This alert is a reminder to be aware of emails that appear to have been sent from a legitimate organisation. Fraudsters often use fake email addresses designed to encourage recipients to open attachments or links. You are advised that if you are in any doubt as to the origin of an email, do not open it. Consider that emails can be spoofed and used to generate spam to recipients far and wide. If you receive a spam email, you MUST NOT open it. Instead, delete it from your email system to avoid infecting your device. If you have opened an attachment from a spam email, you should get your device checked over by a professional and change the passwords for all your bank, email and online shopping accounts.

Protect yourself:

- Do not click or open unfamiliar links in emails or on websites.
- Make sure you install and use up-to-date anti-virus software.
- Have a pop-up blocker running in the background of your web browser.
- If you have opened an attachment and 'enabled macros' it is very likely that all your personal data will have been breached. You MUST change all your passwords for personal accounts, including your bank accounts.
- Ensure Adobe, Flash and any similar software is up to date on your computer.

If you think you have been a victim of this type of email you should report the email to Action Fraud, the UK's national fraud and cyber crime reporting centre: www.actionfraud.police.ukIf you do make a report please provide as much detail as you can about the email and any effects it has had on your computer. Additionally if your Anti-Virus software detects any issues in relation to this email please provide us with the details.