Public Guide

Protecting you against Cyber Crime

Lancashire Cyber Crime Unit

Contents

This guide provides an overview of steps that can be taken to help protect yourself from Cyber Crime.

Contents:

Smartphone Devices

With smartphone technology being at the forefront of our lives, it is important to know how to protect your device.

Public Wi-Fi
The wireless connection used by most public Wi-Fi hotspots is not encrypted. Therefore, anybody nearby can read data being sent between the device and the hotspot. This could include sensitive information such as passwords and personally identifiable data.

Utilise 3G/4G or VPNs when dealing with sensitive information instead of connecting to public Wi-Fi.

Do not utilise public Wi-Fi to make purchases or access your personal accounts.

For more information about the risks of public Wi-Fi visit the ‘common questions’ section in the NCSC End-of-User Guide https://www.ncsc.gov.uk/collection/end-user-device-security/eud-overview/common-questions#wifi

Mobile Ransomware
Ransomware is a type of malware that prevents you from accessing your device (or the data that is stored on it). The device itself may become locked, or the data on it might be stolen, deleted or encrypted.

Normally you're asked to make a payment (often demanded in a cryptocurrency such as Bitcoin), in order to unlock your computer (or to access data). However, even if you pay the ransom, there is no guarantee that you will get access to your computer, or your files.

The NCSC advise that victims **DO NOT** pay ransoms, instead report to Action Fraud. For more information on how to mitigate malware and ransomware attacks please visithttps://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Quick Tip:
Save your online shopping until you are home!
Protect your payment and login credentials online.

Smartphone Devices

With smartphone technology being at the forefront of our lives, it is important to know how to protect your device.

Patching

- Vulnerabilities in technology are always being discovered and in response, manufacturers regularly issue security updates to plug the gaps. Applying these updates - a process commonly known as patching - closes vulnerabilities before attackers can exploit them.
- Patching can also fix bugs, add new features, increase stability, and improve look and feel (or other aspects of the user experience).
- Visit NCSC guidance on Vulnerability Management for more informationhttps://www.ncsc.gov.uk/guidance/vulnerability-management.

Cloud Storage

- If your device is infected by a virus, malware or accessed by a cyber criminal your data may be damaged, deleted or affected by ransomware, preventing you from accessing it. A cloud service is useful because you are saving a copy of your data elsewhere, hosted by someone else out on the internet. This means that if your device is stolen/damaged/you have a fire or you suffer a ransomware attack, your data is not lost.
- Utilising cloud storage can ensure you will have a backup of all your important data and information.
- Visit NCSC Cloud Security for further guidancehttps://www.ncsc.gov.uk/collection/cloud-security.

Quick Tip:

Help prevent the accessibility of Siri whilst iPhones are locked. Go to *Settings>Siri & Search>Allow Siri when Locked>Disable*.

Smart Devices

With an increase in smart devices and new technology, it is important to be aware of the related risks of owning such devices.

Default Settings

- Some devices may be insecure when they are first switched on, so you'll need to take some quick steps to protect yourself.
- If your device comes with a default password, change it to a secure one. Usually, passwords can be changed in the application used to manage the device. More information on password protection can be found on page 6.
- Ensure your privacy settings are locked down. For more guidance visit: https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home.
- Activate Two-Factor Authentication if possible, see page 7 for more information.

Patching

Keep your smart devices secure by regularly updating them, and if available switch on the option to install software updates automatically so you don't have to think about it.

Using the latest software will not only improve your security, it often adds new features. Note that the software that runs your devices is sometimes referred to as firmware, so look for the words update, firmware or software within the app.

Risk

Just like a smartphone, laptop or PC, smart devices can be hacked to leave your data and privacy at risk. The NCSC are encouraging manufacturers to ensure their products are secure.

A code of practice has now been determined to help keep consumers safe whilst utilising new technology. Find the code of practice here:https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security

Quick Tip:
Check reviews of the product and manufacturer before purchase to ensure the product is what you expect it to be.

Password Protection

Passwords offer first line defence for potential cyber threats, ensure they are strong to deter the likelihood of an attack.

