

**IT Information Sheet 1****About Spam (Unsolicited) Email****What is Spam**

Spam is a term used to describe unwanted, unsolicited email sent to your Mail Box. In a nutshell, it's effectively the electronic version of junk mail you receive in your home mailbox.

Spam emails may contain anything from things for sale, pornography, information about 'get rich quick' schemes, chain letters, and hoax virus alerts. Spam mails may also contact attachments with viruses, which can damage your computer files.

Spam, like viruses, is an inherent risk of using the internet and email. While Spam is basically impossible to stop, there is ways to limit your exposure to spam mail.

Why is unsolicited email called Spam

The term Spam has no particular meaning, nor is it an acronym for some complicated computer term. The general consensus is that the term Spam originated from the Monty Python skit about Spam (The ham in a tin variety) in the early 70's. As most computer geeks seem to be big Monty Python fans, it was only a matter of time before a computer related topic got a Monty Python name assigned to it. Under this definition, Spam does not related to the ham in a tin variety of Spam.

How Spam works

Spammers use a range of clever ways to deliver Spam email. The most common method is to use a free email address from a large email provider, like Hotmail or Yahoo. The Spammers use an address for a week or so sending out as much email as they can, before being stopped by the free email service. Once they are stopped, they will move on to a new email address, and continue sending emails from the new address.

Another method used by Spammers is to find a poorly managed email server and hack the mail server to send out spam using that mail server's email addresses.

How does a spammer get my email address?

Again, there is a range of clever ways that spammers can use to obtain your email address. The most common method is to harvest email addresses from the internet by searching things like -

- posts to online forums.
- mailing lists.
- web pages.
- ICQ and chat rooms.
- gaining access to unsecured mail servers and computer networks.
- using Spam generators to target particular email addresses or email domains

The most common form of Spamming directed at CSU and other Universities is where Spammers attempt to guess email addresses.

Spammers will generate a list of common names and send spam mail to these names at the CSU email server (@csu.edu.au). The guessing is done on the basis that most email addresses are usually based on the firstinitialsurname@csu.edu.au (eg. jbloggs@csu.edu.au)

The Spammer will then wait for either an error message to return by email, indicating that the email address is incorrect, or for a confirmation. A confirmation could be generated by inserting non-standard but commonly used mail headers requesting that the delivery system send a confirmation of delivery or reading.

Why doesn't CSU stop spam mail getting into my account?

Unlike viruses which can be detected by common attributes, such as particular attachments, Spam is purely subjective in content. CSU does not censor email coming into the University. It would be impossible to check every piece of email to determine whether it is Spam or not.

CSU does not apply Keyword filters either, as it is not possible to block certain common spam words without also blocking legitimate email messages. For example, to block the word Sex may stop some pornography spam email, but would also stop emails regarding topics such as Sexual Harassment or Sex Discrimination. CSU does have in place a facility to attempt to filter and reduce the amount of spam you receive. Whilst this facility works on most spam, spammers alter the way they send email over time to specifically avoid such filters. We modify our facility, but we (and no one else in the world can) cannot guarantee to remove all Spam.

How to minimise your exposure to Spam Mail

The best defense against Spam is to be pro-active, and ensure that you use common sense when using email and the internet. Listed below are some simple steps to take in limiting your exposure to spam.

- Just delete any spam or unsolicited email message as soon as you get it.
- Don't ever reply to spam, under any circumstances. By replying to spam, you are only letting the spammer know of your existence, which is exactly what they want you to do.
- Don't click on links to unsubscribe your address from an email list. This is usually just another trick used by Spammers to confirm your existence.
- Don't answer online requests for information from unknown or untrusted sites (in other words, think carefully before filling in forms contained on web pages or email messages).
- Be careful when using ICQ or similar chat programs online.
- Never respond to popups by clicking on links.
- Install and keep your computer antivirus software up to date at all times, and regularly scan your computer.
- Be careful of giving out your email address to people or organisations you are not familiar with.
- Try to avoid having your email address listed on web sites.

Be careful when downloading Adware, Freeware and Shareware. The process of downloading such software often requires you to provide your email address which may be used to send you advertisements, viruses, more spam or even download secret files into your computer which can compromise your PC's security.

Using the Rules feature in Outlook to develop a Spam Rule

Students and staff using Outlook can set up their own anti-spam filters by using the Rules Feature in Outlook. This feature allows you to set up specific filters to detect and delete various known forms of spam from entering your inbox. For instructions on how to set up and use the Rules features, go to the DIT web site at http://www.csu.edu.au/division/dit/f_staff.html and click on the Spam Rule link.

Virus Hoax Mail

Virus Hoaxes are emails that claim to warn users about a dangerous new virus doing the rounds on the internet. More often than not, these emails are forwarded by unsuspecting people, thinking they are doing the right thing. In reality, it's just more unnecessary spam mail. Another problem with some Virus Hoaxes is that they contain instructions on how to protect yourself against a bogus virus. In some cases, following these instructions will only damaged your computer, not protect it. If you receive a virus warning, it is suggested that:

- you do not forward the email onto other people, particular if the email suggests doing so.
- you do not follow the instructions contained in the email or forward the email to others;
- you ignore such virus warnings unless they are clearly from an authoritative source, and back up their claims with references to credible sources.

The CSU Division of Information Technology does not email virus warning to Students and Staff. All formal DIT issued notices regarding viruses are posted as What's New notices in the my.csu portal, and via the IT Issues Forum.

This IT Information Sheet was produced by Client Services – CSU Division of Information Technology. For further information, please contact the IT Service Desk on 1300 653 088 or internal CSU call on 84357