Staying Safe Online

Email Scams

Phishing emails are a common type of email fraud, where scammers will send emails pretending to be from a trusted organisation. This is to trick you into clicking through to a fake website where you're prompted to enter your personal details.

Scam emails can look genuine and appear to be from official places, like HMRC or a bank, but you can often tell it's a scam.

Look out for:

- errors in spelling or grammar, or an unusual style of writing
- requests for personal information, such as your username, full password or bank details – genuine organisations will never ask this
- threats that unless you act now, a deal will expire or your account will be closed.

If you see a suspicious email, don't reply with your details or open any links or documents. Delete the email straight away.

Fake Websites

Scammers create fake websites which look official and persuade you to provide personal or financial information. For example, a scammer might create a fake website for the bank you use, and ask you to update your account or security information on it. Often, these websites can look very convincing and only a few details might be different.

There are also websites set up to look like a copy of a service offered by government websites. For example, websites that offer to help you apply for a passport renewal or a new driving licence. Although they aren't illegal, these websites charge extra money if you use them, rather than going directly through the official government department where the service is free.

Visit your bank's website by typing their official web address in your internet browser – you can find this on letters from the bank. If you aren't sure about which website to use for a government service, go through GOV.UK, the government's official website, to find what you need.

What should I do if I think I've been a victim an online scam?

Scammers are constantly finding new ways to trick people and online scams are changing all the time. Lots of people get scammed – it's not unusual and you shouldn't be embarrassed. The best thing you can do is report it and talk about your experience. It may even help other people avoid getting scammed in the future.
If you've been scammed, report it to Action Fraud. You can either:

- report the scam online on the Action Fraud website
- call Action Fraud on 0300 123 2040 (lines are open Monday to Friday, 8am-8pm).

You might be worried about installing anything on your device or computer. If you're unsure, check the source, reviews and check with someone you trust.