How to avoid online phishing scams

During these difficult times BT are helping to keep the nation connected with a range of Top Tips on Tech. The following are a range of suggestions to help you avoid online scams, known as 'phishing'.

What is phishing?

Phishing is when someone tries to obtain your personal information, like usernames, passwords or credit card details by disguising themselves as a trustworthy person or business. This could be done using email, calls, texts or even fake social media accounts.

Tip 1: Keep your eyes peeled for scammers

Fraudsters know most people will be at home at the moment, so be wary of those offering help; common scams include pretending to be your employer, the government, energy companies, broadband providers, banks and even the NHS.

For more Top Tips on Tech visit: BT.com/Tech-Tips

BT BEYOND LIMITS

Tip 2: How to avoid getting scammed

There are plenty of ways to avoid email scams. Here are our top watch-outs:

- Beware of **RE: URGENT** subjects, these aim to get you to react without thinking.
- Always check to see if the spelling and format of a sender's email address looks legitimate; bad spelling and grammar through the email is also a red flag.
- If the email address changes when you hover your mouse over it (this is known as spoofing), don't trust it and delete the email.
- If there are attachments in an email you are uncertain about, don't click on them.
- Make sure that any phone numbers mentioned in the email match those on the company's website before calling.
- Remember you can hover over any links before you click through to see if they look genuine. If you do click through and get redirected to another website, chances are it's a scam. Watch out for clever fake or similar designs.

For more Top Tips on Tech visit: BT.com/Tech-Tips

BT BEYOND LIMITS

Tip 3: Never post personal information:

It's obvious but really important, never post personal information like your date of birth, addresses or your phone number publicly on social media. Anyone can lift this straight from the site and use it to try to scam you. The same is true if you don't ecognise or trust a website, email or text.

Tip 4: Staying up-to-date

Phishing can happen at any time so always think before you click. Use anti-virus software where you can and always be wary of those little pop-up ads when you're surfing the internet. You can stay up-to-date through useful sites like Met Police, Citizens Advice Bureau, Action Fraud, and National Cyber Security Centre. For the Government's latest updates please go to www.gov.uk

- Met Police
- Citizens Advice Bureau
- Action Fraud
- National Cyber Security Centre

For more Top Tips on Tech visit: BT.com/Tech-Tips

BT BEYOND LIMITS

Tip 5: Better safe than sorry

If any emails look suspicious you can forward them to report@phishing.gov.uk, a new service run by the National Cyber Security Centre (NCSC) Suspicious Email Reporting Service.

The NCSC's automated programme will immediately test the validity of the site and if found to be phishing scams, they will be removed immediately.

If you have family or friends who need help identifying scams online please share this PDF with them.

For more Top Tips on Tech visit: BT.com/Tech-Tips

BT BEYOND LIMITS