Guidelines for sending bulk email to large groups

What is bulk email?

Bulk email can be an efficient way of communicating information to a large number of people – for example instructing recipients to visit a website or online system. However, the characteristics of bulk emails mean they are often mistaken for phishing scams[1].

This means that our mail filters may direct your legitimate email straight to recipients' Junk Email folders; or that your recipients suspect your email is a phishing scam and delete it.

The aim of these guidelines is to help you prepare bulk emails that achieve a balance between ease of use and reassurance for recipients.

Notes:

It may not be possible to adhere to all the guidelines listed below on every occasion.

It is important to be aware that targeted attacks (spear phishing) may use information readily available on the University of Aberdeen website in order to mislead recipients. You can offer *your* recipients a level of reassurance by including a detailed explanation of the purpose of the email (see item 2, below) and by providing named and verifiable contact information (see item 8, below).

When composing a bulk email:

1. Include information that a phisher would be unlikely to have access to, for example:
   - Greet the recipient using their first name if possible, i.e. something that is not part of their email address.
   - Include details of a recent action, e.g. '*You last used the system at 14:32 on 9th May*'.
   - Include a high resolution University logo.
2. Provide a detailed explanation of why you are sending the email. Phishing emails by comparison are often vague about their purpose – '*We need you to verify your details*', for example.
3. Double check your email carefully for grammatical errors and spelling mistakes before you send it out. Phishing emails commonly contain such errors.
4. **Never** ask recipients to supply sensitive information (such as username/password, bank details, PIN numbers) by replying to the email, completing a document and sending it back, or clicking on a link and filling in an online form.

[1] See also our user guides for help with 'Protecting yourself from Phishing Scams' and 'Dealing with Junk Mail and SPAM'.

5. It is preferable not to include any links, but if you must:
   - Write all links out in full, using https not http, e.g. https://www.abdn.ac.uk not University website.
   - Avoid using deep or complex links, such as: https://www.abdn.ac.uk/staffnet/documents/policy-zone-information-policies/DIT_cond-IT.pdf

   Note: You may not be able to follow this advice if links are unique to recipients – links to an online survey, for example. If this is the case, try to ensure that nothing else about your email makes it looks like phishing.
6. If you need recipients to go to a web page to login to a system, instead of including a direct login link, describe the simplest way to navigate to the page.
   - For example: 'Go to **StaffNet** and select **Outlook Web Access** from the **Quick Links** section' instead of '*Login to Outlook Web Access*'.
7. Don't attach documents to your email. Instead, ask recipients to download documents from the University website, describing the simplest way to navigate to the document location.
   - For example: 'Download our **Self Certification Form** from the **Holidays, Leave and Absence** section of StaffNet'.
8. Provide a way for recipients to check that your email is genuine.
   - Name an individual or team whose contact details are available in Outlook's address book or can be validated on University website. This allows a recipient to get in touch by other means.
   - Refer recipients to the University website for further information to help validate your message, e.g. '*Search for **TaD Team** on the main University website*'.
9. Emails sent from external systems can be particularly problematic. Before sending, contact the IT Service Desk to ensure that our mail filters will not prevent delivery.
10. Always send emails from a valid University of Aberdeen email address.

Help and Support

Contact the IT Service Desk at https://myit.abdn.ac.uk