How to stay safe online

We have pulled together some information from public advisory websites on how to keep yourself and your equipment secure while working online.

1. Use strong and unique passwords

When you create a password for an account, try to include a mix of numbers, symbols, and letters, using both uppercase and lowercase. A strong password is regarded as being at least 12 characters long.

- Try abbreviating a phrase. For example, "Coffee at dinner keeps you up at night" could become **'C@dKuU@n2!?$'** or combine 3 random words like **'BicycleFishRainbow2!'**
- Turn on 2-step verification, also known as two-factor authentication, where available. Using two-factor authentication stops hackers from accessing your accounts even if they know your password
- Keep your accounts secure by making sure your important accounts such as email, social media, banking and shopping accounts are each protected by a different **strong password** that you do not use anywhere else. That way, if fraudsters become aware of one password, they will not have access to all your other accounts.

2. Report suspicious emails, calls or texts

If you have received a suspicious email, forward it to the Suspicious Email Reporting Services (SERS) at **report@phishing.gov.uk.**

If you are telephoned out of the blue by someone you don't know and asked for personal details:

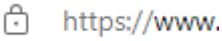
- do not give any details
- hang up
- contact Police Scotland or Action Fraud (England, Wales and Northern Ireland) to establish whether the call was legitimate.

If you receive a suspicious text message, forward it to **7726**. Your mobile network provider can investigate and act if it's found to be a scam.

3. Shop securely online

Here are some steps to follow to help keep your accounts secure:

- Choose carefully where to shop and read feedback from people or organisations that you trust, such as consumer websites
- Some emails and/or texts you receive may contain information on amazing offers but these emails may contain links to fake websites. If you are unsure, do not use the link. Do a search for the site instead using a web search engine such as Google and follow the results
- Only provide enough details to complete your purchase, which means filling in only the required details when completing a purchase. These are often marked with an asterisk (*) and typically include your delivery address and payment details
- If prompted, do not let the website store your payment details for a quicker check out next time

- Use a credit card for online payments. Most credit card providers protect online purchases and must refund you in certain circumstances. Using a credit card (rather than a debit card) also means that if your payment details are stolen, your main bank account won't be directly affected
- When paying for your items, check there is a closed padlock icon in the browser address bar which will look like this: 

If you think your credit or debit card has been used by someone else, let your bank know straight away so they can block anyone using it. Always contact your bank using the official website or phone number found on the back of your card.

If you've lost money, tell your bank, and report it as a crime to **Police Scotland (0141 308 1070)** or **Action Fraud (0300 123 2040 for England, Wales and Northern Ireland).**

If you don't receive the item (or it doesn't match the description given), Citizens Advice (0800 144 8848) has some useful information about getting your money back if you paid by credit card, debit card or PayPal.

Email security

Don't open emails or files from people you don't know. Phishing scammers are people who use fake emails or messages to make you share personal information.

If you see an email from an unfamiliar address, or from an address you know but with a suspicious message, or a message in a style that is unusual for that contact, move it to your spam folder or delete it.

- The email could also include links that might look legitimate, but never click on them until you have verified that it's a legitimate message. Hovering the mouse over the link to view the link address can help to check if the website is legitimate
- **Beware of urgent subject lines.** Scammers will often invoke a sense of urgency to get you to open the email, click on links or open attachments. Common phishing emails may include subject lines like 'Your account has been suspended' or 'Unauthorised login attempt'
- **Never provide login credentials** (i.e., your username or password). Legitimate people and organisations will never ask you to provide your username or password
- Phishing scammers are often looking to obtain your bank account details. Be extra cautious if you receive an email requesting money, login credentials or very personal information. If you suspect you have been scammed Citizens Advice has lots of useful advice to help (see the 'Resources' section below).

Ransomware

Ransomware is malicious software that prevents you from accessing your computer (or data that is stored on your computer). If your computer is infected with ransomware, the computer itself may become locked, or the data on it might be stolen, deleted or encrypted.

Normally you are asked to make a payment (the ransom), to 'unlock' your computer or to access your data.

However, even if you pay the ransom, there is no guarantee that you will get access to your computer or your files and you may be targeted again. This is one of the reasons why it's important to always have a recent backup of your most important files and data.

Below are some ways to protect yourself from ransomware.

