Online Security Checklist

Protecting online accounts:

☐ Password Security:

- Create strong passwords by using 3 random words. You can include numbers and symbols. For example, "**Read421-Plants-!Treasure**". Do not use words that can be guessed (like pet names, family names or birth dates).
- Keeping passwords separate across different accounts can be hard to remember, but it is an essential step in protecting all your online accounts.
- Password managers will help you create and store strong, unique passwords, for all your different accounts. Password managers are easy to use, hard to crack and will save you from having to memorise your passwords (remember to back-up if using this option). Remember to store a copy of the password manager's master password, by writing it down securely at home in a safe and preferably hidden location. Alternatively, you can write down all your passwords at home or save them to your browser if safe to do so.
- For more information: www.ncsc.gov.uk/cyberaware/home

☐ **2-Factor Authentication (2FA):** 2FA can also referred to as 2-step verification, multifactor or biometric authentication. Turning it on is one of the most effective ways to protect your online accounts from cyber criminals and can be applied across most accounts. For example. Device accounts (AppleID, Samsung, Google etc.), email, social media (including WhatsApp) and most online shopping accounts and apps.

- 2FA sends an OTP (One-Time Passcode) or PIN request to a device that only you have access to, such as your phone, or authentication app to prove it's you that is logging in. Visit each online account you have and review the security settings to enable this feature as soon as you are able. 2FA on many accounts and apps turned off by default but setting it up usually takes seconds but improves your overall account security immensely! Prioritize this step.
- If your email does not support 2-Factor Authentication, then it is advisable to set-up a new email address with a new email provider as your email is not secure without it.
  For more information, visit: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email
- Never share an OTP (One-Time Passcode) as this is used to approve a login to your account. Keep them private. You wouldn't share your bank pin so **do not share any OTP codes**!

☐ **Data breach:** A data breach is a security incident where personal information, such as email addresses and passwords are breached/stolen from an organisation you may have been registered with. For more information: www.ncsc.gov.uk/guidance/data-breaches

- Visit: www.haveibeenpwned.com to check if your information has been compromised by a data breach. There is also a "**Notify me**" service available, which when activated, notifies you on future breaches involving your email address.
- Change the password linked to the account involved in a breach using a secure password and enable 2-factor authentication on all online accounts (email, social media, online shopping).

Last updated – 07/04/2025/KJ

Enable strong privacy settings:

☐ Social Media:

- Use a different secure, random password for each social media account and enable 2FA.
- Ensure your linked email is up to date, having an old email account available will leave your account at risk, and will make it extremely difficult if you ever need to recover the account.
- Disable/hide your private email address and mobile number, to prevent search engine queries from locating your social media accounts.
- Review what personal information is stored. For example. Your full date of birth.
- Control who sees your location data, **disable any default location tracking options**.
- Approve who follows you and what you get tagged in.
- Change your settings to '**hide**' your friends/followers or make your account private to protect yourself from falling victim to account impersonation from your friends/followers. This is also often used to expose your friends/followers with targeted scams with you as the origin if your accounts are ever compromised, which can damage your reputation.
- Remove old or unused connected devices.
- **For further information, visit:** www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

☐ **Devices and other software:** Each time you download new software or an App, you will be approving access to various amounts of personal data. You can review all the privacy settings within devices, software, and the online accounts you have. For example, device security:

- iOS (Apple) devices have a **'Privacy'** setting which allows you to review what applications are accessing by selecting each option displayed (Location, contacts, calendar, photos etc).
- Android users can review each application and what that application is accessing within the **'Apps'** setting.
- For desktop PC or laptop specific advice, visit: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

Device Security:

☐ Software:

- Turn on automatic updates for your devices and software that offer it. This will mean when a new update is available it will download when your phone is resting and has full charge.
- Turn off '**location services**' within privacy settings where appropriate or change your device privacy settings to '**only whilst using the app'**. Turn off the option to display screen notifications and services such as virtual assistants like Siri/Alexa when your phone is locked.

☐ **Backing up data:** Backing up regularly means you will always have recent copies of your information saved. This will allow you to recover data which has been lost or stolen.

