Online Safety Checklist

☐ Think you've been hacked?

- Recovering a hacked account- www.ncsc.gov.uk/guidance/recovering-a-hacked-account
  Recovering a hacked device - www.ncsc.gov.uk/guidance/hacked-device-action-to-take

☐ Passwords:

- Keep passwords secure by using 3 random words, mixed in with numbers and symbols, for example: **'3RedConnect!pug27'**
- **Visit:** https://howsecureismypassword.net/ to test the strength of your password
- Don't use information that may be in the public domain or easily worked out from social media or ancestry sites, such as your mother's maiden name or your place of birth.
- Need help to remember passwords? Use a password manager to securely store passwords. These can be found on your devices app stores. Don't share your password with anyone else.
- Don't use the same password on multiple accounts
- Change any default passwords as quickly as possible.

☐ Security Questions:

Use strong security questions to protect the forgotten password facilities to your accounts
STOP - Using facts about you & memories that the person attempting to make unauthorised access might know, or can discover through social engineering. Never duplicate an answer to a security question. There is no requirement for you to actually answer the question truthfully.
START - Making up the answers, so long as you can remember them is all that matters!
Why not use a password manager to help you remember answers: www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers

☐ Two-Factor Authentication (2FA):

Turn this on for all of your online accounts. This is an extra layer of security for your online accounts as it makes you verify your identity when logging in. An example of this would be after you have entered your username and password it will send you a verification code via text. The account you are logging into will then make you enter the code before giving you access to the account. This stops an unauthorised person being able to hack into your accounts.
Search your online accounts here: https://twofactorauth.org/ for instructions on how to enable this feature.

Antivirus & firewalls:

- Make sure your firewall is switched on. A firewall protects your device and private network from malicious software.
- If you have a Windows device, ensure Windows Defender is turned on
- It's also important to have Anti-Virus. You get what you pay for with Anti-Virus; although there are free versions available, they offer far less security options
- Make sure you are using the most up to date version of the software

www.ncsc.gov.uk/guidance/what-is-an-antivirus-product

Software:

- Ensure all software is regularly updated on your device including operating systems (e.g. iOS) and apps. Updates include security patches to fix virus vulnerabilities. If you can, select **'Auto Update'** ensuring device protection.

- Back up any important data, as this will stop any loss of files, your device breaks, gets lost/stolen or is infected by malware. This can be a physical backup (USB etc) or on the cloud.

- Before disposing of any device, ensure you have performed a factory reset to wipe all of your personal information.

- Turn off **location services** where appropriate, or change your settings to 'only whilst using the app'. Turn off screen notifications and services such as Siri when your phone is locked.
  Android: https://support.google.com/accounts/answer/3467281?hl=ens
  Apple: https://support.apple.com/en-gb/HT207092

Dealing with suspicious emails, phone calls and text messages:

Be careful with any unexpected emails or text messages, even if the sender is known. Phishing messages are intended to look like they are from a legitimate source to trick the reader into parting with sensitive data or the message could contain malware.

Never respond directly to messages asking for your personal or financial details. Don't click on the links or attachments; contact the apparent sender directly via a trusted source. For example, if the message is from your bank, contact them using the phone number on the back of your card. www.ncsc.gov.uk/guidance/suspicious-email-actions

Sextortion scams: These scams are on the increase so be aware of these scams should you become targeted

☐ WiFi:

- Do not trust public WiFi as criminals can set up fake WiFi hotspots, enabling them to intercept your personal information
- Turn off 'auto-connect' options
- Use a **Virtual Private Network (VPN)** or use your own mobile data to protect you on all public WiFi networks. A VPN is a technique that encrypts your data before it is sent across the internet.

☐ Social media:

- Think about what **personal** information is stored within your account & what data you've historically shared that could compromise you, e.g. if you have liked a particular bank on social media, that could be an indicator of who you personally bank with
- Make sure you have strong privacy settings on, choose 'friends only' or 'only me' when choosing your security settings
- Be careful when checking in and letting the world know your location. This can allow a criminal to work out patterns of behaviours, which could compromise your home and online security
- Change your settings to 'hide' your friends list to protect their security too as this will avoid duplicate friend profiles adding you as a friend as a way to bypass your privacy options set.
- Approve who follows you and what you get tagged in, this simply puts you in full control of what happens on your account.
- Check that your email address and mobile number cannot be used to find your social media accounts in a search engine.
- Remove unused connected devices that aren't required – do this before you set up 2FA
- If someone is trying to contact you via social media and you do not want them to see your account, there is always the option to block them.
- **Use a different password for each social media account**

www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

☐ Websites:

Look out for the padlock and HTTPS within your browser for the most secure way of browsing (this 'S' stands for secure). Make sure the web address is spelt correctly to help avoid accessing a fake site.

