Phishing: Spot and report scam emails, texts, websites and calls

How to recognise and report emails, texts, websites, adverts or phone calls that you think are trying to scam you.

What is phishing?

'Phishing' is when criminals use scam emails, text messages or phone calls to trick their victims. The aim is often to make you visit a website, which may download a virus onto your computer, or steal bank details or other personal information.

This page explains how to report phishing attempts, and protect yourself from scammers.

Why you should report phishing scams

The National Cyber Security Centre (NCSC) is a UK government organisation that has the power to investigate and take down scam email addresses and websites.

Reporting a scam is free and only takes a minute. By reporting phishing attempts, you can:

- reduce the amount of scam communications you receive
- make yourself a harder target for scammers
- protect others from cyber crime online

As of August 2024 the number of reports received stands at more than:

34m reported scams

Which has resulted in:

193k scams being removed across 352,679 URLs

What to do next

Report a scam email

How to report suspicious emails, and what to do if you think you've responded to a scam email.

Report a scam text message

How to report suspicious text messages, and what to do if you think you've responded to a scam text.

Report a scam phone call

How to report a suspicious phone call, and what to do if you think you have been the victim of a phone scam.

Report a scam website

How to report a suspicious website, and what to do if you think you've shared personal information.

Report a scam advert

How to report an online advert that you suspect is trying to scam you.

Phishing scams: What to do if you've shared personal information

What to do if you've shared personal information with someone you think might be a scammer.

How to spot a scam email, text message or call

Recognise the signs someone is trying to scam you, and learn how to check if a message you have received is genuine.

Make yourself a harder target

Criminals use information about you that's available online (including on social media sites) to make their phishing messages more convincing.

You can reduce the likelihood of being phished by thinking about what personal information you (and others) post about you, and by reviewing your privacy settings within your social media accounts.

PUBLISHED

26 November 2021

REVIEWED

5 September 2022

VERSION

2.0

WRITTEN FOR

Individuals & families