

# How to detect a phishing email

## 1. What are they?

- An email from an unknown person **masquerading as a trusted source**, usually claiming to be from an organisation you know such as a bank, government agency, ISP, or that is ‘phishing’ for information.
- The email will try and trick you into **disclosing personal information** such as your password, name, address, phone number, or credit card details by directing you to click on a link, open an attachment, or submit information via an enclosed form.
- Phishing emails usually attempt to acquire user **account details and passwords** from unsuspecting staff and students by requesting users ‘reset’ their accounts or ‘re-validate’ their email mailbox.

## 2. How do I spot a phishing email?

Fortunately, there are a number of common characteristics found in most phishing emails that make them easier to spot.

### The sender

- In most cases, phishing emails will claim to be from a **sender that is external** to the company, such as a known legitimate organisation, like a bank or social media website.
- The email address used by the sender will usually be made to look **similar to the actual email address** of the organisation they are pretending to be, but with some small differences.
- Emails can also be made to **look like they are from the company** however, and may include other Company contact details within the email to make them look more legitimate.

### The addressee

- Phishing emails are usually sent in bulk and so will often contain a **generic greeting** that is not personally addressed to you.
- Sometimes phishing emails will address you personally, making them harder to spot. In these cases, incorrect punctuation or using your **user name as your name** will be giveaways. Also beware of any email that contains your **name in the subject line**.

### What it will look like

- Most phishing emails will use **legitimate logo and branding** in their attempts to masquerade as a known and trusted organisation. Sometimes the quality of this branding is poor or sufficiently different that you will be able to tell something is wrong. Some senders, however, will go to great lengths to make their email look exactly like the real thing.
- The **language** used in phishing emails will often be a giveaway - poor spelling, grammar, or phrases that sound like they have been translated from another language are common.
- Phishing emails often contain **odd formatting**, such as the incorrect use of capital letters and unusual spacing.

- Phishing emails will almost always include a **hyperlink or attachment**. Hyperlinks may display an unusual web address or one similar to an official web address such as "http://syd.ney.com.au/validate" (note the full stop in the middle of the word 'sydney').
- Hyperlinks may even display a correct, legitimate web address, but the link actually takes you to a different, external site. When you hover your cursor over the link you will be able to check the real target web address.

#### **What it will be about**

- The objective of a phishing email is to **obtain information**. Be suspicious of any email that asks you for anything, especially personal information, financial information, account details, or passwords.
- The tone of phishing emails will often convey a **sense of urgency** in an attempt to get users to provide information without considering the risks.
- Phishing emails will often include some **specific detail** to make requests sound more legitimate, such as providing the name of a contact individual (even if it's not a real person) or referencing a particular date.

#### **3. What can I do?**

- **Be suspicious** of emails from people you don't know or expect.
- **Don't provide personal details** via email. Remember, our company will never ask you to provide private information by responding directly to an email. If we require your details or need you to confirm the validity of your account, we will ask you to contact the ICT Helpdesk and speak to one of our staff.
- **Don't click on the link** – always hover your cursor over the link to identify its true location.
- **Never open a file** you are not expecting.
- Use **spam filters**.
- If you received a phishing email, or if you think you may have already responded to such an email, you should **reset your password** and **contact the ICT Helpdesk**.