Junk Mail – what it is and how to deal with it

Junk mail is mail that arrives in your mailbox unsolicited and unconnected to your normal sphere of correspondence, eg 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).

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 junk email does get through to your Inbox, far more is intercepted and dealt with on your behalf.

Our mail filters scan all incoming email as it arrives on the University mail servers and give it a **score** based upon keywords, patterns and blacklists. This includes any message that has an attachment with a file extension type recognised as having the potential to carry virus infections is rejected – see list of blocked file extensions. Email with a high score is automatically rejected and is not delivered to your Inbox. This highly effective system routinely intercepts and blocks many thousands of spam email messages per day.

Why is some legitimate email marked as Junk?

Unfortunately, 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.

To deal with this, we direct low scoring email directly to your **Junk Email** folder in Outlook and add **SPAM** to the Subject field. This makes it easy for you to check for any valid mail that might have been put there by mistake.

Do I need to do anything?

Yes. You should check your **Junk Email** folder every day to to check for legitimate messages that may have been incorrectly classified as spam.

Messages in the Junk Email folder are converted to plain text – links and other functionality are disabled. If you spot a message that you know *absolutely* is not spam and you want to act on it, drag it to your Inbox, or right-click on it and select **Move > Inbox** from the pop-up menu. **If in any doubt about any message's authenticity, delete it**.

Can I prevent legitimate emails being marked as Junk?

Yes. If you find a valid message in the Junk Email folder, you can nominate the sender (or its domain) as being safe to ensure that future messages get through to your Inbox.

1. Click on Outlook's **Junk Email** folder in the Folder pane.

2. Select the message that you know is from from a trustworthy person, right-click on it, and select **Junk > Never Block Sender** (or **Never Block Sender's Domain**) from the pop-up menu.

    -   If you are using Outlook on the web, select the message, then click **It's not junk** above the message.

3. If you see a confirmation message, click **OK**.

You can also add the sender, or sender's domain, to your Safe Senders list.

Add to Safe Senders list using Outlook

1. Click on the **Junk Email** folder in Outlook's Folder pane.

2. Select the message that you know is from from a trustworthy person, right-click on it, and select **Junk > Junk Email Options…** from the pop-up menu.

3. In the Options dialog, click the **Safe Senders** tab, click **Add…** and type in the email address, or domain, that you want to add to your Safe Senders.

4. Click **OK** – note that you can also choose to trust all email from your Contacts by ticking a checkbox.

5. Click **OK** again to exit the options dialog and save your changes.

Add to Safe Senders list using Outlook on the web

1. Click on **Settings** (the cog icon at the top right of the screen) and **View all Outlook settings.**

2. **Select Email > Junk email in the Settings dialog.**

3. Under **Safe senders and domains**, click **+ Add** and type in the email address, or domain, that you want to add to your Safe Senders – then press Enter to add to your list.

4. Click **Save** then close the Settings dialog.

> You may want to add your Junk Email folder to the **Favorites** section at the top left of Outlook's navigaton pane where it is easier to access. Simply right-click on the Junk Email folder and select **Add to F̲avourites** from the pop-up menu. This creates a handy shortcut to the Junk Email folder at the top of Outlook's navigation pane.

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

The best way to deal with junk mail is to delete it quickly, or use the [Report Phishing](#) button in Outlook for suspected phishing emails. Don't waste time trying to work out why you received it – just press the delete key, or Report Phishing.

- Don't respond to an email from an unrecognized sender or source.

- 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. Click [Report Phishing](#).

- 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, eg 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.

---

[1] IT Policies are published in the Policy Zone on StaffNet – see www.abdn.ac.uk/staffnet/governance/