ActionFraud ALERT

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Over 5M Suspicious Emails Reported

Phishing remains the most successful attack vector for cyber criminals targeting individuals and businesses.

Cyber criminals love phishing. Unfortunately, this is not a harmless riverbank pursuit. When criminals go phishing, you are the fish and the bait is usually contained in a scam email or text message. The criminal's goal is to convince you to click on the links within their scam email or text message, or to give away sensitive information (such as bank details). These messages may look like the real thing but are malicious. Once clicked, you may be sent to a dodgy website which could download viruses onto your computer, or steal your passwords.

As of 30 April 2021, over **5.8 million** emails were reported to the Suspicious Email Reporting Service (SERS). The tool, which was launched by the National Cyber Security Centre (NCSC) and the City of London Police last April, allows the public to forward suspicious emails to an automated system that scans it for malicious links. Since its launch, over **43,000 scams** and **84,000 malicious websites** have been removed.

What are the most common phishing scams?

The most commonly spoofed organisation reported in phishing emails was TV Licensing, with victims of these emails reporting losses totalling **£5.3m**. The majority of losses occurred as a result of victims following malicious links in the emails and inputting their personal information into what they thought was the legitimate TV Licensing website. Shortly after, they would receive a call from criminals impersonating bank staff who was able to convince them that their bank accounts were compromised and persuaded them to transfer all of their money to a new 'safe' account. Some of the other most commonly impersonated organisations included HMRC and DVLA. We also received more than 40,000 suspicious email reports relating to COVID-19.

How you can protect yourself from phishing messages.

Fake emails and text messages can sometimes be difficult to spot and criminals are constantly getting better at finding ways to make them seem more authentic. Email address spoofing, for example, is just one of the tactics criminals will use to try and make their fake emails look real. Here are some tips you should follow to protect yourself, and others, from scam emails and text messages:

1: Be cautious of messages asking for your personal information. Official organisations, such as your bank, should never ask you for personal or financial information via email or text message. If you receive a message and you want to check that it's legitimate, you can call the organisation directly using a known number, such as the one on a bank statement or utility bill.

2: Report suspicious emails. If you receive an email you're not quite sure about, you should report it to the Suspicious Email Reporting Service (SERS) by forwarding the email to: **report@phishing.gov.uk.** Your reports will help government and law enforcement agencies to remove malicious emails and websites.

3: Report suspicious text messages. If you receive a suspicious text message, you can report it by forwarding the message to **7726**. It's free of charge and enables your mobile network provider to investigate the origin of the text and take action, if found to be malicious.

4: Report fraud. If you've lost money or provided personal information as a result of a phishing scam, notify your bank immediately and report it to Action Fraud.

For more information on how to protect yourself from fraud and cyber crime, please visit: actionfraud.police.uk/cybercrime