IT Security – Phishing Scams

IT Services will NEVER ask you for your University username/password combination by email. If you receive an email that asks for this information – even if it appears to have come from IT Services or from the IT Service Desk – **delete it**.

See the third page of this fact sheet for our quick tips on how to spot a phishing email. You may want to print this out and keep it to hand as a ready reference.

What is phishing?

Phishing is a form of identity theft. Hackers, exploiting our natural human tendency to trust, use spoof emails and/or fake websites to trick us into divulging personal data or downloading malware. It's a low-tech kind of intrusion that relies heavily on human interaction.

A phishing email may appear to come from a trusted source (e.g. the University, or your bank) and may ask you to provide personal confidential information (password, PIN number, or card details) or to click on a link.

Often the email will have a sense of urgency to it; it may suggest that your bank account is about to be closed, or that your mailbox is over quota. It may even hint at the potential repercussions if you don't respond.

It may invite you to click on a link within the message or to open an attachment. Doing either could launch executable files or install malware such as viruses on your computer.

How can I tell if an email is a phish?

While some phishing emails are blatantly fake, many others are more sophisticated.
If you're not sure if an email is genuine or not, read the content carefully; there are many clues which if you're vigilant are easy to spot. For example:

- Be suspicious of any email that requests confidential personal or financial information. No reputable institution or organization, including the University, will ever ask you for such details by email.
- Don't fill out embedded forms that ask for personal information such as usernames, passwords, and PIN numbers.
- 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.
- Don't open files attached to suspicious email messages or if the message is from an unknown sender.
- Don't click on a web link embedded in a suspicious email, or if the email is from an unknown sender. If in doubt, type the link into a web browser manually (don't copy and paste). Or, *before* you click on a link:

  Laptops: Hover your cursor over a link to reveal where the link will really take you.

  Mobile devices: Gently press and hold on a link (long tap) to reveal where the link will really take you

For more quick tips on how to spot a phishing email, see the third page of this fact sheet.

What should I do if I think I've received a phishing email?

Don't respond. Your computing account and computer could be compromised, and the perpetrator could use the information supplied to commit identity theft.

Trust your instincts. If you think it's a phishing email, it probably is. Click the **Report Phishing button** on your Outlook ribbon. If you are using the Outlook Web App or Mobile App, click the 3 dots at the top right of the email to expand the More actions menu and select Report Phishing.

A copy of the email will instantly be sent to the IT Department, who will assess it based on various factors including the reach of the message and severity of the threat. We will then take action to protect the University where necessary.

Additionally, your report will be plugged into Microsoft's global threat intelligence network, helping them prevent malicious emails being delivered to anyone using their email service.

If you're unsure, or you would like advice, contact the Service Desk - servicedesk@abdn.ac.uk or myit.abdn.ac.uk.

Why must I be so vigilant?

The University mail filters scan all incoming messages for phishing and spam email. Email is scored based on keywords, patterns and blacklists. Email with a *high* score is automatically rejected and doesn't make it to your Inbox.

Unfortunately, filtering is not an exact science. The mail filters cannot always distinguish between valid and unsolicited mail; sometimes valid emails will be rejected, and sometimes phishing and spam emails make it through.

To deal with this, we direct low scoring email to your **Junk Email** folder in Outlook and add **SPAM** to the Subject field. This allows *you* to decide what to do with it; after all, one person's junk could be another person's legitimate correspondence.

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

See page three of this guide for our quick tips on how to spot a phishing email.

