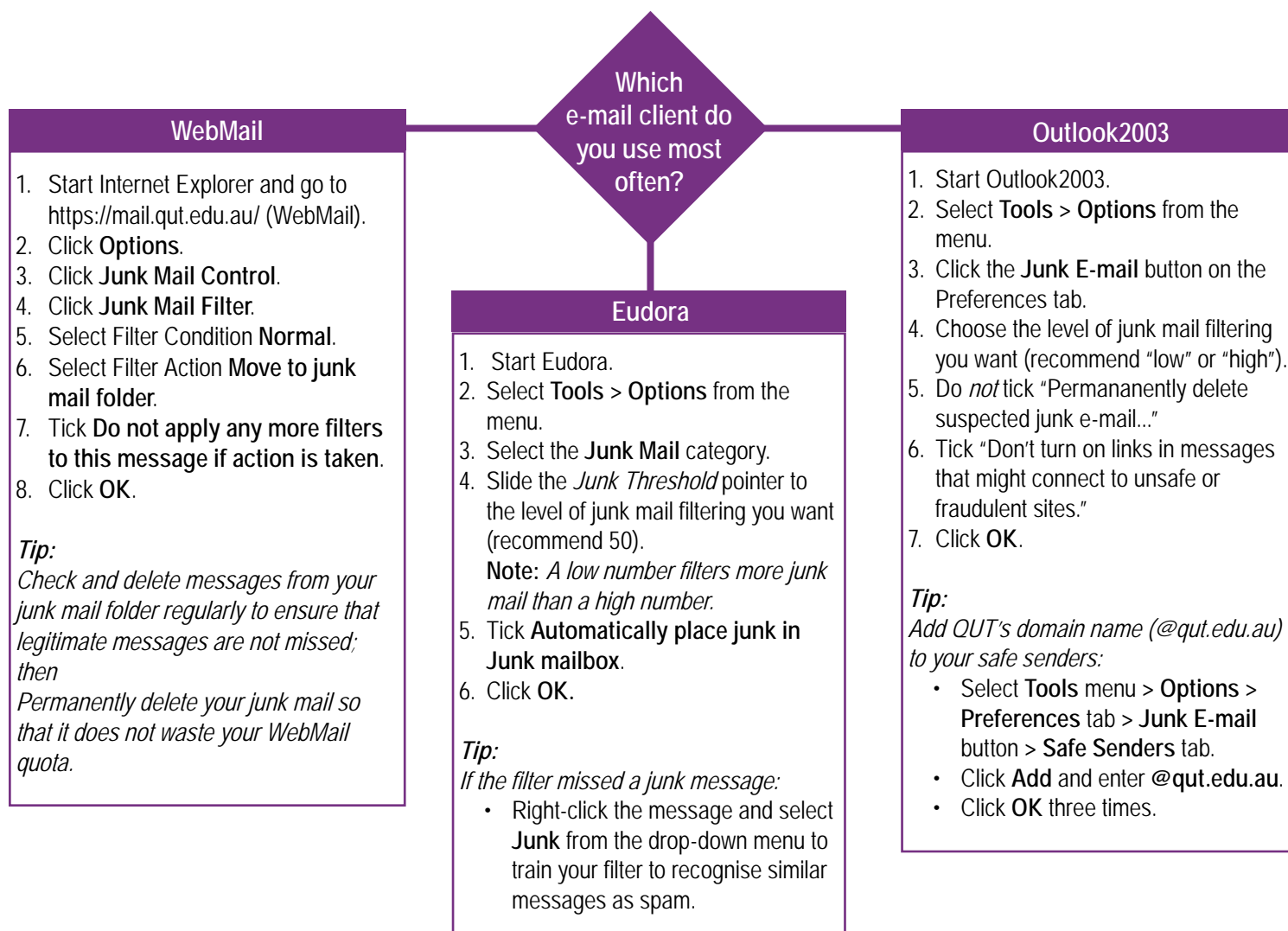


Glossary

SPAM	Unsolicited, unwanted, irrelevant or inappropriate e-mail messages, especially commercial advertising sent indiscriminately in mass quantities.
UCE	"Unsolicited Commercial Email" is another term for spam.
White List/Safe Senders	A user managed list of e-mail addresses which are exempt from junk mail filtering.
Black List/Blocked Senders	A user managed list of e-mail addresses from which you do not wish to receive e-mail (i.e. all messages from that e-mail address are treated as spam).
Junk Mail Filter	A filter/rule automatically sorts and performs actions on email messages as they arrive or when being sent.

QUT uses various technologies to minimise and manage spam coming into university staff and student e-mail accounts. To further reduce spam, it is highly recommended that you activate a junk mail filter in the e-mail client you use most often.



Check the junk mail folder regularly to recover any messages you wish to keep and delete junk mail permanently.
Add any legitimate e-mail addresses to your white list/safe senders.

Simple Steps to Combat Spam

To help combat spam, follow these recommendations:

- ① Never make a purchase from an unsolicited email.
- ① If spamming were not economically viable, it would be obsolete. Not only can an email user fall prey to a potentially fraudulent sales scheme, but his or her email address can also be added to the numerous email lists that are sold within the spamming community, further compounding the number of junk emails received.
 - Never provide your email address on websites, newsgroup lists or other online public forums.
 - Never give your primary email address to anyone or any site you do not trust
 - Share your email address only with your close friends and business colleagues.
- ① If you do not know the sender of an unsolicited email message, delete it.
- ① While most spam is usually just annoying text, a spam email message could actually contain a virus and/or other exploit that could damage the computers of all who open it.
- ① Never respond to any spam messages or click on any links in the message.
- ① Replying to any spam message, even to “unsubscribe” or be “removed” from the email list only confirms to the spammer that you are a valid recipient and a perfect target for future spamming.
- ① Avoid using the preview functionality of your email client software. Many spammers use advertising techniques that can track when a message is viewed, even if you do not click on the message or reply. Using the preview functionality essentially opens an email and tells spammers you are a valid recipient, which can result in even more spam.
- ① Sending email where all recipient addresses are “exposed” in the “To” field makes it vulnerable to harvesting by a spammer’s traps.
- ① If you need to fill out web registration forms, or surveys at sites from which you do not want to receive further information, consider using secondary addresses to protect primary email accounts from spam abuse. Also, always look for a box that solicits future information/offers, and be sure to select or deselect as appropriate.