GUIDANCE

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.

This page:

- collects advice provided by the major social media platforms on how to set up privacy controls
- suggests some tips on how to use social media safely

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
- **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 that are protected using 2SV.

- The Cyber Aware website contains links on how to set up 2SV across popular online services such as **Instagram**, **Snapchat**, **Twitter** 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, which is a term used to describe the entirety of information that you post online, including photos and status updates. Criminals can use this publicly available information to steal your identity, or use it to 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, CPNI'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 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 Twitter.
- 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
- **Internet Matters.Org**: Social Media Tips
- **NSPCC**: keep your child safe on social networks

PUBLISHED

24 January 2019

REVIEWED

5 September 2022

VERSION

1.0

WRITTEN FOR

Individuals & families