

INFORMATION

Phishing: how to report to the NCSC

Discover how to report a potential phishing message to the NCSC using the Suspicious Email Reporting Service (SERS)



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.

Have you spotted a suspicious email?

If you have received an email which you're not quite sure about, forward it to the Suspicious Email Reporting Service (SERS):

report@phishing.gov.uk

The message might be from a company you don't normally receive communications from, or someone you do not know. You may just have a hunch. If you are suspicious, you should report it.

Your report of a phishing email will help us to act quickly, protecting many more people from being affected.

In a small number of cases, an email may not reach our service due to it already being widely recognised by spam detection services. The vast majority of reports do reach our system so please keep reporting any suspicious emails you receive.

If you continue to have problems then please [contact us](#) so we can investigate it further.

As of **30 September 2020** the number of reports received stand at more than 2,930,000 with the removal of 13,291 scams and 30,344 URLs.

Thank you for your continued support.

Reported an email? Here's what happens next...

The NCSC will analyse the suspect email and any websites it links to. We'll use any additional information you've provided to look for and monitor suspicious activity.

If we discover activity that we believe is malicious, we may:

- seek to block the address the email came from, so it can no longer send emails
- work with hosting companies to remove links to malicious websites
- raise awareness of commonly reported suspicious emails and methods used (via partners)

Whilst the NCSC is unable to inform you of the outcome of its review, we can confirm that we do act upon every message received.

Please note...

You should not report a crime to the NCSC in this way. If you think you may have been a victim of fraud or cyber crime, and live in England, Wales or Northern Ireland, you should report this to Action Fraud at www.actionfraud.police.uk or by calling 0300 123 2020. If you live in Scotland, you should report to Police Scotland by calling 101.

Protecting yourself from phishing attacks and staying secure online

If you have reported a suspicious email or message then thank you – this will help us to track and stop many cyber criminals using phishing as a form of attack.

There are a number of ways you can protect yourself from attacks like this and the NCSC has published plenty of advice which will help you to stay secure online:

- [The NCSC's top tip for staying secure online](#)
- [Phishing attacks: how to deal with suspicious messages and emails](#)
- [Securing your devices](#)

For a full overview of the NCSC's advice for the general public please head to our dedicated [individuals and families webpage](#).

How we handle the information you send to us

- Information provided to the NCSC is protected in the same way we protect our own confidential information: It is held securely, with strictly limited access.
- We may share details with our Law Enforcement partners, such as the National Crime Agency and the City of London Police, to help identify investigation and mitigation opportunities.
- The information we hold is exempt from Freedom of Information requests.
- For further detail on how we handle information you send us, please see our [Privacy Statement](#).

PUBLISHED

21 April 2020

REVIEWED

2 September 2020

WRITTEN FOR [Individuals & families](#)