Secured by Design

SBD

Official Police Security Initiative

PDSC
POLICE DIGITAL SECURITY CENTRE

NaCTSO
National Counter Terrorism Security Office

Top 10 Cyber Security Tips for **Working at Home**

1 **Strong password policy** Use a strong password for all devices and social media accounts. Change default passwords on all your devices when initially installed (especially your Wi-Fi router at home or any Internet of Things devices you may have) and consider using password managers to store and protect your passwords.

2 **2FA** Turn on the two-factor authentication setting on all your accounts and devices.

3 **VPN** Use a Virtual Private Network (VPN) to protect and encrypt the data you send or receive. It will also scan devices for malicious software.

4 **Software update** Set all your devices and apps to download and install updates automatically to ensure that any crucial fixes are not missed and the risk of your devices being infected with malware is reduced.

5 **Back up** To safeguard your most important personal data and information, back them up to an external hard drive or cloud-based storage system.

6 **Phishing emails** Cyber criminals are targeting people and businesses with fake emails about the coronavirus. Phishing emails may appear genuine but are embedded with a virus that could compromise your device, as well as manipulate you into sharing personal or financial information.

7 **Install anti-virus** Install and activate anti-virus software on all your devices, preferably set it to update automatically. This will help you to run a complete scan of your system and check for any malware infections.

8 **Safe online browsing** Only visit trusted websites especially when online shopping. Keep an eye out for websites that have a padlock sign in the address bar, as this shows that the connection and your personal information (e.g. credit card information) is encrypted and secure.

9 **Social media** It is important to review the privacy, password and security settings for all your social media accounts to ensure they are as secure as possible.

10 **Communication** Maintain contact with your team, as it is easy to feel isolated or lose focus when working at home.

More information on working from home is available from the National Cyber Security Centre:
https://www.ncsc.gov.uk/guidance/home-working

For more information from the Police Digital Security Centre, visit: www.policedsc.com

New Counter Terrorism ACT App Launched

Despite the current threat from Covid-19, it is still important to remain alert and vigilant to terrorist activity.

Live-time information from Counter Terrorism Policing, plus all the very latest protective security advice, is now available at your fingertips 24/7 – wherever you are.

If you have a phone then you can keep updated where and when it matters most – all through the new easy-to-navigate Action Counters Terrorism (ACT) app.

More than a thousand specialists from across the UK have been helping officers trial this new product, including leading organisations from the security, sporting and retail sectors.

Powered by Urim, the ACT app is free for businesses and has been developed in partnership with industry specialists from Marks and Spencer and Highfield eLearning. Available from Google Play or App Store, the app will provide access to:

■ Practical advice and guidance to help you protect your business, plus information on how to respond in the event of an attack.

■ Information on Counter Terrorism Policing's suite of ACT training products, plus access to the online e-Learning package.

■ Suite of National Counter Terrorism Security Office guidance videos.

■ Latest reference documents and publications.

■ ACT online reporting form and confidential hotline.

■ Emergency response and post-incident guidance.

■ Live-time news updates from UK Protect.

COUNTER TERRORISM POLICING

ACT ACTION COUNTERS TERRORISM

IN THE RARE EVENT OF
a firearms or weapons attack

RUN HIDE TELL