- You can also turn on automatic backups, this will regularly save your data to cloud storage.
- Manage what is backed up in device settings, this will allow you to back up important data.
- For more information, visit: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data

☐ **Dealing with suspicious emails and text messages:** Criminals are great pretenders. They may contact you pretending to be a trusted person or company. Millions of people are targeted by scam messages or phone calls like this every year. If you receive anything or are approached by anybody who seems suspicious or the contact is unexpected, such as requests for money or information, cease the contact and reach out to the organisation directly by using their legitimate contact details from their official website or app. Do not allow criminals to trick you.

- Always question why someone is calling, texting, or emailing you. You are in control of who you speak to or respond to. Never feel pressured. Assume all contact is a scam until verified: www.ncsc.gov.uk/collection/phishing-scams
- Enable the spam filter within your email account to minimise the risks.
- Email compromise: www.eastmidlandscybersecure.co.uk/personal-email-compromise
- Sextortion scams: www.ncsc.gov.uk/guidance/sextortion-scams-how-to-protect-yourself
- Spot the most obvious signs of a scam: www.ncsc.gov.uk/guidance/suspicious-email-actions

☐ **Websites:**

- When using a browser, you will find an address bar or URL bar. This is the bar at the top of your screen where the website address is displayed. Check this bar for the **padlock symbol** and **https://** which shows that it is secure, before entering personal or payment information.
- Always check the spelling is correct, with no additional letters or words included and look out for numbers used instead of letters as this is a method used by fake websites.
- When you have finished using an account, remember to log-out, especially in public settings.
- For online shopping advice, visit: www.ncsc.gov.uk/guidance/shopping-online-securely

If your personal details have been compromised, please consider:

☐ **Credit Reference Agency (CRA):** Do your research for the most applicable services and to review for a good reputable one. Credit Reference Agencies allow you to view your credit report. Credit reports show your financial history and credit score. You could check your report at the start of each month to monitor key changes or updates, as this could help identify fraudulent activity and any unrecognised searches. A search could be for a new credit application, credit increase, loan application or for other financial services. If you do identify an unrecognised search, you can report this directly with the organisation linked to the search. Most Credit Reference Agencies also offer a credit lock to secure your credit report, this is another advisable action to consider, which will help stop fraudsters applying for credit in your name.

☐ **CIFAS:** CIFAS is a non-profit membership association, it acts as a dedicated Fraud Prevention Service within the UK and is used by most banks, credit, loan, finance and insurance companies. CIFAS is unique and is the world's first non-profit fraud prevention data sharing scheme which serves to allow its members share information about identified frauds and fraud trends. Adding a fraud marker can apply additional security for credit applications in your name. For more information, visit: www.cifas.org.uk/ or to add a Fraud marker, visit: www.cifas.org.uk/services/identity-protection/protective-registration/application-form

Worried about identity theft? Visit: https://ico.org.uk/for-the-public/identity-theft/

Last updated – 07/04/2025/KJ

Areas on the internet that may store your personal data:

☐ **Open Register:** You are automatically added to this when registering to vote on the Electoral register. If you don't opt some of the details that you supply will become public information. For more information, visit: www.gov.uk/get-on-electoral-register

☐ **192.com, yell.com and ukphonebook.com:** You can review these sites as they can hold personal data about you. This can include who you live with, how long you have lived at your address and how old you are. These websites, along with others, harvests data taken from the open register, and nefarious elements e.g. fraudsters, may use this information against you:

- To remove details from 192.com, please visit: www.192.com/c01/new-request
- To remove details from yell.com, call their customer service number: 0800 555 444 Mon-Thu 9am-5pm, Fri 9am-4:30pm.
- To remove details from the UK phonebook, visit: www.ukphonebook.com/remove_me?uen
- Please note that there may be other websites not listed here that share personal information. You can research what personal data might be on the internet about yourself further, by using a reputable search engine such as Google etc; to search for your name and town. It is also a good idea that when doing this review, you also spend some time to search for your social media accounts, to review what information is available about you publicly.
- Google removal form to request removal of results that include your name (Google only): www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&pli=1
- If you are or have been a company director: www.gov.uk/stop-companies-house-from-publishing-your-address

Once you have reviewed this checklist, we would really appreciate your feedback by completing our brief 2-minute survey:

If you are a victim: www.smartsurvey.co.uk/s/NottinghamshireVictimIndividual/

For anyone else: www.smartsurvey.co.uk/s/NottinghamshireIndividuals/

If you need more information with any online security visit:
www.eastmidlandscybersecure.co.uk

Last updated – 07/04/2025/KJ