How to spot a phishing email

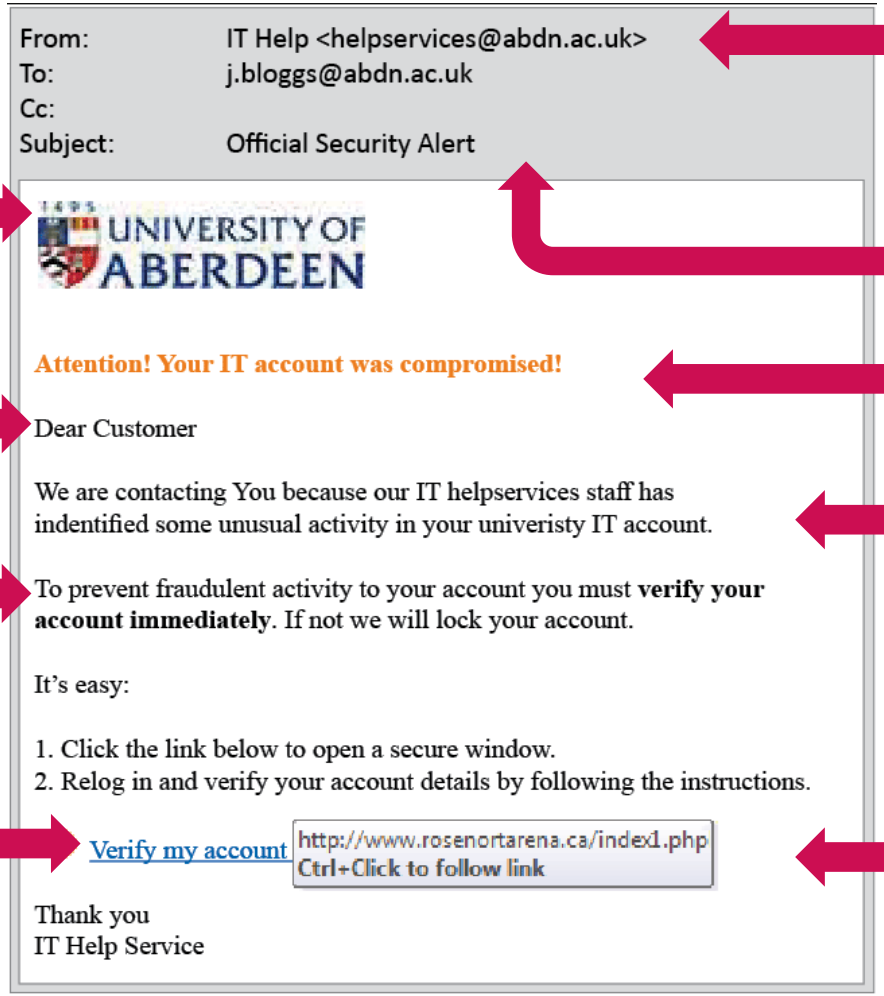
Here are some clues that might help you spot a phishing email.

Logo or other branding.
To fool you into believing the email is genuine. The image may be of poor quality or be used incorrectly.

Impersonal greeting.
A generic salutation such as 'Dear Customer' or 'Dear User' can indicate that an email is spam.

Sense of urgency and threat of repercussion.
To make you respond without thinking.

Invitation to click on a link.
To persuade you to visit a fake website, often inviting you to submit personal, confidential information. Often the action of clicking a link is enough to install malware on your computer.



Forged sender's address.
A phishing email may appear to come from a trusted source but it's easy for phishers to forge an email address. Don't be fooled just because it looks like a real address.

Alarmist or deceptive Subject line.
To persuade you to open the email.

Scare tactics.
To intimidate you.

Spelling mistakes and grammatical errors.
Phishers are not known for their good spelling and grammar! In addition, misspellings make it easier for messages to bypass 'spam filters'. Email from legitimate organisations is usually proofread carefully before being sent out.

Fake URL? *Before* you click on a link…
On laptops: Hover your cursor over a link to see where it will really take you.
On mobile devices: Gently press and hold on a link to see where it will really take you.

Still not sure an email is genuine? Don't click on links, open attachments, or respond in any way. Use the **Report Phishing** button. You can contact the Service Desk for advice at myit.abdn.ac.uk or at servicedesk@abdn.ac.uk. **And remember – IT Services will NEVER ask you for your username and password combination by email.**