AWARE | SECURE | RESILIENT

PHISHING ATTACKS

Dealing with suspicious emails.

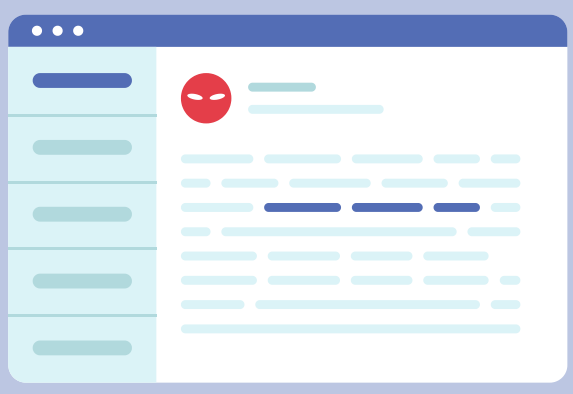
What is phishing?

- Phishing is when criminals masquerade as a legitimate person or organisation in an attempt to trick people into following out instructions that can lead to personal or sensitive information being stolen or to the installation of malicious software (malware).
- Phishing can be conducted over email, social media and other messaging platforms. Phishers also use voice calls (vishing) and SMS text messages (smishing).
- They will typically request the user to click a link or open an attachment. Doing so can result in malware being downloaded and installed or lead to malicious websites.

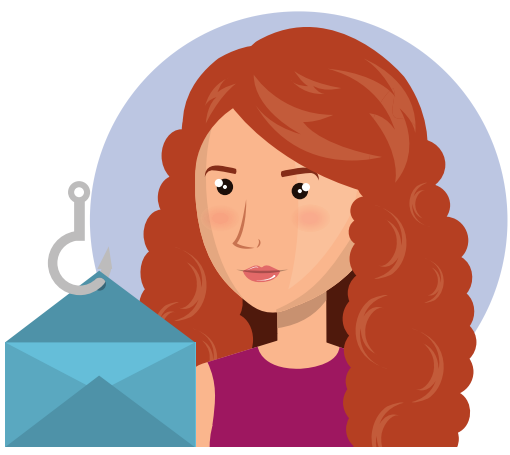
What does a phishing email look like?

Many phishing emails will have poor grammar, punctuation and spelling but that isn't always an indicator. Criminals are improving their technique and some can be difficult to identify.

- Is the design and overall quality what you would expect from the organisation the email is supposed to come from?
- Is it addressed to you by name, or does it refer to 'valued customer', 'friend', or 'colleague'? This can be a sign that the sender does not actually know you.
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'click here immediately'.
- Look at the sender's name and email address. Does it sound and look legitimate, or is it trying to mimic someone you know?
- If it sounds too good to be true, it probably is.
- Your bank, or any other official source, should never ask you to supply personal information from an email.



What should I do?



If you receive a suspicious email:

- Don't click on any links, open attachments or reply to the email.
- If in doubt, contact the person or organisation directly using known contact information.
- Flag the email as spam/junk or use the report function if available on your email client or website, and then delete it. Any future emails from that address should then not be received to your inbox.

If you have already clicked on a link, opened an attachment or provided information:

- Run a full system scan on your anti-virus software and follow any instructions given.
- If you have provided information such as your password, change your password for all accounts using that password.
- If you have lost money, contact your bank as soon as possible.

For more cyber security guidance and resources, please take a look at our OCSIA Knowledge Base. If you have any concerns, or have been affected by a cyber-related issue, report it to OCSIA by submitting a Cyber Concerns Online Reporting Form at www.gov.im/ocsia.