Do you know how to spot a phishing email?

GET SAFE ONLINE .org

www.getsafeonline.org

email has always been the most commonplace method used by online fraudsters to trick innocent people out of their money, their identity… or both.

It still is. And currently, they're exploiting the current Coronavirus pandemic with persuasive messages ranging from vaccines and cures to tax refunds and fake charity appeals.

Fraudsters send emails containing links which seem authentic, but actually lead to websites designed to capture your confidential details, or infect your devices with viruses and other malware. Or they attach malicious files which, if opened, do the same.

These days, fraudulent emails are becoming ever more convincing, looking as if they come from your bank, favourite retailer, NHS, HMRC, law enforcement, courier company or other organisation you know and trust. You can't rely on poor spelling, bad grammar and far-fetched messages any longer to spot a fake. Fraudsters can even spoof their sender address to make them seem completely authentic.

Our experts have compiled some simple tips to help you protect yourself from falling for fraudulent emails.

#safeemail

Top tips for using email safely and securely

- **If you receive an email you haven't requested or it seems suspicious in any way,** make sure it's actually from the person or organisation who claims to have sent it. Do this by calling the actual person or organisation on a number you know to be the right one.
- **Don't click on links in emails from unknown sources,** or if it seems strange that the email would come from that source.
- **Never open attachments from unknown sources,** or if it seems strange that the email would come from that source.
- **Check for poor design, grammar and spelling,** and whether the email addresses you by your name. However, even if an email passes these tests, it may still be from a fraudster.

- **Don't make purchases,** payments or charity donations in response to spurious emails.
- **Beware of emails which suggest that you need to transfer money,** provide personal details or perform some other critical action urgently to 'resolve a problem'. Banks, government departments, the police and other trusted organisations would never communicate with you in this way.
- **Don't reply to an email which you suspect is fraudulent,** and don't forward it unless you're reporting it.
- **Don't click on 'remove' or reply to unwanted email** – this simply tells senders that your account is live, and may result in you getting a flood of unwanted scam or spam emails.
- **Make sure spam filters are switched on and set up appropriately to avoid unwanted emails getting through,** but permitting authentic ones from trusted sources. Check junk mail folders regularly in case a legitimate email is filtered there in error.
- **Use strong passwords to prevent your email accounts from being hacked.** Keep passwords to yourself, and don't use the same or a similar one for more than one online account.
- **When sending emails to multiple people,** list their addresses in the 'BCC' (blind copy) box instead of in the 'To' box. In this way, no recipient will see the names of the others, and if their addresses fall into the wrong hands there will be less chance of you or anybody else receiving phishing or spam emails. Delete everyone in the email trail before forwarding or replying.
- **Think twice** before you click on anything.

During this pandemic, we have seen a huge increase in the number of fraudulent emails being sent by cybercriminals. For comprehensive, practical, impartial advice on safe and secure email, visit www.getsafeonline.org/safeemail

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by a number of government departments, law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit **www.getsafeonline.org**

If you think you have been a victim of fraud, report it to Action Fraud at actionfraud.police.uk or by calling 0300 123 2040. If you are in Scotland, contact Police Scotland on 101.

GET SAFE ONLINE .org

www.getsafeonline.org

OFFICIAL PARTNERS

TESCO · kaspersky · Gumtree · Standard Life · first direct · PayPal · HSBC · Royal Bank of Scotland · NatWest · M&S BANK · LLOYDS BANK · HALIFAX · BANK OF SCOTLAND · creativevirtual · ROYAL AIR FORCE · HM Government · CITY OF LONDON POLICE · NPCC · NATIONAL TRADING STANDARDS eCrime Team · cifas · VICTIM SUPPORT · EUROPOL EC3 European Cybercrime Centre · NCA National Crime Agency · ActionFraud · METROPOLITAN POLICE · Ofcom · CYBER AWARE