Cumbria Fire & Rescue Service

Information Security Month October 2025

Newsletter 1 | Information Security and You

Welcome to the first of five newsletters which will be shared with you during October to mark Information Security Month.

Information Security Month is an international initiative aimed at raising awareness about cyber security threats and educating individuals and organisations on how to protect themselves.

The theme of this week's newsletter is Cyber/Information Security and You: Keeping you and your family safe online. In this newsletter you'll learn:

- Helpful tips for securing your online accounts
- Top tips for using social media safely
- A "Did you know?" case study on LinkedIn's Artificial Intelligence content grab
- Guidance for high-risk individuals
- Advice on how to protect your devices.

Securing Online Accounts

You wouldn't leave your front door open, so why leave your online accounts unprotected?

Here are some easy tips for securing your online accounts for email, banking and shopping.

****	Use strong and non-repetitive passwords, a combination of three random words, numbers and special characters
	Use separate passwords for every online account
	Use multi-factor authorisation where available to add an extra layer of security
	Review activity for online accounts, such as login information on multiple devices
	Remember to log out of each application after use
	Turn on alerts for suspicious logins
	Review personal details periodically to ensure your details are up to date

Social Media: How to use it safely

Use privacy settings across social media platforms to manage your digital footprint.

Social media is a great way to stay in touch with family, friends and keep up to date on the latest news. However, it's important to know how to manage the security and privacy settings on your accounts, so that your personal information remains inaccessible to anyone but you.

Advice from social media platforms

The following guidance is provided by each of the major social media platforms. Click to read detailed information:

Facebook
Basic privacy settings and tools

X (formerly Twitter)
How to protect and unprotect your Tweets

YouTube
Privacy and safety

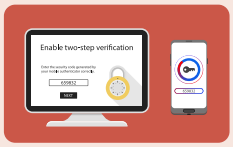
Instagram
Privacy settings and information

LinkedIn
Account and privacy settings overview

Snapchat
Privacy settings

Tiktok
Privacy and security settings

Use 2-step verification (2SV) to protect your accounts



2-step verification (often shortened to 2SV and sometimes called two-factor authentication) provides a way of 'double checking' that you really are the person you are claiming to be when you're using online services, such as social media, banking or email. Even if a criminal (or someone simply looking to cause mischief) knows your password, they won't be able to access any of your accounts without also providing the second form of verification. This may be a code texted to your phone or email account or biometrics for example.

- The **Cyber Aware website** contains links on how to set up 2SV across popular online services such as **Instagram, Snapchat, X** and **Facebook**.
- For more information on why you should use 2SV wherever you can, read the **NCSC's official guidance on 2-step verification**.

Understanding your digital footprint

It's worth exercising some caution when using social media. Not everyone using social media is necessarily who they say they are. Take a moment to check if you **know** the person, and if the friend/link/follow is genuine.

Less obviously, you should think about your digital footprint, a term that describes the information about you that is available online. Criminals can use this to steal your identity, or make phishing messages more convincing. You should:

- Think about **what** you're posting, and **who** has access to it. Have you configured the privacy options so that it's only accessible to the people you want to see it?
- Consider what your followers and friends **need** to know, and what detail is unnecessary (but could be useful for criminals)
- Have an idea about what your friends, colleagues or other contacts say about **you** online.

Although aimed at businesses, **NPSA's Digital Footprint Campaign**, contains a range of useful materials (including posters and booklets) to help understand the impact of your digital footprint.

Spotting and reporting fake accounts

Scammers will make fake accounts and/or hack real accounts to use them to commit a range of fraudulent activities. Many sites have a process to verify accounts, such as verified badges for Instagram and Facebook. This can help to identify real accounts against fake accounts pretending to be a well-known person. Other things to look out for include:

- Where an account has a date indicating when it was set up
- Nonsensical names (appears to be random letters and numbers)
- The number of followers (although note that followers can be bought).

It is not just celebrities' accounts that are targeted by scammers. If a family member or friend posts something that appears suspicious or out of character, contact them by another method (in case their account has been hacked). If it transpires their account has been taken over, they should follow the NCSC's **guidance on recovering hacked accounts**.

You can also report fake posts or accounts directly with the provider.

