Cyber Security (Jun 2025 update)

As of April 2025, the total number of phishing scams reported to the Suspicious Email Reporting Service (SERS) reached over 41 million since its launch in April 2020. This has resulted in 217,000 scams being removed from across 393,395 websites pages by the National Cyber Security Centre.

Insight revealed by Action Fraud shows the top industries impersonated in reported phishing emails were streaming services, tech and telecommunication companies, with some posing as various UK government schemes.

Action Fraud, the national fraud and cyber crime reporting service, launched a phishing awareness campaign to urge the public to beware of phishing scams and report all emails and messages if they look suspicious.

Spam calls and suspicious text messages can be reported too. By using 7726, a free service offered by mobile network providers, customers can forward suspicious text messages, which helps the removal of scam websites and allows networks to block users sending scam text messages. Between April 2020 and April 2025, more than 27,000 scams were removed as a result of being reported using 7726.

Superintendent Amanda Wolf, Head of the National Fraud Intelligence Bureau at the City of London Police, said:

“We know it can be difficult to spot fake messages or tell if a call is genuine. Criminals can change tactics fast and use the technology available to constantly create genuine looking emails and messages or facilitate calls that feel authentic - all designed to trick us and try and steal personal and financial information.

“Every phishing email reported helps us gain a better understanding of the tactics being used and enables us to tackle it head on by identifying malicious URLs trending in phishing emails and texts - they can be taken down and disrupted, preventing further activity. The more reports received, the more people we can protect, preventing them from becoming victims.

“Don’t get caught out, Stop, Think Fraud, and make sure you report suspicious-looking emails or messages if you receive them. You can forward emails to report@phishing.gov.uk, or forward spam text messages to 7726.”

Sarah Lyons, NCSC Deputy Director for Economy and Society Resilience, said:

“Since 2020, over 41 million phishing attempts have been reported to the Suspicious Email Reporting Service — a powerful sign that the public is staying alert to online threats, helping to protect themselves and others.

“But cyber criminals aren’t giving up - they’re constantly finding new ways to trick people into clicking malicious links, sharing personal information, or handing over money.

“That’s why it’s more important than ever to stay alert. You’ll find clear, practical advice on how to spot and report scams - and how to stay secure online - on the NCSC website.”

What is phishing?

'Phishing', ‘quishing’ or ‘smishing’ is when criminals use fake emails, text messages, QR codes, or phone calls to trick victims.

The goal of a phishing message is to encourage the victim to click a malicious link, or scan a fraudulent QR code, which usually leads them to a genuine-looking website, designed to make victims part way with their financial and/or personal information. Criminals will use well-known brands or organisations the victim already has a connection with, like a bank or tradesperson, to make fake emails seem genuine and more convincing.

How can you protect yourself?

If you’ve received an email that doesn’t feel right, STOP!

□ break the contact – don’t reply, click on any links, call any phone numbers or make any payments

□ check if it’s genuine: contact the organisation directly using an email address or phone number you know is correct, e.g. from your utility bills, via a search engine, on the back of your card or by calling 159 for banks

□ before you delete the email, forward it to report@phishing.gov.uk

If you’ve received a text message that doesn’t feel right, STOP!

□ break the contact – don’t reply, click on any links, call any phone numbers or make any payments

□ check if it’s genuine: contact the organisation directly using an email address or phone number you know is correct, e.g. from your utility bills, via a search engine, on the back of your card or by calling 159 for banks

□ forward the message for free to 7726

If you’ve received a call that doesn’t feel right, STOP!

□ hang up

□ check if it’s genuine: contact the organisation directly using contact details you know are correct, such as those on a utility bill, official website, the back of your card or by calling 159 for your bank

□ don’t trust the Caller ID display on your phone – it’s not proof of ID

□ report it by sending a text to 7726 with the word ‘call’ followed by the scam caller’s number

For more advice on how to protect yourself from fraud: https://stopthinkfraud.campaign.gov.uk/

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.