Online Safety Advice for Parents and Carers

Cybercrime Harm
Prevention Unit, Police Scotland

10/08/2021

Table of Contents

1 Staying Safe Online 2
1.1 Introduction 2
1.2 Cyber Security Top Tips 2
1.3 Staying Safe Online (Children) 2
1.4 Online Gaming 3
1.5 Parental Controls 4
1.6 Buying and Selling Devices 4
1.7 Social Media 4
1.8 Understanding your digital footprint 5
2 DEALING WITH COMMON CYBER PROBLEMS/FAQs 5
2.1 Identity 5
2.1.1 I have been hacked. How do I recover my account? 6
2.1.2 Should I Pay a Ransom To Unlock my Computer? 6
2.1.3 My Username and Password Have Been Stolen. 6
2.1.4 I Might Have Malware on my Device. 6
2.1.5 I`ve Received a Suspicious Email,Call or Text. 7
3 SUPPLEMENTARY 7
3.1 Useful Links and Further Information 7
4 CYBER SECURITY COURSE 8
4.1 Introduction 8
4.2 Police Scotland Digital and Data Skills Academy 8
4.3 NCSC Cyber Career (National Cyber Security Centre) 8
4.4 Young Scot 8
4.5 FutureLearn 8

1 Staying Safe Online

1.1 Introduction

The internet is a useful tool for shopping, staying in touch with friends, sharing experiences and exchanging content. However, there are some potential risks such as; Disclosure of private information (either by you or your contacts), Emails and messages that seem to be from friends or social networking sites but are actually luring you to fraudulent sites.

Online fraud and computer misuse crimes are on the rise and can be prevented by making a few small changes in online behaviour.

To avoid becoming a victim of online crime, developing a few good online habits drastically reduces your chances of becoming a victim of cybercrime, makes you less vulnerable and lets you use the web safely.

1.2 Cyber Security Top Tips

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

- Use a strong password or passphrase, which is at least 12 characters long and contains a mixture of letters, numbers and symbols
- Never give personal or sensitive details out online or over email
- Make sure all devices have up-to-date anti-virus software and a firewall installed
- Keep software and apps regularly updated
- Only download from legal, trusted websites
- Only open emails and attachments from known and trusted sources
- Look for the padlock icon in the address bar when paying for goods or services online – it means the website is trusted and secure
- Check the address starts with https:// whenever you're asked to enter sensitive information online
- Avoid using public Wi-Fi hotspots that are not secure or ask you for personal information to access it
- Regularly back up your data
- Control your social media accounts – regularly check your privacy settings and how your data is being used and shared
- Be cautious of internet chats and online dating – there's no guarantee you're speaking to who you think
- Be extremely cautious if you're asked for money

Visit Cyber Aware for step-by-step instructions on keeping your devices up to date with t he latest security updates, and for more online security advice.

1.3 Staying Safe Online (Children)

The internet is a fantastic place for children to learn, create and have fun, but they may occasionally have to deal with a variety of sometimes challenging issues.

These might include cyberbullying, the pressure to take part in sexting, encouragement to self-harm, and viewing pornography, along with various others. But there are positive things you can do to equip yourself and your child, support them in resolving any issue they may face.

Behind every device that allows and provides connectivity and communication online from social media platforms, gaming, messaging there is a human element, within that element are some who masquerade as someone else, a different gender, a different age group etc. in an attempt to lure, coerce, exploit, intimidate and do harm to our Children and young people.

As a Parent/ Carer, you can find support to enhance your Children or young people's safety, security and awareness at a time when they will be spending more time online. Please have a look at the links below which are very informative, easy to follow and will provide the opportunity to start the discussion about online safety.

Thinkuknow is the online safety education programme from the National Crime Agency and their website has home activity packs from the ages of 4yrs to 14+yrs to take support from.

NSPCC, CEOP and Internet Matters have created a number of advice hubs to help you learn more and deal with these issues with your child. Please click on the following links for more details.

1.4 Online Gaming

Gaming is a great way for young people to relax, socialise with their friends and have fun. Children can play on games consoles, apps or websites, mobiles, tablets, PCs, or through smart speakers and virtual reality headsets. They can also chat to other players using messaging platforms for gamers or watch livestreams of well-known gamers.

