emily carr
university of art + design

1399 Johnston Street, Vancouver, BC, Canada V6H 3R9

FIGHTING SPAM/JUNK MAIL

This information sheet provides some basic information on the topic of Spam/junk mail and how to help manage the problem on your computer.

What is Spam ?

> *From http://spam.abuse.net/overview/whatisspam.shtml:*
>
> "Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender.
> …
> Email spam targets individual users with direct mail messages. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses."

How Can I Reduce the Amount of Spam that I Receive?

From one recent report, it is estimated that in 2004 approximately *two thirds of all e-mail traffic* on the Internet is Spam (http://www.msnbc.msn.com/id/5032714/). Unfortunately, one of the only things you can do to limit spam from getting to you is to limit the public accessibility of your e-mail address to spammers on the Internet. Spammers often use automated "harvesting" tools to scan websites, discussion forums and newsgroups looking for valid e-mail addresses. There are several techniques you can use:

- Try not to display your e-mail address in newsgroup postings, chat rooms, websites or in an online service's membership directory. You may also want to opt out of member directories for your online services. If you must list your e-mail, one common technique (though not foolproof) is to obscure or "munge" your e-mail address by adding some noticeable text to the address. For example, if my e-mail was "janedoe@here.ca", I may list it publically as "janedoe@nospam.here.ca". People who want to contact you must remove the "nospam" text from your address before sending their e-mail.

- Check the privacy policy when you submit your address to a website. See if it allows the company/organization to sell your address. You may want to opt out of this provision, if possible, or not submit your address at all to websites that won't protect it.

- Read and understand the website submission forms before you transmit personal information through a website. Some websites allow you to opt out of receiving e-mail from their "partners" - but you may have to uncheck a preselected box if you want to opt out.

- Decide if you want to use two e-mail addresses - one for personal messages and one for newsgroups and chat rooms. You also might consider using a disposable e-mail address service that creates a separate e-mail address that forwards to your permanent account. If one of the disposable addresses begins to receive spam, you can shut it off without affecting your permanent address.

How Should I Deal With the Spam that I Receive ?

Because of the overwhelming amount of Spam on the Internet today, increased efforts have been made by Internet Service Providers (ISPs), network administrators and software manufacturers to deal with the problem. There are no 100% foolproof methods for properly detecting and filtering out all spam from getting to a recipient, but there are ways to greatly reduce the amount which you receive.

Most ISPs and network administrators have now installed spam detection software on their mail servers which attempt to identify and reject spam based on certain characteristics of an e-mail (e.g. if the subject contains the word “great deal”). This software helps to prevent a large number of spam e-mail from reaching your e-mail inbox, but is not foolproof. Emily Carr University currently uses spam filtering software which helps to reject many unwanted e-mails from getting to students, staff and faculty, but it can not eliminate all of it.

There are many free and commercial “anti-spam” software packages available for dealing with spam in your inbox. These programs work similarly to the software used by ISPs and network administrators. These programs do not prevent the mail from reaching you, but try to isolate it from your inbox by sending it to a special “junk mail” folder for automatic deletion or manual processing. To find one that suits your needs, try doing a bit of research on the Internet (eg. search for “spam software reviews”).

What to do with the software which does eventually reach your inbox ? The Microsoft spam information site offers some good tips for dealing with unsolicited e-mail:
http://www.microsoft.com/athome/security/spam/options.mspx

- Don't reply to e-mail asking for personal information.

- Watch out for spoofed mail. "Spoofing" refers to duplicating a legitimate e-mail, such as a company's newsletter. These spoofed mails may be used to trick you into downloading a virus or sending personal information, such as a credit card number. When in doubt, contact the company you think sent the e-

mail.

- Don't buy anything from a spam mail.
- Never, ever contribute to a charity from spam mail.
- Think twice before opening attachments, even if you know the sender. If you cannot confirm with the sender that a message is valid and that an attachment is safe, delete the message immediately, and run up-to-date antivirus software to check your computer for viruses.
- Don't forward chain e-mail messages. Chain mails may be hoaxes, or even a virus delivery system. Plus you lose control over who sees your e-mail address. Additionally, there are reports that spammers use chain letters to gather e-mail addresses.

Resources

- Spam information from "One of the best anti-spam sites on the net": http://spam.abuse.net
- Privacy Commissioner of Canada: "*Protecting Your Privacy on the Internet*" http://www.privcom.gc.ca/fs-fi/02_05_d_13_e.asp
- Microsoft: "*What you can do about Spam*" http://www.microsoft.com/athome/security/spam/
- British Columbia Freedom of Information and Protection of Privacy Act http://www.oipcbc.org/

Disclaimer

Emily Carr University assumes no liability for personal or workplace computing equipment used during your course of study. We are not liable for damages caused by or thought to have been caused by the installation of software purchased from us, provided by us or obtained through links posted on our website. We are not accountable for issues you may have surrounding the installation and/or use of said software.