32 Million suspicious emails reported by the public [#278126363]

From: North Yorkshire Community Messaging (alert@neighbourhoodalert.co.uk)

To: editorbmtoday@aol.com

Date: Friday, 28 June 2024 at 20:15 BST

northyorkshire community messaging

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

32 Million suspicious emails reported by the public

Dear subscriber,

Over 32 million suspicious emails have been reported to the Suspicious Email Reporting Service (SERS), with more than a third of all emails reported in the last year, new figures reveal.

The reports have led to more than **329,000 websites addresses being removed** by the National Cyber Security Centre. Action Fraud, the national fraud and cybercrime reporting service, launched a national phishing awareness campaign on 24 June 2024, as reporting reached its highest level since SERS launched. New data shows a rise of 44% year-on-year, with almost 11,611,400 reports made to SERS in 2023, up from 8,074,200 reports in 2022.

Alongside emails, there has also been a huge number of text messages reported to 7726. In March 2024, **more than 60,000 malicious websites were removed as a result of being reported using 7726**. This is a free service, offered by mobile network providers, allowing customers to report suspicious text messages in order to prevent other people from receiving them too.

Claire Webb, Deputy Head of Action Fraud, said:

“When fraudsters go phishing for valuable information, anyone could be a target. They will hook an unknowing victim with a genuine-looking email, in a bid to get them to share personal information, or bank details.

“Year on year, the amount of people reporting phishing emails and texts is growing. Action Fraud is urging everyone to be extra vigilant of suspicious-looking emails landing in their inbox, which could contain malicious links leading to unknown websites.

“Remember, if you think you have received a phishing email or text message, make sure you report it. You can forward emails to report@phishing.gov.uk, or forward spam text messages to 7726.”

SERS was launched by the National Cyber Security Centre (NCSC) and the City of London Police in April 2020, to enable the public to forward suspicious emails and report any malicious website links. Since its launch, more than 32 million reports have been made to the service.

What is phishing?

'Phishing', 'quishing' or 'smishing' is when criminals use scam emails, text messages, QR codes, or phone calls to trick victims. Whether it's an email asking you to "verify" your bank account details, or a text message claiming you've missed a delivery and are required to pay a redelivery fee, the goal is usually the same - to trick you into revealing personal and financial information.

In 2023, a doctor from London lost more than £150 to a fake email claiming to be from TV Licensing. The email claimed that they needed to renew her TV licence as soon as possible. What made the phishing email so believable was that the victim's TV licence had recently expired and the link in the email led to a fake TV Licensing website that replicated the real one.

Here's some practical advice you can follow when it comes to dealing with suspicious messages and calls:

If you have any doubts about a message, contact the organisation directly using the contact details on their official website.

- Do not use the number or web address in the message. Your bank, or any other official source, will not ask you to provide sensitive information by email.

Received an email that doesn't feel right? STOP! Report suspicious emails by forwarding them to: report@phishing.gov.uk. Send emails to this address that feel suspicious, even if you're not certain they're a scam – they will be checked. Always report suspicious text messages or scam call numbers, free of charge, to 7726. Your provider can find out where the text came from and block or ban the sender.

- To report a scam text, forward it to 7726 and then send the sender's number when prompted.
- To report a scam call, simply text 7726 with the word 'Call' followed by the scam caller's number.

If you've lost money or provided financial information as a result of a phishing scam, notify your bank immediately and report it to Action Fraud at actionfraud.police.uk or by calling 0300 123 2040. In Scotland, call Police Scotland on 101.

(If you found this information useful, please share it)

Message Sent By
Action Fraud
(Action Fraud, Administrator, National)