Online Security Checklist

Think you have been hacked?

www.ncsc.gov.uk/section/information-for/individuals-families#section_3

How to report cyber crime:
If you think you might have been a victim of Cyber-Crime, please visit: www.actionfraud.police.uk or call: 0300 123 2040, to report the incident.
Alternatively, if you are currently being subjected to a live and ongoing cyber-attack then please contact us on 101.

Report a scam website: www.ncsc.gov.uk/section/about-this-website/report-scam-website

Protecting online accounts:

☐ Password Security:

- Create strong, sperate, memorable passwords by using 3 random words. You can include numbers and symbols if you need to. For example, "**ReadPlantsTreasure4!**". Do not use words that can be guessed (like your pet's name or other family names or birth dates).
- Keeping passwords separate across different accounts can be hard to remember, but an important step to protect all online accounts.
- Saving your passwords in your browser/password manger will help you manage them (we highly recommend enabling a master password within the browser to protect saved passwords): www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers
- Think about password recovery answers for forgotten password options too, if they can be easily acquired, this option could be used to bypass the password.
- For more information view our online webinar here: https://youtu.be/F-20oYJZUMY

☐ Two-Factor Authentication (2FA):

- Two-factor authentication (2FA) helps prevent hackers from gaining access to your accounts, even if they have your password.
- For more information, visit: www.ncsc.gov.uk/cyberaware/home#action-4

How protected is your data?

☐ 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.

- ✓ Visit www.haveibeenpwned.com to check if your personal data has been compromised by data breaches. There is also a "Notify me" service available that notifies you on future breaches involving your email address.
- ✓ Change passwords if your accounts have been involved in a data breach.
- ✓ Keep passwords separate and random to reduce the risk of a data breach compromising all your online accounts.
- ✓ For more information: www.ncsc.gov.uk/guidance/data-breaches

☐ Digital Footprints:

Your digital footprint is your new CV for future employers and can be used against you by Criminal Hackers or Fraudsters!

- ➢ Think about what you share and how this can be used against you in the future.
- ➢ Using a search engine, search your name & city to see how much of your personal information is publicly available.
- ➢ Request removal of personal data where possible and delete old accounts that are no longer in use.
- ➢ For more information visit: www.eastmidlandscybersecure.co.uk/digital-footprint

Enable strong privacy settings by:

☐ Social Media:

- ✓ Approving who follows you and what you get tagged in
- ✓ Checking that your email address and mobile number cannot be used to find your social media accounts in a search engine.
- ✓ Change your settings to 'hide' your friends list to protect yourself from falling victim to account impersonation, these are set up to bypass privacy settings and target friends/followers with scams.
- ✓ Remove unused connected devices that are no longer required.
- ✓ Think about what personal information is stored
- ✓ Don't let the world know your location
- ✓ Use a different password for each social media account.
- ✓ For guidance on implementing these settings refer to: www.eastmidlandscybersecure.co.uk/socialmedia

- ➢ Snapchat support: www.eastmidlandscybersecure.co.uk/safetyonsocialmedia
- ➢ If your social media has been hacked it's important to check your email to see if this has also been compromised, for more information: www.eastmidlandscybersecure.co.uk/compromised-emails-individuals
- ➢ For a helpful video for further support, visit: www.youtube.com/watch?v=H8ZlbA4HiYA

Device Security:

- **Device security including Anti-virus:** www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/antivirus-and-other-security-software
- **Buying and selling second-hand devices:** www.ncsc.gov.uk/guidance/buying-selling-second-hand-devices
- **'Smart' security cameras: Using them safely in your home:** www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home
- **Smart devices: using them safely in your home**: www.ncsc.gov.uk/guidance/smart-devices-in-the-home
- **Video conferencing services: using them securely:** www.ncsc.gov.uk/guidance/video-conferencing-services-using-them-securely

☐ Software:

- Out-of-date software, apps, and operating systems contain weaknesses. This makes them easier to hack.
- Companies fix the weaknesses by releasing updates. When you update your devices and software, this helps to keep hackers out.
- Turn on automatic updates for your devices and software that offer it. This will mean you do not have to remember each time.
- Some devices and software need to be updated manually. You may get reminders on your phone or computer. Do not ignore these reminders. Updating will help to keep you safe online.
- 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
Apple: https://support.apple.com/en-gb/HT207092

For further information: www.ncsc.gov.uk/cyberaware/home#action-5

☐ Backing up data:

- ✓ Backing up regularly means you will always have a recent version of your information saved. This will help you recover quicker if your data is lost or stolen.
- ✓ You can also turn on automatic backup. This will regularly save your information into cloud storage, without you having to remember.
- ✓ If you back up your information to a USB stick or an external hard drive, disconnect it from your computer when a back-up isn't being done. If you back up your information to a USB stick or an external hard drive, disconnect it from your computer when a backup isn't being done.
- ✓ For more information: www.ncsc.gov.uk/cyberaware/home#action-6

☐ Dealing with suspicious emails and text messages:

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.

How to spot the most obvious signs of a scam, and what to do if you've already responded: www.ncsc.gov.uk/guidance/suspicious-email-actions

- ✓ Always question why someone is calling, texting, or emailing you
- ✓ You are in control of who you speak to or respond to
- ✓ 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, go directly to the organisations website or through the appropriate App to query the contact.
- ✓ Never feel pressured
- ✓ Enable the spam filter within your email account to minimise the risks
- ✓ Be careful when clicking on links from Social media as these could be fake offers, websites, vouchers
- ✓ Sextortion scams – how to protect yourself - www.ncsc.gov.uk/guidance/sextortion-scams-how-to-protect-yourself

To report a fraudulent email then they can forward it to the National Cyber Security Centre inbox: report@phishing.gov.uk or for text scams forward the original message to **7726** (spells SPAM on the keypad).

☐ Websites:

- ✓ Within the browser, the bar at the top of your screen where the website address is displayed, check for the padlock symbol and https (this 'S' stands for secure) 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 to trick you.
- ✓ When you've finished using an account, remember to log-out.
- ✓ Shopping online securely: www.ncsc.gov.uk/guidance/shopping-online-securely

☐ Wi-Fi:

- ➢ **Secure your home WIFI:**
  Home users connect to the internet via a Wi-Fi router or 'Hub'. As such, it is often targeted by cybercriminals who wish to hijack your online connection or infiltrate your home network for personal gain. For more information visit: www.eastmidlandscybersecure.co.uk/the-home-hub and view our online webinar: https://youtu.be/c69JA35dcD0
- ➢ **Public Wi-Fi:**
  Don't use public Wi-Fi to transfer sensitive information such as card details
  Cyber criminals can set-up fake Wi-Fi hotspots, enabling them to intercept sensitive information you are transferring online. Either use your own data or a Virtual Private Network (VPN).