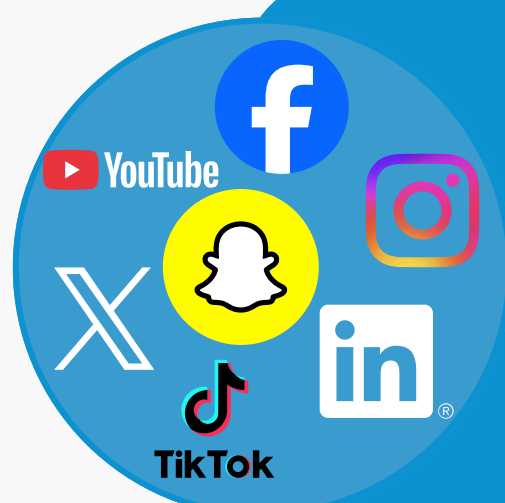


# 5 Tips For securing digital technology



## 1. Secure Social Media- use the links

- Facebook [Basic privacy settings & tools](#)
- X (formerly Twitter) [How to protect your Tweets](#)
- YouTube [Privacy & safety](#)
- Instagram [Privacy settings & information](#)
- LinkedIn [Account privacy settings overview](#)
- Snapchat [Privacy settings](#)
- Tiktok [Privacy & security settings](#)

## 2. Use 2-step Verification (2SV)

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.



## 3. Practice good Password Hygiene

You can either use 3 random words + a number, auto-generated passwords (using your smart phone) or condensed sentences (MfaniSasmgt: My favourite aunt's name is Susan and she makes great trifle).

## 4. Use the 'Digital Breakup Tool'

This interactive tool created by Refuge and Avast is designed to provide awareness and understanding of the various digital platforms a partner might have access to, whether it's social media accounts, online banking, or live location through apps such as Uber and Strava.



## 5. Defend against phishing & social engineering

- Don't open unexpected attachments or click links from unknown senders.
- Verify requests for sensitive info over a second channel (e.g., call the person).
- Be cautious about public Wi-Fi.