ROYAL borough of GREENWICH

ALERTS
TRADING STANDARDS
22/09/2025

Scam warning: fake government Emergency Alerts emails

These bogus emails ask for feedback on the recent Emergency Alerts test **that took place on 7 September.**

The worryingly convincing emails appear to come from ‘Government Digital Services’ and recipients may be easily tricked into clicking a malicious link to complete a survey about the recent test.

Emergency Alerts email scam

One email titled ‘Emergency Alerts - Confirmation’ contains many hallmarks of an email that could appear to be trusting. It has gov.uk branding, the style of the email feels genuine, and it even contains links to genuine government advice pages about the Emergency Alerts test.

On closer inspection of the email, recipients will quickly find that it isn’t from ‘Government Digital Services’, as it suggests. Instead, the sender's email has been masked, or 'spoofed’, to disguise the random email address that the sender is using. Spoofing the email address to make it appear as though the email is from a trusted source is a common tactic and one that's not always easy to spot.

Most worrying though, is that the email asks whether you received the Emergency Alert test on 7 September, prompting you to click on either ‘yes’ or ‘no’. Reports suggest they contain malware. This is a type of software that can be installed on your device after you click on it and allows a scammer to steal personal information or take over accounts.

There are several different email senders, none of which are genuine .gov.uk email accounts. The government has also confirmed that it is not sending emails asking for feedback.

How to spot and report scam emails

Always be suspicious of an unexpected email, especially if you're being asked to click on a link, make a payment or log in to an account.

Pay attention to the sender's details by hovering over the email address on a computer or inspecting the email address with a long press on a mobile device. This will reveal the sender's true email address.

Forward scam emails to report@phishing.gov.uk, as this is the quickest way to get them taken out of circulation. Also, flag it as 'spam' in your inbox to tell your email provider to direct dodgy emails like these straight to your spam folder.

If you're concerned that an email could be genuine, don't click on any links or follow any instructions from the email. Instead, you should verify the email with the organisation it claims to be from by contacting them directly using details found on its website.

If you lose any money to a scam, call your bank immediately using the number on the back of your bank card. Report scams to Action Fraud.

WHERE TO REPORT

Protect others by reporting incidents like this.

Report suspicious texts you have received but not acted upon, by forwarding the original message to 7726, which spells SPAM on your keypad.

Report suspicious emails you have received but not acted upon, by forwarding the original message to report@phishing.gov.uk

If you, or anyone you know, have been affected by this fraud or any other scam, report it to Action Fraud by calling 0300 123 2040 or visiting www.actionfraud.police.uk

tradingstandards@royalgreenwich.gov.uk