- **Report a fake Facebook profile or page**
- **Report a post or profile on Instagram**
- **Report impersonation accounts on X**
- **Report someone on TikTok**
- **Report fake LinkedIn profiles**
- **Report a Safety Concern on Snapchat**
- **Reporting YouTube videos and channels.**

Social media and children

Most social media accounts require users to be at least 13 years old. However, it is easy to sign-up with a false date of birth. For expert advice about how to keep children safe online, please refer to:

- **Thinkuknow: National Crime Agency - education programme for children**
- **Internetmatters.org - Social Media Tips**
- **NSPCC - keep your child safe on social networks.**

CASE STUDY

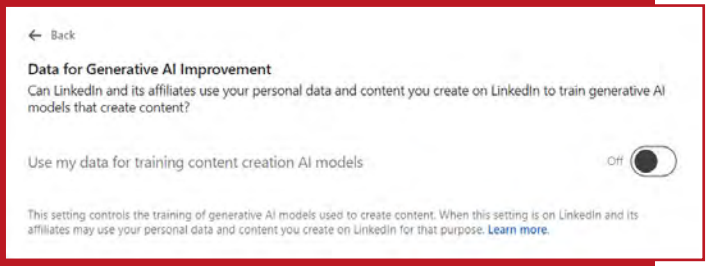
Did you know?

LinkedIn has quietly slipped into its terms and conditions a new usage for your data to be trained on their Artificial Intelligence (AI), including sharing it with some of their models that are provided by Microsoft's Azure OpenAI service.

Essentially, this means that LinkedIn and its affiliates can now use your personal data and the content you create on LinkedIn to train generative AI models to create content.

More information can be found here **linkedin.com/help/linkedin/answer/a5538339**.

To opt out, go to **linkedin.com/mypreferences/d/settings/data-for-ai-improvement** and opt out, as in the image below.



To manage, restrict or delete your LinkedIn data go to **linkedin.com/mypreferences/d/categories/privacy**.

Are you a High Risk Individual?

In a cyber-security context, you are considered a high-risk individual if your work or public status means you have access to, or influence over, sensitive information that could be of interest to nation state actors.

High-risk individuals include those working in political life (including elected representatives, candidates, activists and staffers), academia, journalism and the legal sector.

In recent years there have been a number of targeted cyber-attacks against high-risk individuals in the UK, to attempt to gain access to their accounts and devices. This has resulted in the theft and publication of sensitive information, which can also cause reputational damage.

How and why you may be targeted

There are different ways an attacker may gain access to your accounts or devices. Common attack methods include **spear-phishing** and **social engineering** to compromise victims' accounts and devices.

A **joint NCSC advisory** with international partners describes spear-phishing in more detail and details how an actor attributed to the Russian state has used it to target high-risk individuals. Another **advisory** describes how cyber attackers working on behalf of the Iranian state have used the same methods.

The NCSC has **also assessed** that Chinese state-affiliated organisations and individuals were responsible for online reconnaissance activity in 2021 against the email accounts of UK parliamentarians.

Using this guidance

This guidance will help you improve the security of personal accounts and devices, and keep you better protected online.

Personal accounts and devices are the responsibility of the individual and may be considered an easy target for threat actors, as they may perceive them to have fewer security measures in place.

You should continue to use corporately managed accounts and devices for your work, as they will be centrally managed and secured.

Protecting your accounts

Your personal accounts are a likely target for attackers. If an attacker gains access to one of your accounts, they may be able to gain access to the information on them. Taking the actions below will significantly reduce the chance of a successful attack.

1. Use strong passwords
2. Enable 2SV on your accounts
3. Review your social media use and settings
4. Review your use of messaging apps such as WhatsApp, Messenger and Signal

Protecting your devices

As with your accounts, attackers may also try to compromise your devices – computers, phones or tablets – to achieve their aims. If they manage to access them, they can steal sensitive or personal information, carry out monitoring, or even impersonate you.

There are several things you can do to secure your devices.

1. Install updates
2. Use 'Lockdown Mode'
3. Replace old devices
4. Protect physical access
5. Know how to erase data from devices

What to do if you think you've been attacked

If you receive a suspicious email, do not click on any links, or reply to the email. Avoid entering any credentials if prompted, even if the sender is genuine. You should report it to IT support, who will be able to offer advice, even if it has been sent to a personal account.

The **NCSC has guidance on how to spot and deal with phishing emails**.

If you have clicked on a link, or think you've been hacked, don't panic, even if you think you have made a mistake. If something goes wrong on a device or account that your organisation has provided, report it to IT support. The security team won't blame you for reporting that something has happened to you, as it helps them fix things, and **try to stop it happening again**, to you or anyone else.

Send us your comments and feedback

Share your comments and feedback with us, including any suggestions for how information security could be improved, or an example of good Information Security practice from a colleague, or team.

The best examples will be included in our fifth and final newsletter at the end of the month.

Send your comments, suggestions and examples of good Information Security practice in an email with the subject line **"Information Security Month Feedback"** no later than Friday 24 October to **security@cumbriafire.gov.uk** and remember to include your full name and contact details.

Thanks for reading this far! The theme of next week's newsletter will be Data Protection and how to 'Be Data Smart!'

In the meantime, if you have any questions, please send them to: **security@cumbriafire.gov.uk**.

#StrongPasswords #CyberAware #BrowseSafe #ThinkCyber #MindfulClicks #OwnYourSecurity