☐ **Routers:**

If you don't know how to make changes to your router or home network, you can contact your Internet Service Provider and they should be able to talk you through any changes

- Change the name and password of your home network from the default settings to something more secure and also consider changing the admin password
- Set up a guest user, so any guests who connect to your WiFi does not have full admin rights.
- You can also set up parental controls so any children do not have admin access. Consider setting up a separate network for your child so you can control what they access online and you could even turn it off when you don't want them accessing the internet. www.techadvisor.co.uk/how-to/network-wifi/second-home-wi-fi-network-3785748/

Further Considerations:

☐ **Check your digital footprint:**
Using a search engine, search your name & city to see how much of your personal information is publically available.

☐ **Open register:** www.gov.uk/get-on-electoral-register
You are automatically added to this when registering to vote. This is a way for your personal information to be sold on to third parties and becomes public information. This does not affect your right to vote and is separate to the electoral roll. It is advisable to remove yourself from this. To do this, you need to contact your local Electoral Registration Office.

☐ **192.com & ukphonebook.com:**
Check your details on these sites as they can also hold personal data about you such as who you live with, how long you've lived at your address and approximately how old you are. This website, along with others, harvests data taken from the open register. Remove your details from **192.com**: www.192.com/c01/new-request, the **UK phone book:** www.ukphonebook.com/remove_me?uen & **Companies House** if you're or have been a company director: www.gov.uk/stop-companies-house-from-publishing-your-address

☐ **Financial details compromised:**

- Contact your bank or credit card directly – if possible, call via your mobile banking app or call the number on the back of your card.
- **Credit Reference Agency (CRA):** A credit score is a tool used by lenders to help determine whether you qualify for credit. You can monitor your credit file activity or report any fraud to a CRA. You can also request a password to be placed on your credit file with all the credit reference agencies. This will help prevent credit being taken out in your name; this isn't a 100% guarantee but a good free facility for additional protection.

- **Get added to CIFAS: www.cifas.org.uk/**
  Call **0330 100 0180** (this service costs £25.00 every 2 years). This allows public authorities share information to prevent fraud.
  If you are adding yourself to CIFAS, please be aware that it could significantly delay any credit applications you are making, so only use this if it is necessary.

☐ **Data breach:**

A data breach is a security incident where personal information, such as email addresses, passwords, are stolen or taken from a system without the knowledge or authorisation of the owner. The consequences of a data breach can include identity theft or the details can be sold on to other criminals.

- **www.haveibeenpwned.com** - this website that allows you to check if your personal data has been compromised by data breaches. Their "Notify me" service allows visitors to subscribe to notifications about future breaches.
- Change passwords and security questions if your accounts have been involved in a data breach – this is an example of why you shouldn't use the same password on multiple accounts.

☐ **ID Material compromised:**

Check with HMRC and the electoral register to ensure your details haven't been changed. For example, address details.

- **Passport:** Passport photo or copy of passport sent – Tel: 0300 222 0000 or visit www.gov.uk/passport-advice-line
- **Driving licence:** If this is compromised, contact your insurance company and contact the DVLA.
- **National Insurance number:** Contact the Inland Revenue/HMRC to confirm the compromise. Tel: 0300 200 3500 (Mon - Fri: 8am to 8pm & Sat: 8am to 4pm)

Financial / Support Services:

☐ **A power of attorney to next of kin:** Age UK can assist with this or visit: **www.gov.uk/power-of-attorney**

☐ **Citizens Advice:** Free legal advice in some parts of England. Free general support, advice & guidance. Call 0344 411 1444 or visit **www.citizensadvice.org.uk**

☐ **Welfare Rights:** Provides free advice & help with claiming correct or emergency benefits, tax credits & advice on managing debt. Visit: **www.nottinghamcity.gov.uk/welfarerights**

☐ **Financial Ombudsman Service: www.financial-ombudsman.org.uk/**

@NottsCyberCrime
Nottinghamshire Police
Nottinghamshire Police

If you haven't already, please ensure any incident of Cyber Crime or Fraud is reported to Action Fraud.

Tel: 0300 123 2040
www.actionfraud.police.uk