Cyber Security Alert

Scam Emails

Police Scotland Cybercrime Harm Prevention Team.
26.06.2025

Recognise, Reject and Report scam emails, texts, websites.

Cyber-criminals will take advantage of any situation to target and scam the public and we can expect to see scam email and texts in circulation, purporting to be from organisations who have been the victim of cyber-attacks.

You may or may not be associated to an affected organisation, but the cybercriminals don't care about that, they want you to be drawn into their scam.

Part of that scamming process is to send out thousands of emails and texts which have been very carefully written and presented, perhaps with an affected organisations logo, to catch their victims out.

These scam emails and text messages are made very personal and could relate to pensions, benefits, allowances and other services.

They do this to quickly gain your trust. This makes the scam look and sound more authentic and will most offer some form of incentive for the victim. This could be to open a link to claim a reward or download a voucher as a form of apology as affected customer.

In some cases, the scam email will put the victim under pressure saying there is a limited time to respond, or some other negative comment or urgency to reply such as to pay a parking fine within a limited amount of time.

In addition to links, cybercriminals can also include QR codes which, when scanned, will trick the victim into visiting scam websites.

It is vitally important that you do not respond to these scams or share your personal details / data on any online platform or through any communication you have not initiated.

If you receive any suspicious email or text, take your time to consider if it is genuine, does it really relate to you and your personal circumstances. If not and you are unsure how to deal with it, please take your time and read the information in the links below and share this guidance document.

We have included the following links to the NCSC (National Cyber Security Centre) for your information and added awareness in [How to spot a scam email, text message or call - NCSC.GOV.UK](#)

If you think you have responded to a scam email, or been tricked into scanning a QR code or shared password or banking details, please take action with this [Phishing scams: If you've shared sensitive information - NCSC.GOV.UK](#)

If you suspect your details have been included in a Data Breach this link will provide you with support on how to manage that. [Data breach guidance for individuals – NCSC.GOV.UK](#)

To help tackle cybercriminals who send scam emails, you can help us by reporting these to **[Report a scam email - NCSC.GOV.UK](#)**

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101.