



Police Crime Commissioner Elections

Cyber Security Awareness

The following cyber security advice has been curated to provide awareness, advice, and recommendations to nominated Police Crime Commissioners participating in elections across the UK in May 2024.

In a cyber security context, PCC nominees are considered a high-risk individuals since your proposed work and/or public status means you have potential access to, or influence over, sensitive information that could be of interest to foreign nation state actors.

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.

Cyber Security Advice and Recommendations

Protecting your Accounts

Use **strong passwords** - Use three random words to increase complexity and make passwords unique for each account. Consider using a password manager for effective management.

Use **two-factor authentication** - 2FA adds an additional layer of security so that even if an attacker knows your password, they still can't access your account.

Think about how **social media** is used and what personal information is shared – review privacy settings regularly!

Protecting your Devices

Install updates - If you receive a prompt to update your device or apps, do it – it stops attackers taking advantage of security issues which they can exploit. If your device is old and cannot be updated – upgrade as soon as possible.

Only **download software and apps from official stores**, like Google Play or Apple App Store

Use **Lockdown Mode** (Apple) and enable '**Find my**' devices on both Apple and Android

Reporting Incidents

Don't panic if you've clicked on something – **report it** to either your corporate IT, your local police force, or the NCSC, even if it happened on a personal device.

If you have received an email which you're not quite sure about, forward it to report@phishing.gov.uk

Furthermore, you can report related suspicious activity to the NCSC report.ncsc.gov.uk

Further Advice

Should you require **further advice**, please do not hesitate to reach out to the National Management Centre (NMC) at Police Digital Service on threatintel@nmc.police.uk.

The NMC in conjunction with the NCSC are happy to offer Individual Cyber Defence accounts which will monitor for any suspicious cyber activity associated with your personal accounts. If you wish to take up this service, please contact the NMC at threatintel@nmc.police.uk.