

# Helpsheet:

## Perils of email

---

Email is a wonderful communication tool used widely throughout the University; however there are some 'nasties' that can be described as the 'perils of email'.

### Viruses

More and more viruses now enter the University through email. Here are some tips for the detection and prevention of viruses:

- Due to the high incidence of viruses distributed through zip files you should take extra care when receiving these files.
- Do not open any files attached to an email if the subject line is questionable or the message is from an unexpected source.
- Do not download any files from strangers.
- Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one.
- When in doubt, always err on the side of caution and do not open, download, or execute any files or email attachments.
- Eudora users can activate a 'Preview Pane' window which splits the viewing screen into 2 sections. The top section lists your incoming mail and by clicking once and highlighting an entry from this list the body of the mail message will be displayed on the screen below. This enables you to preview the contents of a message before actually opening it – a very good tool for protecting yourself from email viruses etc. To activate the preview pane in Eudora, go to the **Tools** menu and select **Options**. Scroll down the **Category** list and select **Viewing Mail**. Place a **tick** in the **Show message preview pane** box.
- Keep your virus protection software up to date.

### Spam

Unsolicited (or junk) email, commonly known as spam has become more prevalent with the increasing use of email. The University has instigated a mechanism whereby suspected spam is checked before it comes into the University's email server. Email passes through various checks and stages. If email fails to pass, it, is not passed to the Deakin mail server and will never be received by the recipient.

Filtering is available in most email packages but staff should be aware that Eudora and Deakin Webmail are the only mail packages supported by ITSD. Staff using other packages will need to consult their IT support staff or email software documentation for assistance in setting up a filter.

All email users should periodically check their SPAM and/or Junk folders to ensure that no legitimate messages have been moved there by mistake. It is also good practice to review and delete the contents of these folders and empty your Trash regularly, so that suspect attachments are removed from your computer.

You can find more information on spam and how you are protected from it, at [www.deakin.edu.au/its/common/spam.php](http://www.deakin.edu.au/its/common/spam.php)

## ***Phishing***

Phishing is a high-tech scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, passwords or other sensitive information. The message usually says that you need to 'validate' or 'update' your details and directs you to a website that looks just like that of a legitimate organisation. The aim of this is to trick you into entering your information so the originators can steal your identity and run up bills in your name, or worse.

To help avoid these pitfalls:

- Be very wary of emails asking for your personal details, such as those supposedly from banks requesting your account details.
- Always enter a URL directly into your web browser rather than clicking on a link in a message.
- Never email personal or financial information.

You can find more information on phishing and steps to protect yourself at:

<[www.deakin.edu.au/its/it-security/known-issues/fraud-emails.php](http://www.deakin.edu.au/its/it-security/known-issues/fraud-emails.php)>

## ***Chain emails***

The modern equivalent of chain letters, chain email is designed primarily to clog up email servers and networks.

Make sure you:

- Delete chain emails and junk email. Do not forward or reply to them.
- Ignore emails that urge you to urgently 'warn your friends' about a virus.

## ***Rules on sending emails***

You should always follow these rules when sending emails:

- Make sure confidential emails are sent to the right people. Verify the recipients before sending.
- If you select a group, make sure everyone in the group should be receiving the email.
- When sending confidential email, be sure to confirm receipt of the material.
- Encrypt highly sensitive information before sending it.