POLICE SCOTLAND
POILEAS ALBA

Cybercrime Harm Prevention Guidance for Scottish Environment Protection Agency (SEPA)

Version1.0 **12/01/2021**

1 CYBER SECURITY

1.1 Introduction

Cyber security is the means by which individuals and organisations reduce the risk of being affected by cyber crime.

Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access online - both at home and work - from theft or damage. It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online.

Cyber security is important because smartphones, computers and the internet are now such a fundamental part of modern life, that it's difficult to imagine how we'd function without them. From online banking and shopping, to email and social media, it's more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data, and devices.

If hackers get into your device or accounts, they could access your money, your personal information, or information about your business.

1.2 Cyber Security Top Tips

You can improve your cyber security by taking the following actions:

- Secure your passwords
- Turn on two-factor authentication (2FA)
- Update your devices
- Back up your data
- Securing your devices
- Social Media

1.2.1 Secure Your Passwords

Improve your password security

Hackers can get access to your account by using software to crack your password, by trying one password in lots of places or by trying to trick you into disclosing your password through scams.
Creating strong, separate passwords and storing them safely is a good way to protect yourself online.

1.2.1.1 Use a Strong and Separate Password For Your Email

If a hacker gets into your email, they could:

- reset your other account passwords
- access information you have saved about yourself or your business

Your email password should be strong and different to all your other passwords. This will make it harder to crack or guess.

Using 3 random words is a good way to create a strong, unique password that you will remember.

You should also protect your other important accounts, such as banking or social media.
How to change your password in:

- Gmail (opens in a new tab)
- Yahoo! Mail (opens in a new tab)
- Outlook (opens in a new tab)
- BT (opens in a new tab)
- AOL Mail (opens in a new tab)

If your email is not listed here, you should search online for advice from your provider on how to change your email password.

1.2.1.2 Create Strong Passwords Using 3 Random Words

When you use different passwords for your important accounts, it can be hard to remember them all. A good way to create strong, memorable passwords is by using 3 random words.

Do not use words that can be guessed (like your pet's name). You can include numbers and symbols if you need to. For example, *"RedPantsTree4!"*

1.2.1.3 Save Your Passwords in Your Browser

Saving your passwords in your browser will help you manage them.
Saving your password in your browser means letting your web browser (such as Chrome, Firefox, Safari or Edge) remember your password for you.

This can help:

- make sure you do not lose or forget your passwords
- protect you against some cyber crime, such as fake websites

It is safer than using weak passwords, or using the same password in more than one place.

Find out how to save your passwords in:

- Google Chrome (opens in a new tab)
- Microsoft Edge (opens in a new tab)
- Firefox (opens in a new tab)
- Safari (opens in a new tab)

1.2.1.4 How to protect your saved passwords

Make sure you protect your saved passwords in case your device is lost or stolen. Someone who gets access to your device may be able to use your saved passwords to access your accounts. This kind of cyber crime is much less common than remote attacks over the internet, where passwords are cracked using software.

To make sure you are protected, you should:

- turn off or lock your device when you are not using it
- use a strong password to protect your device
- turn on two-factor authentication for all your devices and accounts
- turn on biometrics (Face ID or Fingerprint recognition) if your device supports this

You should also back up your data regularly. This will help you recover your important information if your device is lost or stolen.

1.2.2 Turn on Two-Factor Authentication (2FA)

Two-factor authentication (2FA) helps to stop hackers from getting into your accounts, even if they have your password.

Some online banking uses 2FA automatically. It does this by asking for more information to prove your identity, such as:

- a PIN, password or code
- Biometrics - a fingerprint or face ID

How to turn on two-factor authentication (2FA)

You will need to manually turn on 2FA for most of your accounts. Not all accounts will offer 2FA. Online banking uses 2FA automatically. 2FA is also known as two-step verification or multi-factor authentication.

Turn on 2FA for email

- Gmail (opens in a new tab)
- Yahoo (opens in a new tab)
- Outlook (opens in a new tab)
- AOL (opens in a new tab)

Turn on 2FA for social media

- Instagram (opens in a new tab)
- Facebook (opens in a new tab)
- Twitter (opens in a new tab)
- LinkedIn (opens in a new tab)

1.2.3 Update Your Devices

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.

