CYBER SAFETY CHECKLIST

- Do not reuse passwords or use the same password on more than one account.
- Always use strong passwords. A strong password can easily be made by combining three random words with a few numbers and symbols eg. *GiraffeBubb!esD@ncing*.
- Avoid using any personal details such as pet's name, date of birth, favourite movie, show or sports team in your passwords or account security questions.
- Ensure default passwords have been changed on your network router, smart devices and Internet connected toys and games. Also change your default WiFi hotspot name.
- Consider using a reputable password manager. These can generate, store and enter all your passwords for you, making logging-on quicker, easier and more secure.
- Make sure your laptops, phones, tablets and other mobile devices are secured with a strong password and/or a biometric (finger/face/retina) lock.
- Enable two-factor authentication (2FA) on each account, to add an extra layer of security that can keep your account safe even when someone obtains the password.
- Keep all your devices, software and apps up-to-date to fix new security vulnerabilities and bugs. Do not use devices that can't be kept up-to-date or are no longer supported.
- Only use official app stores (Play Store, App Store, etc.) to download apps and games.
- Regularly backup your important files and photos. Use a separate USB memory stick, hard drive or a cloud based storage service to keep copies of all your important data.
- Phishing emails and messages are used to steal your passwords and personal information by tricking you into entering them on a page that looks like a genuine logon screen or site. Cyber criminals may spoof the sender's email address and use real names, logos and other content to make fake messages seem authentic.
- Criminals may also spoof phone numbers which may result in your smartphone unknowingly adding a scam text (SMS) to an existing message-thread that you trust.
- The best way to stay safe from phishing attacks is to avoid clicking links in any unexpected email, text or message no matter how important or urgent they may seem. Instead, access the account in question by typing the web address for your existing account into your browser, or make contact using a known and trusted phone number.

Email CyberProtect@northants.police.uk for further Cyber Safety information or to arrange free cyber security training for your community group, organisation or business.

Northamptonshire Police
Fighting crime, protecting people

CYBER SAFETY CHECKLIST

- If you have already filled in your personal details on a fake or scam webpage, notify your bank and credit card provider and check the information below on identity theft.

- Check your bank and card statements and report any rogue payments, subscriptions or loans. Visit cifas.org.uk for information on protecting yourself from identity theft.

- Criminals may phone you purporting to be customer service or technical support staff, calling on behalf of a computer, phone or Internet service provider. They will claim that they have identified a problem with your device or Internet connection that needs fixing immediately. They can be extremely convincing and manipulative and may even seem helpful or polite. It is important to ignore their instructions and just hang-up the call.

- Pop-up messages, warnings or alerts may appear on your computer or device, claiming to have detected viruses or other security or Internet issues. These may tell you that you must call a phone number or visit a website for urgent support. If in doubt, contact your choice of reputable computer company or support service that you trust.

- Visit the the gov.uk website to access, search or check any online government department or service to ensure you are using the genuine site and information.

- Always pay for online purchases and services using a credit (not debit) card or reputable payment provider that offers buyer protection, and never by bank transfer.

- Your personal information may have been leaked as part of a company data breach, after a website or online service you have used was hacked or made a data processing error. Your password, address and other account details may have been made available on the Internet and used by criminals to carry out cybercrime or fraud.

- Online accounts that you have set-up but no longer use may still contain personal information that could be at risk from cyber criminals. Secure these dormant accounts by changing the password, removing data or closing down the account.

- A useful website to check if any of your online accounts have suffered a data breach is haveibeenpwned.com Visit this site and enter your email address to find out if any of your personal account data has ever been leaked.

- Further Cyber Security information can be found at:

  CyberAware.gov.uk

  NCSC.gov.uk

  GetSafeOnline.org

Jan-2021

✓ AM I NOW CYBER SECURE?

○ I will not reuse passwords or use the same password on more than one account.

○ All my accounts now use long and strong passwords.

○ I have enabled two-factor authentication (2FA) on all my online accounts.

○ I have enabled the auto update feature on all my devices, to ensure I always have the latest apps and system software on my phone, computer and tablet.

○ I have checked my email on haveibeenpwned.com for data breaches that affect me.

○ I have closed or secured all my old, unused or dormant online accounts.

○ I know that scam emails contain links to phishing websites that are designed to steal my passwords, personal information and financial details.

○ I know that criminals send fake texts that appear to come from organisations and people I know or trust.

○ I know to avoid clicking links from unexpected and unverified texts, emails and social media messages.

○ I know to ignore pop-ups or alerts that appear, telling me to ring a specific phone number or enter personal information to rectify a claimed computer or Internet issue.

○ I am aware that an unexpected caller may phone me, claiming to be a computer company, Internet provider, bank, police or other organisation and attempt to gain remote access to my computer, documents and bank accounts.

○ I know to never download or add software to my computer, or reveal account details at the request or instruction of an unexpected caller or text message.

○ I will ensure that I verify messages that request gift cards, vouchers, money and payments before sending any funds or purchasing the requested items.

○ I will ignore messages claiming that my accounts or Internet access will be locked or suspended unless I respond immediately with information or payment details.

○ I will regularly backup all my important photos and documents on each device, to ensure I can restore my data after a ransomware attack or system failure.

○ I will not log-on to my accounts on untrusted or publicly accessible computers.

WE'RE ASKING THE NATION TO: TAKE FIVE TO STOP FRAUD™

- Never assume an email, text, social media post or phone call is genuine
- Stay in control – verify the email, text or call using another trusted means
- Don't be rushed into clicking a link or supplying financial information
- Don't pay unexpected bills, fines or charges unless they've been verified
- Never reveal personal details such as your password or PIN

Find out more: **takefive-stopfraud.org.uk**