HOW TO SPOT AND REPORT SCAMS

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

What is phishing?

'Phishing' is when criminals use scam emails, text messages, instant messaging (such as Messenger or Whatsapp) or phone calls to trick their victims. The attacker usually pretends to be from a well-known company, or poses as someone trusted. Their goal is usually to convince you to click on a link, which allows them access to your computer or phone, or to trick you into providing sensitive information such as bank details or other personal information.

Some initial phishing emails don't contain a link or attachment and are simply testing if they can get a reply before they send malicious links or ask for your personal information.

Recognise the signs someone is trying to scam you

If a text or instant message, email or call doesn't feel right, stop and consider these tell-tale signs:

- Authority - Is the message claiming to be from someone official? For example, your bank, doctor, a solicitor, or a government department. Criminals often pretend to be important people or organisations to trick you into doing what they want.
- Urgency - Are you told you have a limited time to respond (such as 'within 24 hours' or 'immediately')? Criminals often threaten you with fines or other negative consequences.
- Emotion - How do you feel when reading the message – Panic? Anger? Curious? Triggering human emotions is a common way to get people to respond to the email. Scammers try to quickly gain your trust and they aim to pressure you into acting without thinking. Many phishing emails are connected to topics that provoke quick reactions such as payment issues, security alerts, or urgent action required. Criminals may often use threatening language, make false claims of support, or tease you into wanting to find out more.
- Perks, prizes or promises - Is the message offering something in short supply, like concert tickets, money or a cure for medical conditions? Fear of missing out on a good deal or opportunity can make you respond quickly.
- Current events - Are you expecting to see a message like this? Criminals often exploit current events such as news stories, major events or specific times of the year (like tax reporting or COVID-19) to make their scam seem more relevant to you.
- Spelling and grammar - Phishing emails often contain spelling mistakes along with poor grammar or may feature imagery or design that is blurry, or just feels 'off'. Though it's worth remembering that scammers are getting really good at copying brands, so this isn't always the case.

Source: National Cyber Security Centre (NCSC)

How to check if a message is genuine

If you have any doubts about a message, contact the organisation directly. Don't use the numbers, links 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, text or instant message.

Protect yourself from phishing attempts and scammers on social media

Social media is a useful way to stay in touch with family, friends and keep up to date on the latest news. However, 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 and strengthening your privacy settings within your social media accounts. Most sites will make this easy for you to do by explaining what each setting means.

Reporting and taking action on 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. If you have received an email which you're not quite sure about, you can forward it to report@phishing.gov.uk. You can send emails that feel suspicious, even if you're not certain they're a scam – the NCSC can check.

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

Remember to NEVER click on any links in a suspicious email, even the "Unsubscribe" button. You can find further information **here** about what to do if you think you have been the victim of a scam.

COVEA INSURANCE PLC
Registered Office: A&B Mills, Dean Clough, Halifax, HX3 5AX
Registered in England and Wales No. 613259
Authorised by the Prudential Regulation Authority and regulated by the
Financial Conduct Authority and the Prudential Regulation Authority No. 202277

Source: National Cyber Security Centre (NCSC)