

# Aardvark's Email Virus Avoidance Checklist

3 October 2002 distribute freely.

- 1. Make sure your OS, browser and email software are current and up-to-date.**  
If you don't have IT staff to take care of this for you, make sure you check at least once a week that there aren't new updates or security fixes for your software.
- 2. Make sure you have anti-virus software installed, operating and up-to-date.**  
If you don't have IT staff to take care of this for you, make sure you check for new updates **every single day**.
- 3. Make sure you have a personal firewall or that your network has its own firewall.**  
There are many good products available for free – try ZoneAlarm.com for an example.
- 4. NEVER, NEVER open unsolicited email attachments even if you know the sender.**  
If you're in any doubt, email the sender and get confirmation that it was actually them who sent the file and ask them to confirm the filename and its contents.
- 5. Set your Windows or mail program options to show the full name of email attachments.**  
This reduces the risk of an executable file masquerading as text or a document.
- 6. Don't use email to share joke files with friends or workmates.**  
This practice makes it very easy to mistake a virus for just another funny program or animation.
- 7. Do not use attachments when plain emails will do.**  
Don't use MS Word or other attachments in your email if the same information can be easily conveyed by including the details in the body of your message as plain text.
- 8. Check to see what/if new viruses have been reported by the media.**  
Of course [Aardvark.co.nz](http://Aardvark.co.nz) is a great place to find this information. Forewarned is forearmed.