Article: COMPUTERS BEHAVING BADLY
Topic: Viruses
Author: Mark Ahearn

If you have a computer and use the Internet, you MUST have virus protection. This is the cold reality of the era we live in. 2003 saw the greatest growth, both in terms of volume and success rates, in virus activity.

Viruses, Trojans and Worms are all programs that share a common goal – to invade your computer, without your knowledge and to spread chaos. Once resident on your machine, they can delete files, render the machine unbootable, spread themselves to other contacts in your address book via email, or reconfigure access channels into your computer for entry by other intrusive software, just to name the common effects.

Anti-virus (AV) software is your easiest line of defence and, combined with other forms of protection, can form part of a safety-net that goes a long way to helping ensure that your computer is as secure as you can humanly make it.

Mandatory requirements for any AV software is that it does automatic updates from the Internet whenever you are connected, automatically scans all incoming emails and is started whenever the computer boots up. Some packages don't have all these features, or they are required to be turned on by the user.

The most common method for infection is through emails. You can minimise your exposure by following these steps. They may seem mundane but are surprisingly effective.

- Nearly all Internet Service Providers (ISP's) have a facility to check your mail from their computers. This way your emails are never downloaded unto your computer. Look on your ISP's home page for links to Email or WebMail or Members Area.
- Don't be a 'sheep' and follow instructions blindly from emails pretending to be Security Updates or Latest Virus Patch. Virus writers will do anything to get your attention to make you open their email. Another common method is to state that the email you sent someone has been returned in error when in fact you never sent any in the first place.
- "Curiosity killed the Cat". Never open emails not directly for you or from someone you know or are expecting.
- Treat any attachment as a potential threat.

It is very easy to jump straight on the computer, connect to the Internet and download your emails – all before your AV software has had a chance to check for updates. Manually update the AV if you can't wait for the automated process to catch up.

Assume the worst!. Always think of 'When I get infected…' and not 'If I get infected…' This will force you to be more cautious of emails, do more backups and run more programs to check for malicious program activity.

There are quite a few free versions of AV software downloadable off the Internet. These typically offer basic protection from viruses. The shop brought versions offer

fancier, automated features. It comes down to a question of budget. Any protection is better then nothing.

Mark Ahearn
c.b.b@optusnet.com.au