National Cyber Security Centre

a part of GCHQ

Advice for MPs

Keeping your data and devices safe

Cyber security advice for Members of Parliament and their staff

The NCSC

It’s our job at the NCSC to keep the UK secure online. An important part of that work involves helping public figures defend against cyber attacks.

You can use the information here to secure your personal accounts and devices. A digital, downloadable version of this advice, with many useful links, can be found at ***www.ncsc.gov.uk/mpguide.***

As an MP you are a high-profile individual.

This increases the risk of you being the target of a cyber attack.

To reduce this risk, you and your staff need to keep your accounts and devices secure.

In recent years, there have been reports from several countries of cyber attacks, targeting elected representatives and their staff. These attacks can, and do, result in serious reputational damage and the leak of sensitive information.

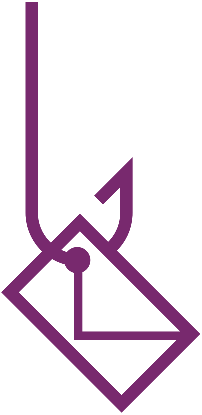
Protecting your accounts

You can take the steps outlined here to protect yourself and your staff from cyber attack. These include measures such as keeping your software and devices up to date and protecting your online accounts with strong passwords.

How you can be targeted

Many cyber attacks begin with a phishing email, designed to discover your login details. This may involve tricking you to reveal your details through, for example, an email which looks like a genuine account reset request, a link to a fake login page, or a request to perform some other action, such as forwarding a document.

The NCSC has seen a number of highly targeted phishing campaigns aimed at MPs' personal email accounts. You can find detailed advice on how to spot phishing emails at **www.ncsc.gov.uk/mpguide.**



Social media accounts

When using social media, you should be aware of how widely you share personal information. This kind of data is often collected and used to refine cyber attacks, for example, by adding details to a phishing email so it seems more convincing.

You should review the privacy settings on all your social media accounts and make sure you are happy with them.

Advice on how to do this is published by most of the major social media platforms. For a comprehensive list, visit ***www.ncsc.gov.uk/mpguide.***

Messaging apps
When using messaging apps, ensure you know who the recipients are. It can be difficult to keep control of private information in a large group chat.

As with social media, you should understand who can see your posts. This includes posts you may have made before becoming an MP.

The risks of password sharing
The social media accounts of politicians are often compromised when a single password is shared by many people.

Once the password is shared, you have no way of controlling who has access to the account. To remedy this, you should set up a multi-user social media account.

Passwords and two-factor authentication (2FA)

Passwords

Weak passwords can be easily cracked. The longer it is, the stronger it becomes and the harder it becomes to hack. **Make yours strong by using a sequence of three random words.**

Accounts which contain sensitive information should have a strong password, used only for that account, and not reused on any of your other accounts.

Remembering lots of passwords can be difficult, so use a password manager to help or store your passwords in your browser when prompted.

Two-factor authentication (2FA)

Any 'important' accounts should be protected with two-factor authentication (2FA). Very often, this involves a PIN code being sent to your mobile phone, the first time you log in from a new device. This acts as a second layer of protection on your account and makes it very difficult for attackers to gain access.

Your primary email address is a perfect example of an 'important' account. If you lose access to any of your accounts, reset details will be sent to your primary email account. As such, this email account provides a key to your online identity, so it should be protected with 2FA.

Protecting your laptops, phones, tablets and PCs

Protecting access

In order to make life difficult for hackers who have managed to get physical access to your devices, you should protect them with a password that must be entered when the device is powered on, or restarted.

To unlock from standby, you can use a password, a PIN, a drawn pattern, or a biometric, such as fingerprint or facial recognition. Use whichever method you find convenient.

Most devices come with a feature to enable you to track the location of a device and remotely wipe it if it is lost or stolen. On an iPhone, make sure “Find My” is turned on. On Android, make sure “Find my device” is enabled.

Keeping your devices up to date

Cyber criminals exploit flaws or bugs in software and apps with the aim of getting access to your devices or accounts. But manufacturers are continuously working to keep you secure by releasing regular updates.

Using the latest software, apps and operating systems on your devices can fix bugs and immediately improve your security.

Update regularly or set your phone, tablet, laptop and PC to automatically update so you don't have to think about it.

Getting help with cyber security incidents

Contact the Parliamentary Digital Support desk on x2001

If you believe you have received a malicious/phishing email, visit:
www.ncsc.gov.uk/guidance/suspicious-email-actions

If an account has been hacked, follow our advice here:
www.ncsc.gov.uk/guidance/recovering-a-hacked-account

You can report cyber security incident to the NCSC 24/7 online at **https://report.ncsc.gov.uk/** or by email to **incidents@ncsc.gov.uk.**

Key points

- **Use strong passwords.** Don’t reuse passwords on other accounts, or share them. Use a password manager to help you remember passwords.
- **Set up two-factor authentication (2FA).** Use this to provide a second layer of protection on all your most important accounts, most notably your primary email account.
- **Don’t ignore updates.** Set your phone, tablet, laptop and PC to automatically update, so you don’t have to think about it.
- **Lock your device.** Use a password, a PIN, a drawn pattern, or a biometric, such as fingerprint or facial recognition.
- **Review your social media privacy settings.** Make sure you’re happy with the privacy settings on all your social media accounts. Don’t share the password, set up a multi-user account.

www.ncsc.gov.uk
@NCSC
National Cyber Security Centre