Password Guidance

- NCSC recommends that passwords are 12-26 characters long and include a mix of upper and lower case letters, numbers and special characters. A minimum of three random words should be utilised as the base of your passwords.
- Avoid predictable passwords or passwords that are somehow related to yourself e.g. date of births, names, pet names etc.
- Activate two-factor authentication and utilise biometrics if available. Both techniques add an extra layer of security to your accounts.

Change all Default Passwords

- Ask discussed in Smart Devices (page 5) it is important to change default passwords to deter unauthorised access to your device and accounts.

'Password Overload'

- Reusing the same password across different accounts can be dangerous. A cyber criminal may steal one of your passwords, and then access other accounts. This means they could break into several accounts despite only knowing one password.
- To help remember different passwords for your accounts, password managers are an application that can be downloaded on your device that stores your passwords securely, so you don't need to remember them all.
- For more information on password managers please visit https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online?curPage=/collection/top-tips-for-staying-secure-online/password-managers

Quick Tip:

Ensure your password is not on this list of the most common 100,000 passwordshttps://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt

Two-Factor Authentication

Activating two-factor authentication (2FA) provides a way of checking that you are really the person you are claiming to be.

However good your passwords are, they can only provide so much protection. They could be stolen from your service provider or your device. You could also get tricked into revealing them though social engineering. Therefore, it is important to utilise 2FA.

What is 2FA?

- 2FA offers an added layer of protection on important online accounts and is relatively easy to activate on many popular sites and applications.
- Accounts that have been set up to use 2FA will require an extra check, so even if a criminal knows your password, they won't be able to access your accounts.
- When setting up 2FA, the service will ask you to provide a 'second factor', which is something that you (and only you) can access. This could be a code that's sent to you by text message, or that's created by an app.

Implementing 2FA

- Activating 2FA on email accounts can help protect other sensitive information. For further information visit https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online?curPage=/collection/top-tips-for-staying-secure-online/activate-two-factor-authentication-on-your-email
- Since any 2FA is better than none, you should use 2FA wherever you can. It only takes a few minutes to set up for each account, and it's well worth it for the amount of additional protection it gives you.

Quick Tip:

Visit https://www.telesign.com/turnon2fa/tutorials/ for guidance on setting up 2FA on your online accounts

Social Media

It is important to be aware of your online presence and whether your settings on social media accounts are protecting you.

Privacy Settings

- When using social media, you should be aware of how widely you share personal information. This kind of data is often collected and used to refine cyber attacks.
- It is important to review the privacy settings on all you social media accounts and make sure you are happy with them.
- More information for popular sites can be found via the links below:

https://www.facebook.com/help/325807937506242/

https://help.twitter.com/en/safety-and-security/how-to-make-twitter-private-and-public

https://support.google.com/youtube/topic/2803240?hl=en&ref_topic=6151248

https://support.snapchat.com/en-GB/a/privacy-settings2

https://help.instagram.com/196883487377501

Location Settings

- By locking down your privacy settings, you will help secure your location settings.
- Ensure your location is not set to public. People can identify when you are away from home and may target your property.
- Ensure your location is only visible to those who you can trust.

Quick Tip:

Visit the NCSC link below for more information on how to use social media safely!
https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

Social Media

Knowing how to complete purchases online safely can help protect yourself from cyber criminals.

Digital Footprint

Digital Footprint is the information about a particular person that exists on the Internet as a result of their online activity.

It's worth exercising some caution when using social media. Not everyone using social media is necessarily who they say they are. Take a moment to check if you **know** the person, and if the friend/link/follow is genuine.

Criminals can use this publicly available information to steal your identity, or use it to make phishing messages more convincing.

You should:

- Think about what you're posting, and who has access to it. Have you configured the privacy options so that it's only accessible to the people you want to see it?
- Consider what your followers and friends need to know, and what detail is unnecessary (but could be useful for criminals).
- Have an idea about what your friends, colleagues or other contacts say about you online.

Quick Tip:

Test your digital footprint by searching for yourself through a clean browser, with no cookies or search history. You may need to add your location or current company name into the search bar if your name is reasonably common.

Online Purchasing

Knowing how to complete purchases online safely can help protect yourself from cyber criminals.

