Online Security Checklist

If you need more information with any online security, fraud, or reporting, you can access our website: www.eastmidlandscybersecure.co.uk/nottinghamshire

Protecting online accounts:

☐ Password Security:

- Create strong passwords by using 3 random words. You can include numbers and symbols. For example, "**ReadPlantsTreasure4!**". Do not use words that can be guessed (like pet's name, family names or birth dates).
- Keeping passwords separate across different accounts can be hard to remember, but it is a key step in protecting all your online accounts.
- Password managers will help you create and store strong, different 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). Alternatively write them down securely at home or save to you browser if no one else has access to it.
- Think about password recovery answers for forgotten password options too, if they can be easily acquired/guessed, this option could be used to bypass the password.
- For more information: www.ncsc.gov.uk/cyberaware/home.

☐ **2-step verification (2SV) -** This can also be referred to as 2-factor or multifactor authentication: 2-step verification (2SV) can help keep criminals out of important accounts, such as your email and social media, even if they know your password.

- 2SV sends a code or PIN to a device that only you have access to, such as your phone, to prove it's you logging in. If 2SV is available for your account, you're usually prompted to set it up. Alternatively, the option to switch it on is usually found in security settings.
- If your email does not support 2-step verification, 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

☐ **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.

- Visit: www.haveibeenpwned.com to check if your information has been compromised by a data breach. There is also a "**Notify me**" service available that notifies you on future breaches involving your email address.
- Change the password linked to the account involved in a breach using a secure passwords and enable 2-step verification on all online accounts (email, social media, online shopping).
- **For more information:** www.ncsc.gov.uk/guidance/data-breaches.

Enable strong privacy settings:

☐ Social Media:

- Use a different secure, random password for each social media account.
- Ensure your linked email is up to date, having an old email account available will leave your account at risk and will make it difficult if you ever need to recover the account.
- Disable/hide your email address and mobile number from linking to your social media accounts within a search engine.
- Think about what personal information is stored. For example. Your full date of birth.
- Do not let the world know your location, do this by disabling your '**location**'.
- 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, these are set-up to bypass privacy settings and target friends/followers with targeted scams.
- Remove old or unused connected devices
- **For further information, visit**: www.eastmidlandscybersecure.co.uk/socialmediascams.

☐ **Devices and other software:** Each time you download a new application (App) or software you will be approving access to various amounts of personal data. Review all privacy settings within devices and software. For example, you can review privacy options by accessing your device settings.

- Apple devices have a '***Privacy***' setting which allows you to review what applications are accessing by selecting each option displayed (Location, contacts, calendar, reminders, 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/guidance/online-gaming-for-families-and-individuals and www.eastmidlandscybersecure.co.uk/nottinghamshire.

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**' 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.
- **For further information**: 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 into cloud storage, without you having to remember. Automatic backups do save all data into the cloud and can use up a lot of storage. You can manage what is backed up in your settings, this will allow you to back up what data is important to you.
- For more information: 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. So if something seems suspicious or unexpected, such as requests for money or information, contact the organisation directly to check. Use contact details from their official website or app, not those given in the message.

- 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 everything sent to you across all communication platforms is a scam until verified.
- 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
- Social media scams: www.eastmidlandscybersecure.co.uk/socialmediascams
- How to spot the most obvious signs of a scam: www.ncsc.gov.uk/guidance/suspicious-email-actions.

☐ Websites:

- Within the browser (this is the bar at the top of your screen where the website address is displayed), check for the **padlock symbol** and **https://** before you enter 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.
- For more information on shopping online securely, visit: www.ncsc.gov.uk/guidance/shopping-online-securely.

Areas on the internet that may store your personal data:

☐ Open Register:

You are automatically added to this when registering to vote from the Electoral register and if you don't opt out of this then your information will become public. For more information on how to opt out of the open register, visit: www.gov.uk/get-on-electoral-register.

☐ **192.com and ukphonebook.com:** You can check your details on these sites as they can also 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:

- To remove details from 192.com, please visit: www.192.com/c01/new-request.
- To remove details from the UK phonebook, visit: www.ukphonebook.com/remove_me?uen.
- Please note that there may be other websites not listed that share personal information.
- If you are or have been a company director: www.gov.uk/stop-companies-house-from-publishing-your-address.

If your personal details have been compromised, please consider:

☐ **CIFAS:** CIFAS is a non-profit membership association, a dedicated Fraud Prevention Service within the UK and is used by most banks, insurance/credit/loan, and finance companies. Members share information about identified frauds in the fight to prevent further fraud. CIFAS is unique and is the world's first non-profit fraud prevention data sharing scheme. 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.

☐ **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 indicate fraudulent activity if you identify any unrecognised searches. A search could be for a new credit application, credit increase 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 lock your credit report, this is another advisable action to help stop fraudsters applying for credit in your name.

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

If you have been a victim, visit: www.smartsurvey.co.uk/s/Nottinghamshire23-24VICTIM/

For anyone else, visit: www.smartsurvey.co.uk/s/Nottinghamshire23-24IND/