How to turn on automatic updates

Find out how to turn on automatic updates for:

- Apple - Mac (opens in a new tab)
- Apple - iPhone and iPad (opens in a new tab)
- Microsoft Windows 10 (opens your MS settings)
- Windows 7 is no longer supported. You should upgrade to Windows 10
- Android smartphones and tablets (opens in a new tab)
- Android apps (opens in a new tab)

1.2.4 Back Up Your Data

A cyber attack may mean you lose some or all of your data, such as pictures, documents, or financial or client information. Backing up regularly will help you get back on track. Backing up means creating a copy of your information and saving it to another device or to cloud storage (online). 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.

How to turn on automatic backup

How to turn on automatic backup for:

- Apple - Mac (opens in a new tab)
- Apple - iPhone and iPad (opens in a new tab)
- Android (opens in a new tab)
- Microsoft Windows 10 and Windows 8 OneDrive (opens in new tab)

1.2.5 Securing Your Devices

Devices like smartphones, tablets and PCs are getting more and more secure, but hackers are getting better at attacking them too. So if you've just bought a new device, or haven't looked at your security settings for a while, you should take some time to make sure you're protected against the latest threats. Fortunately, most manufacturers provide easy-to-use guidance on how to secure your devices.

We've provided some links to their advice below.

We recommend you take some time to go through these guides *(links lead to the relevant external websites)* every few months, or when you get a new device, to make sure you're protected.

- Apple
- Google (Android)
- Samsung
- Microsoft

1.2.6 Social Media

Social media is a great way to stay in touch with family, friends and keep up to date on the latest news. However, it's important to know how to manage the security and privacy settings on your accounts, so that your personal information remains inaccessible to anyone but you.

Advice from social media platforms

The following guidance is provided by each of the major social media platforms. Click to read detailed information.

- **Facebook**: basic privacy settings and tools
- **Twitter**: how to protect and unprotect your Tweets
- **YouTube**: privacy and safety
- **Instagram**: privacy settings and information

- **LinkedIn**: account and privacy settings overview
- **Snapchat**: privacy settings

Use two-factor authentication (2FA) to protect your accounts
Two-factor authentication (often shortened to 2FA) provides a way of 'double checking' that you really **are** the person you are claiming to be when you're using online services, such as social media, banking or email. Even if a criminal (or someone simply looking to cause mischief) knows your password, they won't be able to access any of your accounts that are protected using 2FA.

- The website Turnon2fa contains up-to-date instructions on how to set up 2FA across popular online services such as **Instagram**, **Snapchat**, **Twitter** and **Facebook**.
- For more information on why you should use 2FA wherever you can, read the NCSC's official guidance on two-factor authentication.

Understanding your digital footprint

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.

Less obviously, you should think about your digital footprint, which is a term used to describe the entirety of information that you post online, including photos and status updates. 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.

Although aimed at businesses, CPNI's Digital Footprint Campaign, contains a range of useful materials (including posters and booklets) to help understand the impact of your digital footprint.

2 DEALING WITH COMMON CYBER PROBLEMS/FAQs

2.1 Identity

Your identity is one of your most valuable assets. If your identity is stolen, you can lose money and may find it difficult to get loans, credit cards or a mortgage.

Your name, address and date of birth provide enough information to create another 'you'. An identity thief can use a number of methods to find out your personal information and will then use it to open bank accounts, take out credit cards and apply for state benefits in your name.

Please see the following common FAQ's for guidance and advice.

2.1.1 I have been hacked. How do I recover my account?

Social media, email or online shopping accounts, it doesn't matter what the service is, from time to time someone will find a way in.

If one of your accounts has been hacked, the step by step guide from NCSC will help you regain control and protect yourself against future attacks.

2.1.2 Should I Pay a Ransom To Unlock my Computer?

If your device has become infected with ransomware, you are encouraged **not** to pay the ransom.

If you do pay:

- There is no guarantee that you will regain access to your data/device
- Your computer will still be infected unless you complete extensive clean-up activities
- Attackers may assume that you would be open to paying ransoms in the future
- You will be funding criminal groups

Read NCSC advice on removing viruses and malware from your device.

2.1.3 My Username and Password Have Been Stolen.

Personal credentials, such as usernames and passwords, can be stolen directly from you by criminals using tricks such as phishing emails. They can also be stolen by hackers from the services you use, if they suffer a data breach.

If you suspect either has happened, you should change your password as soon as possible.
If you have used the same password on any other accounts, you should change it there too.

Services such as www.haveibeenpwned.com can tell you if your information has ever been made public in a major data breach, and even alert you if it happens in the future.

2.1.4 I Might Have Malware on my Device.

If you believe your laptop, PC, tablet or phone has been infected with a virus or some other type of malware, there are steps you can take.
Follow NCSC guide to remove viruses and restore your device.

