BTPS

Staying safe online

Getting online can make life easier in lots of ways, but it also comes with the risk of fraud. Online scams are becoming increasingly common, but by knowing what to look out for, you can protect yourself and stay safe online.

Here are some common online scams to be aware of:

Scam emails (junk emails)

Emails designed to trick someone into entering their personal or financial details, often telling you you've won money or a prize, or directing you to a fake website. Some emails may encourage you to click a link or open an attached file, but doing so may harm your device. Scam emails can look genuine, but telltale signs are:

- **Spelling or grammatical errors.**
- **Requests for your username, password or bank details – genuine organisations will never ask for this.**
- **Threats that your account will be closed unless you take immediate action.**

If you see a suspicious email, delete it straight away. Don't reply with your details or open any links or documents. If the email claims to be from an organisation, phone them directly using the phone number on their official website and ask them if they sent the email. To report a scam email, go to the Action Fraud website: **www.actionfraud.police.uk/report-phishing**

Fake websites

These official-looking websites may ask you to provide personal or financial information. For example, a fake council or government website inviting people to apply for a 'replacement winter fuel allowance' if they enter their bank details and other personal information. Often, they will look very similar to the legitimate website.

To be safe, do not click links that encourage you to log on to a website within an email. If you think it's genuine, verify the organisation's website independently, from any correspondence you've had from the company. Then check the website has the prefix **https://** and a locked padlock image in the address bar, as these are good indicators of a legitimate website. For any government website, it starts with **https://www.gov.uk**

Viruses

These are untrustworthy programmes that spread from one computer, tablet or smart phone to another. They might arrive in a spam email as an attachment, infecting your device when you click on it. Criminals might then use this to take control of your computer. A virus might also scan your computer for personal information, slow your computer down, send out spam email to your saved contacts, or delete files.

Anti-virus software is easy to install. New computers often come with industry recognised anti-virus software that is updated regularly. Find more guidance on anti-virus software on the National Cyber Security Centre website at **www.ncsc.gov.uk/antivirus**

Use anti-virus and anti-spyware sortware to protect your computer from viruses.

Top tips to protect your device

You wouldn't leave your front door open, so why leave your devices unprotected? As well as being alert to online scams, there are simple steps you can take to protect your device:

Create strong and separate passwords

Avoid passwords made up of common words, numbers or keyboard patterns (such as 'password' or '123456'). Don't use personal information, such as your name, date of birth or any family members' details. Use three random words to create a password that's difficult to crack, use different passwords for different accounts and don't write them down or store them anywhere visible.

Back up your data

Safeguard your most important data, such as your photos and key documents, by backing them up to an external hard drive or a cloud-based storage system.

Install security software on your devices

Anti-virus software will look for and remove viruses before they can infect your computer. Anti-spyware software prevents unwanted adverts from popping up and stops programmes tracking your activities or scanning your computer, tablet or mobile phone for private data, such as credit card numbers or bank details.

Always check for telltale signs of a scam email, which are:

1. Spelling or grammatical errors.
2. Requests for your username, full password or bank details – genuine organisations will never ask for this.
3. Threats that your account will be closed unless you take immediate action.

If you have any concerns, call the company using the phone number on their official website to check if an email is from them.

Know how to check if a website is legitimate

Check a website has the prefix **https://** and a locked padlock image in the address bar.

1. Cross check the website link with any official correspondence you've had from the company – keep an eye out for small differences in spelling.
2. To be safe, do not click on links that encourage you to log in to a website within an email.

Install the latest updates

Software and app updates contain vital security updates to help protect your devices from cyber criminals. Turn on 'automatic updates' in your device's settings if it's available, to ensure updates are applied promptly.

Protect your wireless network

You need to protect your wireless network (also known as Wi-Fi) so that people living nearby can't access it. Read the instructions that come with your wireless router to find out how to set up a 'key' (a type of password) so that no one else can access the internet through your router.

Stop, think, check

If you are worried, unsure or feeling pressured, do not respond. Stop, think and check. Organisations that are genuine, will understand and will never press for a quick response or action.

Find out more

Visit the National Cyber Security Centre (NCSC) website for more recommendations at **www.ncsc.gov.uk/cyberaware**