

## What is phishing and how does it work?

You wouldn't let a thief enter your home, but what if the thief were masquerading as someone familiar, such as a postman, and tricked you into opening the door? Phishing works in a similar way - criminals impersonate trusted organisations by creating legitimate-looking messages and websites in order to trick people into opening the doors to their personal information. Once criminals have this information, it can be used to perpetrate fraud and cyber against you, or in your name.

### How big is the problem?

Phishing attacks are a common problem faced by both individuals and businesses on a daily basis.

**As of 31st May 2022, the National Cyber Security Centre's Suspicious Email Reporting Service (SERS) has received over 12mn reports from the public and has removed over 83,000 scams and 153,000 malicious websites.** The most impersonated organisations in phishing emails reported last year were the NHS, HMRC and GOV.UK.

Most phone providers are part of a scheme that allows customers to report suspicious text messages for free by forwarding it to **7726**. When a text is reported to **7726**, the provider can investigate the origin of the text and arrange to block or ban the sender if it's found to be malicious. **As of May 2022, 13,000 scams have been removed as a result of suspicious text messages reported using the 7726 service.**

### How can you protect yourself from phishing scams?

Most of the phishing scams reported to us have one thing in common, they started with an unexpected email or text message. Whether it's an email asking you to "verify" your bank account details, or a text message claiming you've been in close contact with someone that's got COVID, the goal of a phishing attack is usually the same - to trick you into revealing personal and financial information.

Here's some simple advice you can follow when it comes to dealing with phishing scams:

**1** - If you have any doubts about a message, contact the organisation directly.


**Don't** use the numbers or address in the message – use the details from their official website. Remember, your bank (or any other official source) will never ask you to supply personal information via email.

2 - If you think an email could be a scam, you can report it by forwarding the email to: [report@phishing.gov.uk](mailto:report@phishing.gov.uk). Send us emails that feel suspicious, even if you're not certain they're a scam - we can check.

3 - Most phone providers are part of a scheme that allows customers to report suspicious text messages for free by forwarding it to **7726**. If you forward a text to **7726**, your provider can investigate the origin of the text and arrange to block or ban the sender if it's found to be malicious.

4 - 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: [www.actionfraud.police.uk](http://www.actionfraud.police.uk)

For more advice on how to protect yourself online, visit: [cyberaware.gov.uk](http://cyberaware.gov.uk)

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

[#safercambs](https://www.actionfraud.police.uk/#safercambs)

**Action Fraud**  
National Fraud & Cyber Crime Reporting Centre  
 **0300 123 2040** 



Over 12 million suspicious emails reported by the public