Encrypted Connection

The padlock sign located in your browser bar means that your connection is encrypted, so your personal information will reach the site without anyone else being able to read it. That's important if you're sending things like credit card details.

Site Legitimacy

Research sites before you use them to check other customer's experiences. If you go ahead with purchases use a credit card if you have one, as most major credit card providers insure online purchases. PayPal is also a secure payment method

Don't Divulge Too Much Information

- Be cautious if sites ask for details that are not required for your purchase.
- Fill in only mandatory details purchasing goods. These are usually marked with an asterisk*. If you can avoid it, don't create an account on a new site unless you will use it in the future. You can usually checkout as a guest. For more information visit https://www.ncsc.gov.uk/guidance/shopping-online-securely

Quick Tip:
Ensure you complete a factory reset before selling your phone to another. Doing so will prevent others getting unauthorised access to your data.

Email Accounts

Email accounts contain vast amount of personal information including log in details, password re-sets etc.

Passwords

- Cyber criminals can use your email to access many of your personal accounts and find out vital personal information, such as your bank details, address or date of birth.
- Having a strong, separate password for your email means that if cyber criminals steal the password for one of your less important accounts, they can't use it to access your email account.
- Go to page 6 for more information on how to formulate a secure password.

Consider using different emails for different purposes

- It is a good idea to consider using different email accounts for different purposes such as work, personal, online shopping etc. This spreads the risk and will also help you figure out what precisely may have fallen into the wrong hands if one of them is hacked.
- Only make your email available to trusted sources.

Account Recovery

- Utilise account recovery settings in case your account is targeted by offenders. Set security questions and answers which cannot be easily guessed, research and do not change over time.

Quick Tip:
Remember to turn on two-factor authentication to provide further protection on your email account!

Digital Parenting

Being aware of what your children are doing online can help protect them and your family.

Age Restrictions

- Be aware of age restrictions for applications that your child is utilising. Most social media sites have an age restriction of 13 years. Remember this when allowing your child to sign up for an account.
- Speak to your child about setting up accounts and profiles to ensure they do not create them without your consent. If your child creates a profile without your consent, speak to them about how they can protect themselves online.
- Age restrictions help protect your child from inappropriate content. Many applications and websites cannot verify an individual's age. However, you can manage accessibility through parental controls.

Parental Controls

- Parental controls are available on all Android, iPhone devices including location settings, purchases and downloadable content.
- Applications from the manufacturers store can be downloaded for further control inc. NannyNet and Quistodio.

Prevention

- Encourage sensible screen times and set boundaries especially at night time.
- Engage in their digital world, show an interest and understand their online activity.
- Educate your child about the dangers online and encourage them to speak to you if they are concerned about anything online.

Quick Tip:

Subscribe to Vodafone's Digital Parenting magazine for more advice
https://www.vodafone.co.uk/mobile/digital-parenting/archive

Experiencing an attack?

What should I do if I am experiencing an attack?

Complete Patching on all Devices
Update all manufacturer-approved updates on your devices to help mitigate any potential vulnerabilities. This may help prevent further attacks.

Utilise Account Recovery Processes
Most popular websites/ applications can recover accounts by providing information about yourself and answering security questions.

Change All Passwords
Change all your passwords and ensure they are different for every account. Download a password manager to ensure you remember all account details.

Notify Others
Notify your friends and family. Many criminals utilise your accounts to request money from others or spread malware. Be aware of who could be affected.

Financial Institutions
Notify your bank if you believe your debit/credit card details have been compromised.

Report all attacks to Action Fraud!
0300 123 2040
24/7 Live Chat
https://www.actionfraud.police.uk

Support

National Cyber Security Centre
https://www.ncsc.gov.uk/

Action Fraud
https://www.actionfraud.police.uk/

Take 5 to Stop Fraud
https://takefive-stopfraud.org.uk/

Get Safe Online
https://www.getsafeonline.org/

Turnon2FA
https://www.telesign.com/turnon2fa/

No More Ransom
https://www.nomoreransom.org/

The Cyber Helpline
https://www.thecyberhelpline.com/

Vodafone Digital Parenting
https://www.vodafone.co.uk/mobile/digital-parenting

Parent Zone
https://parentzone.org.uk