1. Keep your computer's software up to date

Most software updates come with security upgrades, so it's important to always have the latest version installed. To easily download updates as soon as they are released, turn on automatic updates in your computer's Settings.

- Ensure that your computer is running up to date anti-malware software. Microsoft's Windows and Apple's MacOS have built in malware protection tools which are suitable for this purpose
- Check that your computer firewall is on as this creates a barrier between your computer and the internet. To do this on your device, follow these steps:
    - On a Windows device, click on start and type 'firewall'. Click on "Windows Defender Firewall" to check firewall status; or
    - On your Mac, choose Apple menu and open "System Settings". Click "Network" in the sidebar and then click "Firewall".

2. Secure your devices

Smartphones and tablets which are used outside the home need even more protection than desktop equipment such as personal computers. Below are some ways to secure your devices:

- Where possible switch on PIN, password protection or fingerprint recognition for mobile devices
- Keep devices and all installed applications (apps) up to date by using the 'automatically update' option if available
- Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

3. Backup your data

A backup is a copy of your important data that's stored in a separate safe location, usually on the internet (known as cloud storage), or on removable media (such as USB stick, SD card, or external hard drive). Once you've made a backup, if you lose access to your original data, you can restore a copy of it from the backup.

Most backup solutions allow you to choose what data is backed up, for example, documents, photos and other files, or the contents of your phone or computer (including the apps and programs you use).

You should back up anything that you value. That is, anything that would inconvenience you (for whatever reason) if you could no longer access it. Backups are not just for recovering lost, erased or inaccessible data. If you have a new device or computer, you can use backups to transfer across your existing files, apps and settings. If you have a recent backup of your most important files, then you can't be blackmailed.

Below is some guidance on the best ways to backup your data:

- Make regular backups of your most important files such as photos and documents. Check that you know how to restore the files from the backup. If you're unsure how to do this, you can search online
- Make sure the device containing your backup, such as an external hard drive or USB stick, is not permanently connected to your computer
- Where possible turn on auto backup so that data on your smartphone is automatically copied to the cloud. This will allow for quick recovery of your data by signing back into your account from another device
- Many cloud storage solutions provide an amount of storage space for free. This may be enough to store all your important documents
- Remember to protect your cloud accounts and access to your backups by using strong passwords and when possible, turning on two factor authentication (if available).

Protecting your identity

Fraudsters can commit **identity theft** by stealing your personal information by going through your post or rubbish, hacking into your online accounts, finding public details on your social media or by purchasing it from criminals to then commit **identity fraud.** Identity fraud can involve applying for credit or new bank accounts in your name or buying products or services.

Below are some steps you can take to prevent criminals from committing identity theft or fraud.

1. Dispose of papers safely

Action Fraud advise safe destruction of any papers containing personal information, for example by shredding. These are any documents which contain your:

- name
- address
- credit card details or
- bank account details.

2. Check regularly if your personal details have been compromised

If a company which stores your personal details has suffered a data breach, your email address, phone number and/or password may have been exposed to hackers. Hackers may take this data and sell it on a dark market website enabling any other accounts which share the same passwords to also be hacked.

It is important not to ignore any bills, invoices or receipts for services or items you don't remember purchasing or from institutions you don't normally deal with. These documents may have been sent to you because your identity has been stolen so you should contact Action Fraud to ascertain whether identity theft has occurred.

You can check whether your email address has been involved in a data breach using the website **haveibeenpwned.com** and take appropriate action to secure your accounts by changing your passwords for the affected company's account, as well as the compromised email address.

To check whether criminals have stolen your identity and used it to apply for credit in your name, you can sign up to free credit reports for the UK's three major credit agencies **Experian**, **ClearScore** (Equifax) or **Credit Karma** (TransUnion) and check regularly (usually monthly) if there has been any unusual activity in your credit file or bank accounts.

3. Understand your digital footprint

The National Cyber Security Centre suggests exercising caution when using social media as criminals can use publicly available information to steal your identity.

Consider the data you share through social media sites such as Facebook and remind yourself of the information that can be viewed publicly. It is recommended that this is kept to a minimum. In addition, you should review the information you share with your followers and friends and limit to see what is unnecessary and might be used to make phishing messages more convincing (see the 'Email Safety' section above).

Resources

We sourced this information from the following public advisory organisations. They regularly update their websites and we provide links to them below.