How to avoid getting hooked by phishing scams

#ReportThePhish
Most spoofed brands used in phishing emails
HM Revenue & Customs
£405.70 GBP
GOV.UK
NHS
ActionFraud
NPCC
Cyber Aware
Working in partnership to protect the UK public and businesses from fraud and cyber crime.

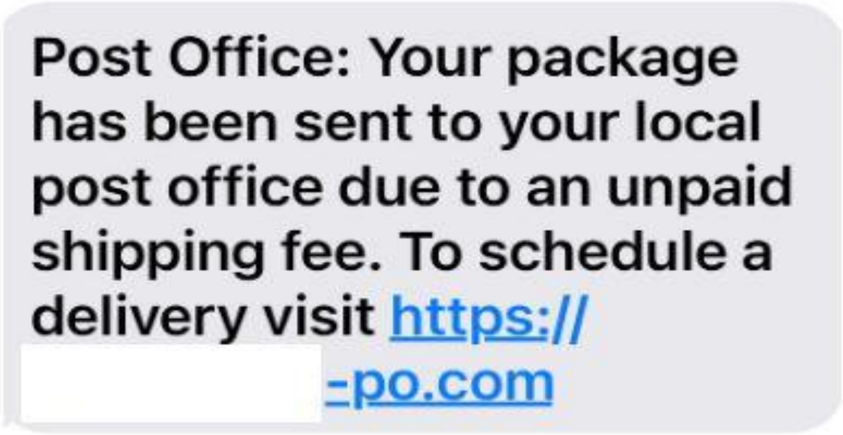
HMRC, GOV.UK, and the NHS were the most spoofed brands used in phishing emails reported to the Suspicious Email Reporting Service (SERS) last year.

Action Fraud and City of London Police are running a national awareness campaign this week.

Avon and Somerset Police are urging people to remain vigilant when it comes to suspicious messages to protect themselves from scammers.

Known as phishing, text messages and emails impersonating well-known organisations remains a common tactic used by criminals. Whether it’s a fake email asking for an individual to ‘verify’ bank details or a text message claiming they have been in contact with someone that has Covid-19, the goal is usually the same – to trick an individual into revealing personal and financial information.

Nationally, the most impersonated organisations in phishing emails reported last year were the NHS, HMRC and Gov.uk.



Post Office: Your package has been sent to your local post office due to an unpaid shipping fee. To schedule a delivery visit https://[redacted]-po.com

An example of a scam where the fraudster pretends to represent the Post Office.

As of 31 May 2022, the public has made more than 12 million reports to the Suspicious Email Reporting Service (SERS), with the removal of approximately 83,000 scams and 153,000 malicious websites.

SERS was launched by the National Cyber Security Centre and the City of London Police in April 2020 to enable the public to forward suspicious emails to an automated system that scans them for malicious links.

DS Tom Williams, of the Cyber Crime team said: “Many people will recall having received a suspicious link or text, as these phishing scams are among the most common threats we face. It can affect individuals and businesses and have significant consequences on the victim’s financial situation.

“It is important that if you ever receive one of these links that you do not click on it and provide personal or banking information. Instead, forward the message to the text or email reporting system and block the email address or phone number so the fraudsters cannot reach you again.”

People are also advised to take time to consider what you have received and what the message is asking you. Discuss the message with family and friends as they will often have experienced something similar and can help you to identify the scam.

PCC Mark Shelford, national PCC lead for Economic and Cybercrime, said: “Phishing scams are another example of fraudsters wanting to financially benefit from both individuals and businesses. Please be vigilant of unexpected messages or calls that ask for your personal or financial information.

“If you do receive call or message that you think might be a scam, do not respond to it. Instead, contact the organisation directly using contact information from the company’s official website and not the links or numbers provided in the message.

“Your bank or any other official source will never ask you to supply personal information via email or text message. The more awareness this is around such scams, the more people we can protect to falling victim to these heartless scammers.”

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 rearrange to block or ban the sender if it’s found to be malicious.

As of May 2022, 13,000 scams nationally have been removed as a result of suspicious text messages reported using the 7726 service.

How to deal 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**. 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**.