National Cyber Security Centre

Phishing attacks

Dealing with suspicious emails

Phishing emails try to convince users to click on links to dodgy websites or attachments, or to give sensitive information away (such as bank details). This advice includes tips about how to spot the most obvious signs of phishing, and what to do if you think you've clicked a bad link. For more information, please visit www.ncsc.gov.uk/phishing .

What is phishing?

Phishing is when criminals attempt to trick people into doing 'the wrong thing', such as clicking a link to a dodgy website.

Phishing can be conducted via a text message, social media, or by phone, but the term 'phishing' is mainly used to describe attacks that arrive by email.

Criminals send phishing emails to **millions of people**, asking for sensitive information (like bank details), or containing links to bad websites. Some phishing emails may contain viruses disguised as harmless attachments, which are activated when opened.

Make yourself a harder target

Information from your website or social media accounts leaves a 'digital footprint' that can be exploited by criminals. You can make yourself less likely to be phished by doing the following:

Criminals use publicly available information about you to make their phishing emails appear convincing. Review your privacy settings, and think about what you post.

Be aware what your friends, family and colleagues say about you online, as this can also reveal information that can be used to target you.

If you have received an email which you're not quite sure about, forward it to the NCSC's suspicious Email Reporting Service (SERS): report@phishing.gov.uk

What to do if you've already clicked ?

The most important thing to do is not to panic. There are number of practical steps you can take:

Open your antivirus (AV) software, and run a full scan. Follow any instructions given.

If you've been tricked into providing your password, you should change your passwords on all your other accounts.

If you have lost money, you need to report it as a crime to Action Fraud. You can do this by visiting www.actionfraud.police.uk.

Tell tale signs of phishing

Spotting a phishing email is becoming increasingly difficult, and even the most careful user can be tricked. Here are some tell tale signs that could indicate a phishing attempt.

Is the email addressed to you by name, or does it refer to 'valued customer', or 'friend' or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.

Others will try and create official-looking emails by including logos and graphics. Is the design (and quality) what you'd expect?

Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.

Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?

Your bank (or any other official source) should never ask you to supply personal information in an email. If you need to check, call them directly.

If it sounds too good to be true, it probably is. It's most unlikely that someone will offer you designer trainers for £10, or codes to access films for free.