties who phone or email you. Verify who they are/