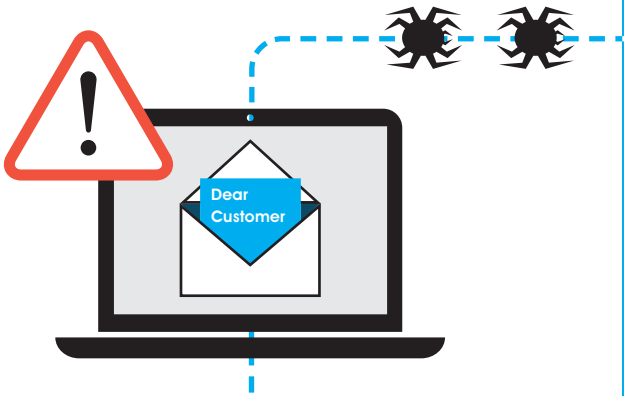


Beware of phishing

Many attempts to defraud start with a 'phishing' email, text or phone call that attempts to convince you to hand over personal details or visit a website being used as part of the scam. Often these will include one or more of the following elements:

Urgency – they may say they will close accounts, halt payments or stop subscriptions if you don't reply.

Authority – stating that they are from an organisation such as the police, HMRC or other government agencies to make you worry about what will happen if you don't comply.

Reward – for instance by suggesting that you will receive a payment, vouchers, rebate, or some kind of prize.

Bullying – occasionally fraudsters will simply adopt a bullying tactic in the hope that victims will comply.

Other signs that a message may be from a fraudster include:

- They don't know your name. You may be referred to as a valued client, dear customer or similar.
- Spelling or grammar in texts or emails may be poor.
- Logos and graphics in emails may be of poor quality.
- Emails containing links to websites or attachments.

It is very difficult to spot a really well-crafted phishing attempt so the best defence is to ask if you are expecting the message or if the supposed sender of the message usually communicates with you in such a way. If you have any reason to be suspicious, it's always safer to call or email using the number or address from an organisation's website, as contact details in an email or text may not be genuine.

Shop safely online

Buying online gives consumers a huge amount of choice and convenience, but it can be much more difficult to have the same degree of confidence in an online supplier than when we walk into a familiar high street store.

Do some research before using an unfamiliar retailer for the first time. Do they have a physical address and phone number, do they have social media pages with reviews from users that appear like real people, can you google if they are a scam site?

Check the web address starts with 'https://' when providing personal details. The 's' stands for 'secure' and shows that communications with the website are encrypted.

Double check the website address in the browser address bar. Criminals can register fake sites based on spelling mistakes or names that look very similar to the legitimate company.

Use a credit card if possible. Most providers carry some protection for purchases in the event of a scam sale. Many banks now provide 'virtual card' functionality that allow you to transact on your main credit card account without revealing your main credit card account number.

Check banking and credit card statements. Make sure that there are no suspicious or extra transactions.

Be cautious if the site asks for an unreasonable amount of information to make a purchase. Whilst it is expected that an address and bank details are needed you wouldn't expect to have to provide much more. This may be an attempt to harvest personal details.

Be on guard for emails and texts about amazing offers or links to discount codes. Check Google to see if a scam has been reported and navigate to any websites yourself rather than click on links.

J152249_05/2021

Avon and Somerset Police

STAYING SAFE ONLINE

We can all be targets of cyber crime. This leaflet can help keep you and your family safe online.

Protect your digital devices

Making sure your digital devices are well protected is a vital part of your online security. If attackers can gain access to your devices by connecting to them through the internet or by installing malicious software on them, then you can be at risk of losing your online credentials, files, banking info and much more. Following these simple security steps can help protect you from attacks.

Install updates. Software vendors work hard to make sure they spot and fix any vulnerabilities before the criminals can get at them. To keep yourself protected make sure you install any updates when they're available. The longer you leave your device before updating, the longer you could be exposed to attacks and viruses.

Make sure your firewall is turned on. The minute you connect to the internet you're potentially exposing your device to machines from all over the world. A firewall is your protection against unwanted connections. Make sure you check it is enabled.

Use an anti-virus product. An uninstalled update, a visit to an unsafe website, or opening a dangerous attachment in an email can all leave you exposed to malicious software. In these instances you need help spotting the dangers and protecting your data. This is the job of anti-virus software, so make sure you have a product keeping you safe.

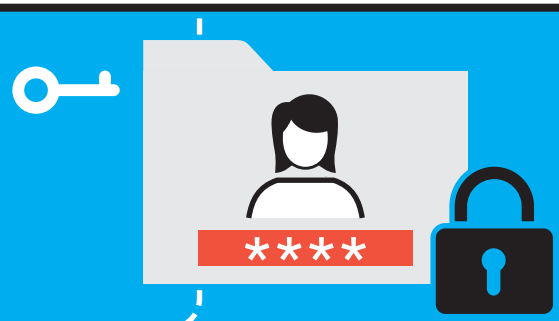
Keep your accounts and online credentials safe

Our online identity is an essential part of our digital interactions and losing control of it can mean being locked out of services we rely on or having identities exploited to commit fraud. Below are some steps you can take to keep your identity and accounts protected.

Use a strong password. Passwords are the most common way to prove an online identity and attackers love nothing better than a weak one. Any password based on football teams, pet's names, birthdays and the like are easy to crack. The National Cyber Security Centre recommends using three random words as a password eg magicduckwindmill. Combining 'three random words' with special characters, misspelt words and adding numbers creates a more complex password making it difficult to crack eg magik£du5ckWinmill.

Don't reuse passwords. Many companies have suffered data breaches over recent years and millions of passwords have been leaked. Armed with this password an attacker may try to access all our online accounts, from Amazon and PayPal, to email and social media. By making sure we have different passwords for different accounts we can limit the damage. Using a Password Manager can help by remembering or generating lots of complex passwords as well as keeping track of all our online registrations.

Use two-factor authentication. One of the most effective ways of proving who you are online is to demonstrate that you are in possession of a unique object that belongs to you. This 'second factor' is generally a mobile phone to which a pin code is sent when a login attempt is made from a device not already associated with you. Most of the popular email providers, payment apps and social media platforms allow you to set up two-factor authentication.



Limit your digital footprint

There are lots of ways attackers may use your personal information against you. They could set up accounts in your name to use to commit fraud, craft convincing scams based on your interests, spoof your credentials to scam your friends or colleagues, or even use what you post to engage in cyber stalking and harassment.

Think about how much of your online presence is publicly available. Social media platforms don't always make it easy to discover who can see what but it is worth spending some time reviewing your privacy settings and asking yourself if you're sharing too much.

Avoid posting information online that you wouldn't share with a stranger. This could include details such as your employer, birthdays, addresses, phone numbers and emails.

Make sure your privacy settings restrict who can see the posts you'd rather keep private. Keep up to date with privacy settings as social media platforms may change the way that they're applied.

Anything you post online can end up being circulated on the internet at any time in the future. If you believe a post could in any way cause you embarrassment in the future then it's probably best to keep it to yourself.

Avoid posting in the heat of the moment. Posts which are offensive or harassing could constitute a crime or could result in unwelcome responses. In some cases people end up having to delete social media accounts or change contact details once the internet collectively goes into overdrive to hound the original poster.