Staying safe from email scams

Fraudsters are constantly coming up with new ways of trying to defraud people in relation to all manner of products and services, including loans, dating, holidays, business opportunities, clairvoyants, pharmaceuticals, lottery prizes, fake COVID vaccines, even recovery of money lost to fraud and a whole lot more.

Here we look into some of the different types of email frauds that are currently quite common and what to look out for to indicate that an email may not be genuine.

COMMON TYPES OF EMAIL SCAMS

- **419 Emails:** You are offered a share in a large sum of money in return for helping to transfer it out of the country. Once you have given the criminals your bank account details, they empty your accounts.
- **Phishing:** An email that purports to be from companies such as banks designed to trick you into revealing your personal information and passwords. REMEMBER: your bank will NEVER contact you out of the blue to ask for your PIN, full password or to move money to another account.
- **Pharming:** Pharming is a term used when you are directed from a link in an email to a website that spoofs a legitimate website in order to access your personal details.
- **Impersonation of UK official websites:** For example HMRC, with an email message claiming you are due a refund and requesting your bank account details or directing you to a website link.
- **Impersonation of UK officials:** Criminals impersonate a UK official to obtain personal information and steal money, often claiming that you are due a refund or must make an urgent payment. Examples of this scam include TV License, the HMRC Tax Rebate and the Council Tax Scam.
- **Investment scams and pension scams:** Emailed offers of worthless, overpriced or non-existent shares, or a time-limited opportunity to convert some or all of your pension pot into cash. Click here to find out more about these.

HOW TO SPOT A SCAM EMAIL

- The sender's email address looks suspicious. Roll your mouse pointer over the sender's name to check it. If it **doesn't match** the website address of the organisation it says it's from it could be a sign of a scam.
- The email **doesn't use your name** – it says something like 'Dear customer' instead.
- There's a **sense of urgency,** asking you to act immediately.
- There's a prominent website link that may look at first glance like the proper address but has **one letter missing or is spelt wrong.**
- There's a **request for personal information**.
- **Poor grammar and spelling mistakes**.
- The **entire text of the email is contained within an image** rather than the usual text format, and the image contains an embedded hyperlink to a bogus site. Again, roll your mouse pointer over the link to reveal its true destination. **But don't click it!**

Staying safe from email scams

It is almost impossible to keep up with the variety of fraudulent emails that are increasingly appearing on our computer screens and smartphones. However, by taking your time and following the simple steps below you can better protect yourself from falling victim to attempted email fraud.

TOP TIPS

REMEMBER: IF SOMETHING SEEMS TOO GOOD TO BE TRUE, IT USUALLY IS!

1. Create a **separate password** for your email accounts

2. Make sure you have **strong passwords with 3 random words** and change these regularly. Find out more about **strong passwords here.**

3. Install **two-factor authentication (2FA)** for your email accounts. This is an additional process to secure your account.

Further actions you can take to keep safe

Look after your **mobile devices**. Don't leave them unattended in public places, and protect them with a PIN or passcode.

Ensure you always have **internet security software** loaded on computers and update to new versions immediately.

Don't assume that **Wi-Fi hotspots** in places like cafes and hotels are secure. Never use them when you're doing anything confidential online, like banking. Use 3G or 4G.

Never reveal too much personal or financial information (such as in emails, on social networking and dating sites). You never know who might see it or use it.

Always consider that online or on the phone, people **aren't always who they claim to be**. Fake emails and phone calls are a favourite way for fraudsters to approach their victims.

Don't click on links or open attachments **if the source isn't 100% known and trustworthy**, or it seems strange that you'd be receiving them.

Always access internet banking sites **by typing the bank's address** into your web browser.

Never pay for anything by direct bank transfer unless it's to someone **you know personally and is reputable**.

Never respond to emails, texts, letters or social media **that look suspicious,** including messages with **bad spelling or grammar.**

Be cautious when going to a website from a link in an email and then enter personal details – **the email could be fraudulent.**

If someone you've never met in person asks you for money, that should be a **red flag**. Tell them you're not interested and stop all contact.

When shopping online always sign up to American Express SafeKey, Verified by Visa and MasterCard SecureCode so look for the padlock or unbroken key symbol when you first visit a site. Where possible **make your purchase with a credit card** or via a credible online payment system (such as PayPal) which protects you in the event of fraud.

If you are at all suspicious, heed your instincts!
You are most probably right to be concerned.
Report all emails that you believe to be fraudulent to report@phishing.gov.uk.