National Cyber Security Centre
a part of GCHQ

Cyber security for high-risk individuals

Follow these steps to be significantly safer online and help defend against targeted attacks.

Help if you're targeted

Don't panic if you've clicked on something – report it to your organisation's IT support, even if it happened on a personal device.

Also tell them about suspicious emails or messages you receive, even if you haven't clicked on anything.

How could I be targeted?

Attackers have used spear-phishing – sending targeted emails which direct the recipient to a bad link or website – to compromise high-risk individuals and try to steal information of interest.

Be aware that your personal accounts and devices may also be at risk, as an attacker may consider them 'easier' targets.

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

Protect your accounts

Use strong passwords

- Use three random words to increase complexity – and make passwords unique for each account.
- Particularly for your most important accounts, like email, social media and online banking.
- You can also use a password manager which helps you remember different passwords for different accounts.

Set up two-step verification

- Use an authentication app like Google Authenticator or Microsoft Authenticator.
- 2SV adds another layer of security so that even if an attacker knows your password, they still can't access your account.

What is a high-risk individual?

If the nature of your work means you have access to certain sensitive information, you may be of interest to nation-state actors. This includes people who work in:

- politics (elected representatives, candidates, activists and staffers)
- academia
- journalism
- the legal sector

Protect your devices

Install updates

- If you receive a prompt to update your device or apps, do it – it stops attackers taking advantage of security flaws which they can exploit to get access.
- Enable the auto-update option, so you don't have to remember.
- Only download software and apps from official stores, like Google Play or Apple App Store

Replace old devices

- Old phones and laptops that are no longer supported are more vulnerable to attack as they can't be updated – upgrade your device if support is ending soon.

Use 'Lockdown Mode'

- On Apple devices, 'Lockdown Mode' provides added security for individuals who might be targeted by sophisticated threat actors – enable it.

Protect physical access

- Use a password or pin that must be entered when the device is powered on.
- Enable the track location functions – 'Find My' on an iPhone and 'Find My Device' for Android.

Think about how you use social media

- Be careful about how much personal information you share publicly.
- Review your security settings to decide who can see what.
- Avoid accepting message requests from unknown accounts - consider calling first to verify who they are.