



Online Security Checklist

Protecting online accounts:

- ☐ **Start an action plan:** www.ncsc.gov.uk/section/advice-guidance/you-your-family

- ☐ **Password Security:**
 - Create strong passwords by using 3 random words. Include numbers and symbols. For example, “**Read421-Plants-!Treasure**”. Avoid pet/family names or birth dates etc. www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words
 - Keeping passwords separate by having a different password for each account you have can be hard to remember but is an essential step to protect all online accounts you have.
 - Use passkeys where possible: www.ncsc.gov.uk/passkeys
 - Password managers will help manage, create and store strong, random passwords for all online accounts. Password managers are easy to use, hard to crack and will save you from having to memorise passwords. Remember to back-up if using this option and store a copy of the password manager’s master password, alongside other master passwords needed in the event you cannot access your devices. Do this by writing them down securely at home in a safe/hidden location. www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers

- ☐ **2-Factor Authentication (2FA):** Also referred to as 2-Step Verification (2SV), 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. www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/activate-2-step-verification-on-your-email
 - 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 as this is not a default feature. 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.
 - Never share an OTP (One-Time Passcode) as this is used to approve a login to your account.

- ☐ **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 have an account with.
 - 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 random password and enable 2-factor authentication if this is not already applied.
 - For more information: www.ncsc.gov.uk/guidance/data-breaches

Enable strong privacy settings:

☐ Social Media:

- Set account to private where possible, especially on personal accounts.
- 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 and remove anything unnecessary.
- 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 to protect yourself from falling victim to account impersonation and your friends/family from being targeted by scammers.
- For further information, visit: www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

☐ Protecting your data:

- 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: 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 more information visit: www.ncsc.gov.uk/section/advice-guidance/you-your-family

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.
- Download apps from trusted app or play stores.
- For more information visit: www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates

☐ **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

☐ **Securing your devices:** www.ncsc.gov.uk/guidance/securing-your-devices

☐ **Dealing with suspicious emails and text messages:** Criminals are great pretenders.

They may contact you pretending to be a trusted person or company. 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.

- Hang-up and don't engage if called, messaged or emailed out of the blue. You are in control of who you speak to or respond to. Assume all contact is a scam until verified.
- Enable the spam filtering within your email, network provider and device settings.
- 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** or **https://** as this confirms the website uses encryption to protect your personal or payment information as it processes through the website. **http://** without the 'S' is unencrypted.
- Check the spelling is correct within any web address to avoid fake malicious websites, with no additional letters or words included. Review the address for numbers used instead of letters and avoid sponsored or prepopulated suggested sites.
- When you have finished using an account, log-out, especially on a device used by others.
- 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 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/individuals Alternatively, call **0330 460 9601**, phone lines are open Tuesday and Thursday from 9.30am to 2.00pm. **Worried about identity theft?** Visit: <https://ico.org.uk/for-the-public/identity-theft/>

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 out 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. Search for your social media accounts to see what data linked to the account is public.
 - 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
 - For company directors: www.gov.uk/stop-companies-house-from-publishing-your-address

For anyone that has already been hacked:

- ☐ **Recovering a hacked account:** www.ncsc.gov.uk/guidance/recovering-a-hacked-account
- ☐ **Reporting:** <https://www.reportfraud.police.uk/>

Once you have reviewed this checklist, we would really appreciate your feedback by completing our brief 2-minute survey to tell us how you got on:



www.smartsurvey.co.uk/t/Nottinghamshire-Individuals/



View this document, privacy setting guidance, our free live webinars, parental settings, online security, fraud and scam protection resources:
www.eastmidlandscybersecure.co.uk/nottinghamshire-event-handout