2.1.5 I`ve Received a Suspicious Email,Call or Text.

Scam emails, calls and texts are a problem for everyone. They're getting more convincing day by day.

Read NCSC advice on spotting and dealing with suspicious emails, calls and texts.

2.1.6 I`m Worried my Banking Details May Be Stolen.

- Contact your bank or building society and speak to their fraud department.
- Your bank will **not** ask you to reply to an e-mail with personal information, or details about your account. If you contact them, use a phone number/email address you have found yourself, rather than one sent to you in the email – it may be false.
- You can check your credit reference file online. You should follow up on any unexpected or suspicious results.

For more guidance on protecting yourself from cyber-enabled fraud, please visit Take Five.

2.1.7 What Signs Should I Look Out For?

There are a number of signs to look out for that may mean you are or may become a victim of identity theft:

- You have lost or have important documents stolen, such as your passport or driving licence.
- Mail from your bank or utility provider doesn't arrive.
- Items that you don't recognise appear on your bank or credit card statement.
- You apply for state benefits, but are told you are already claiming.
- You receive bills or receipts for goods or services you haven't asked for.
- You are refused financial services, credit cards or a loan, despite having a good credit rating.
- You receive letters in your name from solicitors or debt collectors for debts that aren't yours.

2.1.8 How do I Reduce the Risk of Identity Theft?

- Store any documents carrying personal information – such as your driving licence, passport, bank statements, utility bills or credit card transaction receipts – in a safe and secure place.
- Shred or destroy your old documents so that nothing showing your name, address or other personal details can be taken.
- Monitor your credit report and regularly check your credit card and bank statements for suspicious activity.
- When you move house, contact your bank, credit and store card providers, mobile phone provider, utility providers, TV licensing, your doctor and dentist etc, and give them your new address – you don't want the new tenants to have access to letters containing your personal information. You can also redirect your mail by contacting Royal Mail.
- Remember, less is more. The less you give away about yourself, the lower the risk of information falling into the wrong hands.
- Think before you buy online – use a secure website which displays the company's contact details, look for a golden padlock symbol and a clear privacy and returns policy. Check the web address begins with https.

2.1.9 What can I do if I`m the Victim of Identity Theft?

If you think you are a victim identity theft or fraud, act quickly to ensure you are not liable for any financial losses.

- Report all lost or stolen documents, such as passports, driving licences, credit cards and cheque books to the organisation that issued them.
- Inform your bank, building society and credit card company of any unusual transactions on your statement.
- Request a copy of your credit file to check for any suspicious credit applications.
- Contact CIFAS (the UK's Fraud Prevention Service) to apply for protective registration. Once you have registered you should be aware that CIFAS members will carry out extra checks to see when anyone, including you, applies for a financial service, such as a loan, using your address.

  CIFAS – The UK's Fraud Prevention Service
  6th Floor
  Lynton House
  7 - 12 Tavistock Square

London
WC1H 9LT
www.cifas.org.uk

- To report the theft or loss of post and other important documents:
  Royal Mail
  Telephone: 08457 740 740

- Police Scotland Call 101 for advice and support (or call 999 in an emergeny)

You can also get more advice at:

- Police Scotland Fraud Advice Leaflet
- Bank Safe Online
- Take Five
- Financial Ombudsman Service

3 SUPPLEMENTARY

3.1 Resources

Please see resources you may find useful.

3.1.1 NCSC Infographics

The NCSC have produced infographics covering technical guidance for organisations and their staff to keep safe online. Please click on the following links to download them in pdf format.

- Stay safe online: top tips for staff
- Protect devices from viruses and malware
- Phishing attacks: dealing with suspicious emails
- Using passwords to protect your devices and data
- Sextortion phishing scams: how to protect yourself
- A guide to recovering your hacked online accounts
- Video conferencing: using services securely
- Bring Your Own Device
- Homeworking: managing the cyber risks
- Business email compromise: dealing with targeted phishing emails

The full list of infopgraphics is avaible at the NCSC website.

3.1.2 NCSC e-learning Training Package

The NCSC has produced a new e-learning training package: 'Stay Safe Online: Top Tips for Staff'. It's totally free, easy-to-use and takes less than 30 minutes to complete. The training introduces why cyber security is important and how attacks happen, and then covers four key areas:

- defending yourself against phishing
- using strong passwords
- securing your devices
- reporting incidents ('if in doubt, call it out')