Junk and malicious email
IT Services Documentation Team, September 2013 (Reviewed August 2014).

What is it?

Junk mail is mail that arrives in your mailbox unsolicited and unconnected to your normal sphere of correspondence, e.g. hoax virus warnings, financial scams (phishing), product advertising, chain mail, etc. Usually the same message is sent simultaneously to a large number of users (spamming).

Common types of malicious junk email include:

- hoax virus warnings
- financial scams (e.g. Nigerian scam and variants, Banks and on-line payment service scams, Lottery scams, Bogus orders)
- phone this number

Sometimes the content of junk mail makes you think you’ve been personally targeted in some way. Regardless of its content, even if your name is present in the message, it is at least 99.9% certain that a junk mail message is not directed at you personally. Your address just happens to be on a list of addresses that the junk mail sender has obtained.

Why do I get junk mail?

While it is true that some spam email does get through to your Inbox, far more is intercepted and dealt with on your behalf.

We use SpamAssassin and MAPS/RBL to identify potential spam. When an email arrives on the University mail servers, SpamAssassin scans it and gives it a spam “score” based upon keywords, patterns and blacklists.

- If it scores 10 or higher, it is automatically rejected and is not delivered to your Inbox.
- If it scores below 10, it is allowed through.

This highly effective system routinely intercepts and blocks between 200,000 and 250,000 spam email messages per day.

However, detection is not an exact science and some junk mail will always slip through; after all, one person’s junk could be another person’s legitimate correspondence. In addition, the senders of junk mail are constantly devising new ways to outsmart the filters.

What’s the best way to deal with junk mail?

The best way to deal with junk mail is to delete it quickly. Don’t waste time reading it or trying to work out why you received it - just press the delete key!

- Don’t respond to an email from an unrecognized sender or source. If in doubt, and alternative contact details are provided in the message, phone instead - if the message is genuine, the sender won’t mind.
- If you receive an email message from someone other than the University Service Desk warning you about a potential virus, then the message is almost certainly a hoax. Delete it!
- Be suspicious of any email that requests confidential personal or financial information such as online passwords or credit card details. No reputable institution or organization, including the University of Aberdeen, will ever ask you for such details by email. Delete it!
- If it’s chain mail, don’t be tempted to pass the message on to other users. Either delete it or forward the message to the Service Desk - servicedesk@abdn.ac.uk, saying why you have chosen to forward it, e.g. it’s come from another University user, is particularly unpleasant, or you’ve received it many times before.
  - **Note:** The circulation of chain email is a breach of the University of Aberdeen’s Conditions for using IT Facilities\(^1\) and could result in the withdrawal of your access to computing facilities.
- Never give in to the temptation to take the law into your own hands and respond with aggressive tactics like mail-bombing (sending large amounts of junk to the mailbox you think the junk came from). Whatever the circumstances, this is an abuse of the network and will be treated as such.

Can I filter my own mail?

Yes. We add the phrase **SPAM** to the Subject field of spam that makes it past SpamAssassin, i.e. messages that have a spam score of less than 10. This alerts you to any mail that we think may be junk but allows you to decide what to do with it.

You can use an Outlook rule to help filter spam that gets through and move it directly to a Junk Email folder as soon as it arrives in your Inbox. This makes it easy for you to check for any valid mail that might have been put there by mistake.

See our Fact Sheet Outlook 2010: Creating SPAM filters.

---

\(^1\) IT Policies are published in the Policy Zone on StaffNet – see www.abdn.ac.uk/staffnet/governance/