Cyber Security Advice

Emails, Texts & Phone calls

Use the following website regularly to check whether your email address or mobile number has been compromised: https://haveibeenpwned.com/

If your email or mobile number has been compromised, don't panic! You can still use them both safely provided you take the following steps:

1. Change your password on all online accounts immediately, following the advice provided in the 'Strong Password Rules' section below.
2. Use a strong, separate password for your email account(s).
3. You may notice that you receive more phishing emails, texts or telephone calls so learn how to recognise a scam emails, texts or telephone calls by watching this Met Police video: https://www.youtube.com/watch?v=Q1bYf0-pYLs
4. Remember, the Police and the Government will NEVER call you and ask you to provide personal details over the phone.

If you receive a suspicious looking email:

- Don't reply to it or click on any attachments in the body of the email
- Forward it to report@phishing.gov.uk; the National Cyber Security Centre's Suspicious Email Reporting Service
- Delete the email from your inbox and your deleted items

If you receive a suspicious looking text:

- Forward the scam text to 7726 and this will alert your mobile phone provider of the number.
- Block the number from being able to contact your phone.
- Delete the text message and call history for this number.

If you receive a suspicious telephone call:

- Log the incident with Action Fraud either by calling them on 0300 123 2040 or completing their online reporting form on their website: https://www.actionfraud.police.uk/
- Block the number from being able to contact your phone.
- Delete the call history for this number.

Strong Password Rules

Your online accounts are only as safe as your password so make sure you apply the following rules when changing or creating a password:

- The best way to make your password long and difficult to hack is by using a sequence of three random words you'll remember.
- You can make it even stronger by using a combination of upper & lower case letters, numbers and special characters (such as; !#?)
- Avoid using personal data such as relatives' names, sports teams, places or memorable dates (basically, if it's in the dictionary, DON'T USE IT!)
- Check how strong your password is here: https://howsecureismypassword.net/
- It's good practice to use different passwords for the accounts you care most about.
- Of course, remembering lots of passwords can be difficult, but if you save them in your browser then you don't have to.
  OR
- Write your password down and keep it in a safe place at home. Either way you're more likely to create a strong password if you don't have to commit it to memory.

Online Accounts

- Ensure any social media and email accounts have an up to date recovery email address included.
- Check your credit score for any unusual activity or associations.
- Please use 2 factor authentication (2FA) / 2 step security on all devices and online accounts/apps where possible.
- Delete any unused or unwanted apps and accounts from your devices and reinstall any compromised apps.

Device Security

- Please ensure you have a Firewall and Anti-Virus software installed on all of your devices (mobile phones and tablets usually have this function already built in – you can check this in your device's security settings).
- Always have your apps set to automatically update to ensure they have the latest security patches in place.
- Always select 'update now' for any software updates you receive for your devices and set them to automatically update where able.

- Take your device(s) to a reputable I.T. professional for examination if you believe it may have been infected with some malicious software (often referred to as a virus or malware)
- Regularly back up your data to a removable hard drive or a cloud-based service so you are able to retrieve valuable personal data should your device or any online accounts be compromised in the future.

Useful Websites

Please also refer to the following websites for regular updates and advice on how to stay safe online:

https://nerccu.police.uk/ - Our regional website which provides advice on all aspects of cyber security, including signposting to relevant websites and online resources.

https://www.ncsc.gov.uk/cyberaware/home - Advice on digital cyber security (passwords, privacy settings on social media etc.)

https://www.getsafeonline.org/northumbria/ - Advice on all types of cyber security including online grooming, gaming etc.

https://takefive-stopfraud.org.uk/ - Advice on all types of fraud including cybercrime.

https://www.gov.uk/topic/dealing-with-hmrc/phishing-scams - Advice on HMRC-specific scams with examples of fake and genuine communication.