NHS
Informatics Merseyside

SCAM EMAILS

What are scam emails?

Scam emails are fraudulent messages that try to trick you into giving away personal, medical or financial information, or infect your device with malware to steal data. These emails can be very convincing and may appear to come from a legitimate source, such as a person or organisation you know.

How to spot scam emails

SENDER'S ADDRESS

Check the sender's email address carefully. Scam emails may use a fake address that looks similar to the real one but has some subtle differences.

SUBJECT LINE

Look at the subject line of the email. Scam emails may use urgent or threatening language such as "Your account has been suspended" or "You have an outstanding invoice". They may also use generic or vague terms such as "Important message" or "Please read".

CONTENT

Read the content of the email carefully. Scam emails will often include spelling and grammar errors or use poor formatting. They may ask you to do something suspicious like providing your personal or financial information or may offer something that sounds too good to be true such as a job opportunity, refund or prize!

LINKS AND ATTACHMENTS

Hover over any links or attachments in the email before opening them. Scam emails may use fake web addresses that do not match the expected destination. They may also use attachments that contain malware or viruses, such as .exe, .zip, or .docm files.

Protect yourself from scam emails

Scam emails can be very harmful. They can compromise your personal or financial information, damage your device, or expose you and your organisation to further attacks. Here are some tips and best practices to help you protect yourself from scam emails:

- **Verify that the email is genuine.** You can do this by contacting the sender directly using a trusted source such as their official website, phone number, or email address. Do not use any contact details provided in the email, as they may be fake or compromised.
- **Report anything suspicious** immediately to your IT Service Desk.
- **Do not reply to any suspicious emails**. Replying may confirm that your email address is active and encourage the sender to send you more emails or target you with more sophisticated attacks.
- **Do not click or open any links or attachments in suspicious emails**. Clicking or opening may redirect you to a fake or malicious website, or download malware or viruses to your device.
- **Update your device** by regularly restarting to enable important security updates to be installed. Shutting down your computer is not the same as restarting and a full restart is required to enable important security updates to be installed.

For cyber security guidance and advice, please contact your IT Service Desk.