# Cyber Advice Check List - **Steps to protect your information online:**

□ **Passwords:** Think of your password as the front door to your account. Think random by creating a strong password using three random words. For example: **'SataliteScallopHope'** you can even mix this up with numbers '**5atalit5callop4ope'** to strengthen this further. If you've been subject to a breach please change all affected passwords. Change default passwords as these can be accessible to hackers online.
**Visit:** https://howsecureismypassword.net/ to test what a secure password looks like.
STOP - Using family/pet names or key facts about you. Stop sharing & reusing/using generic passwords, especially on your email, home WIFI/Router, banking & social media accounts: www.cyberaware.gov.uk/passwords

□ **Security Questions:** These are the back door to your account. Use strong security questions to protect the forgotten password facilities to your accounts. Keep both doors locked from hackers!
STOP - Using facts about you & completing social engineering questionnaires.
START - Using memories significant only to you or make up the answer, so long as you can remember them – that's all that matters! If you've been subject to a breach please change all affected security questions

□ **Email/Text:** Be careful with any unexpected emails or text messages, even if the sender is known & reflects on a previous message chain. Don't open any attachments, call numbers provided on the message or click on any links sent. Change E-mail account if required. To do this, generate a new account with your chosen provider & update relevant organisations.
www.getsafeonline.org/protecting-your-computer/spam-and-scam-email/

□ **Software:** Ensure all software including device APP & IOS updates are all regularly updated. Whatever devices, operating systems, software or apps you use, always ensure you are running the most up to date versions. Updates include security patches to fix vulnerabilities! If you can, select **'Auto Update'** to ensure devices are always protected.
www.getsafeonline.org/protecting-your-computer/software-updates/

□ **Wifi:** Don't assume Wi-Fi hotspots in places like cafes or hotels are secure - Never use them to do anything confidential like using your email or making a payment. A **VPN (virtual private network)** will protect your information when connected to free WIFI networks, without you run the risk of anyone being able to record any activity you do.
www.getsafeonline.org/smartphones-tablets/wireless-networks-and-hotspots/

□ **Two-factor authentications (2FA):** An extra layer of security. If someone were to try & login to your account, they would not be successful without having access to your phone's text code, so try & use them wherever possible. www.turnon2fa.com/tutorials/

□ **Back-Up** - Regularly back-up your data, securely, to a portable hard drive or online. If your device is lost or compromised, you can then retrieve your essential or irreplaceable information. www.getsafeonline.org/protecting-your-computer/Backups/

□ **Social Media:** Hackers can target social media accounts in various ways from searching using a name, mobile number, email addresses or by sending fake friend requests. www.saferinternet.org.uk/advice-centre/social-media-guides & www.internetmatters.org/advice/social-media-guides-parents/

## Additional Tips to consider:

- **Go for the strongest privacy option available:** For example, if **Only Me**, **Friends** or **Friends of Friends** are the given options you'd opt for **'Only me'.**
- **Approve** who follows you & what you get tagged in
- **Is it Public?** Before joining seemingly **"closed"** groups or liking a page or post, check if the group member's details are open to public before joining. By '**checking in**' you are making your 'check in' post public
- **What are you sharing?** Think about what **personal** information you are storing. For Example. Storing your full date of birth will only be held against you so why not change your year of birth?
- **Check contact details privacy settings:** After each App update to ensure they haven't reverted to the default **"public"** setting
- **Remove unused connected devices:** Remove from your account that aren't required prior to setting up 2FA
- **Block contacts:** All that link to the stalker & hide friend lists to avoid fake friend requests being sent
- **Remove devices** connected to your account that aren't required prior to setting up 2FA

□ **Device & Web:** Don't exit applications, instead **log-out**, otherwise you will likely remain logged in. Look out for the padlock 🔍 ▾ 🔒 ↻ and **HTTPS** within your browser for the most secure way of browsing (this 'S' stands for secure). Don't tick **'remember my password'** within the browser as hackers can use this as a way in to accounts.

□ **Antivirus:** Ensure its installed, updated regularly & running for all devices you use. www.getsafeonline.org/index.php/protecting-your-computer/viruses-and-spyware

## Further Considerations:

- **Check your digital footprint** - Google yourself. Check the UK Phonebook, Online electoral open register & 192.com for entries in your name – Request removal
- **Check your email address** - https://haveibeenpwned.com/ to see if your email has been involved in a data breach & change relevant passwords/security questions if breached.
- **Ensure your home router has a password set** - If it's the original default, change it. Create a guest user for friends & family to connect to when visiting, keeping admin facilities private.
- **Keeping smart devices safe**: www.ncsc.gov.uk/guidance/keeping-your-smartphones-and-tablets-safe
- **Cyber Stalking Advice:** www.getsafeonline.org/safeguarding-children/cyberstalking1/
- **Mobile Apps:** www.getsafeonline.org/smartphones-tablets/mobile-apps/
- **Identity Theft:** www.getsafeonline.org/protecting-yourself/safeguarding-identity/
- **Location Services:** **Android:** https://support.google.com/accounts/answer/3467281?hl=ens **Apple**: https://support.apple.com/en-gb/HT207092

NOTTINGHAMSHIRE
POLICE
PROUD TO SERVE

Created By: Nottinghamshire Cyber Crime Unit – Officer 4653 28/01/2019.

**For updates and tips on how to protect yourself please follow us on Twitter: @nottscybercrime**