How can I spot online fraud?

The internet has made life considerably easier for criminals to commit fraud. This is because of the growing number of people using it, and the fact that we tend to feel more relaxed and trusting online. Cybercriminals, however, never rest and are always looking for an opportunity.

Do you click on links in unexpected emails, posts or texts or open email attachments from sources you don't know? Do you reveal your confidential details to a total stranger who calls, claiming to be from your bank, your credit card company or the police? These may be attempts by cybercriminals to get your online details.

GET SAFE ONLINE

Everything you do online carries some level of risk, but there are a number of tell-tale signs that, if present, should make you stop and think before it's too late.

1. **Approaches** - even if they are from people you know but seem unusual, such as requesting confidential information or telling you something is urgent.
2. **Unexpected attachments** - in emails or links in emails, messages, texts or posts.
3. **Requests for money** from someone you got to know online.
4. **Requests for upfront payments** for certain services or goods, especially via direct bank transfer.
5. **Unsecured payment pages** Secure payment pages should have a website address beginning with 'https://' (the 's' stands for 'secure', and have a locked padlock icon in the address bar. But remember that even a secure site can be owned by criminals, so make sure you type the web address in carefully.
6. **Requests claiming to be from organisations** or individuals who you make regular payments to, asking you to change your payment details.

How can I recognise telephone fraud?

Telephone fraud – known as 'vishing' – is becoming very common and the criminals who carry it out are getting more persuasive and sneakier every day. The fraud may start by receiving a phone call from someone who claims to be from a trusted organisation such as your bank, a government department or a tech company. They then skilfully manipulate you into a position where you can be defrauded.

Fraudsters can achieve this by persuading you that they are authentic and are calling to help you solve an urgent problem or make you an offer you can't refuse. They make themselves appear real by using technology which spoofs real phone numbers and may even hold the phone line open at the end of a call.

If they ask you to call them back, use a phone number from your bank statement or another official document. If you can, use a different phone from the one you received the call on. If this isn't possible, hang up for at least five minutes before you dial out, or call a friend whose voice you recognise before making that call. If the original call is from a fraudster, this should end their phone connection with you and enable you to call trusted numbers to check if the original call was genuine.

Funded by COMMONWEALTH UNITED KINGDOM CHAIR-IN-OFFICE