You can find out more about the different types of games children like to play on Net Aware.

For those with younger family members to think about, online gaming can be a concern. From cyberbullying, to excessive time spent playing games, to unscrupulous games which encourage children to pay for content.

Here are some useful links to sources of information to explain and understand the world of online gaming and encourage children to game safely and responsibly online.

- National Cyber Security Centre Online Gaming Advice
- Thinkuknow Gaming: What parents and carers need to know.
- Internet Matters: Online gaming safety tips for parents
- Internet Matters: Advice on Buying a games console for your child
- Net Aware: Reviews and advice of sites, apps and games.

- UK Interactive Entertainement PLAY has step by step guides for parents

1.5 Parental Controls

Parental controls put you in control of what content your child can see. Combined with privacy settings these can help you protect your children from the things they shouldn't see or experience online.

Internet Matters have guides for step-by-step instructions to set controls on popular entertainment services & search engines.

Internet Matters also have step by step guides to help you set up the right controls and privacy settings on the networks, gadgets, apps, and sites they use to give them a safer online experience.

1.6 Buying and Selling Devices

The NCSC have advice on how to erase the personal data from your phone, tablets, and other devices (and why it's important when you're buying and selling them).

Our devices - and especially our smartphones - contain more work, personal and financial data than ever before. If you are selling, giving away, or trading in your smartphone (or other device), you should erase all of this personal data so it doesn't fall into the wrong hands. If you've just bought a second-hand device, there is also advice included about what to do before you start using it.

1.7 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.

1.8 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.

The Information Commissioners Office (ICO) is the UK's independent body set up to uphold information rights. ICO state that it's your right to be informed about how organisations are using your data, even if it happens behind the scenes. This includes understanding how people use your data to target you with social media adverts.ICO have created a number of resources to help you understand your rights with regards to your online data.

ICO have further guidance on social media privacy settings and factsheets on some of the most popular social media platforms (Facebook, Twitter, Snapchat, LinkedIn and Google) to assist you in taking control over how your personal information is used.

LSE (London School of Economics) have developed toolkits for young people and also for parents to help them talk to children about their data and privacy online, including data protection, the digital economy and a range of privacy issues.

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.

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

3 SUPPLEMENTARY

3.1 Useful Links and Further Information

- **Think you Know:** An education programme for advice about staying safe when you're on a phone, tablet or computer. www.thinkuknow.co.uk
- **Home Activity Packs**: Download home activity packs with simple 15-minute activities for your child to support their online safety at a time when they will be spending more time online at home. www.thinkuknow.co.uk/parents/Support-tools/home-activity-worksheets
- **Internet Matters:** Get expert support and practical tips to help children benefit from connected technology and the internet safely and smartly. www.internetmatters.org
- **Project Evolve:** Resources to equip children and young people for digital life. www.projectevolve.co.uk
- **UK Safer Internet Centre:** Promote the safe and responsible use of technology for young people and provide online safety tips, advice and resources to help children and young people stay safe online. www.saferinternet.org.uk
- **Childline:** Childline is a free and confidential service for children and young people. You can phone them on 0800 11 11 or you can visit their website www.childline.org.uk
- **NSPCC:** If you are an adult and worried about a child you can call the 24-hour NSPCC helpline on 0808 800 5000 or visit their website. www.nspcc.org.uk
- **ParentLine Scotland:** Call 08000282233 or email: parentlinescotland@children1st.org.uk Parent Line's opening hours are from 9am-10pm (Mon-Fri) and 12 noon-8pm at weekends.
- **Crimestoppers:** Call 0800 555 111 or visit their website www.crimestoppers-uk.org
- **Police Scotland:** Call 101 for advice and support (or call 999 if you think a child is in immediate danger). www.scotland.police.uk

- **Internet Watch Foundation:** Report remove nude images shared online.

4 CYBER SECURITY COURSE

4.1 Introduction

The following courses are free to access and provide industry recognised qualifications. Have a look and see if any interest you.

4.2 Police Scotland Digital and Data Skills Academy

The industry standard courses available within the academy are provided for free through the Cisco Academy and contains training and qualifications in Networking, Cyber Security and Programming Languages.

Please feel free to enrol in the courses to take advantage of this valuable opportunity. The link to the website is below

Digital and Data Skills Academy - Police Scotland

4.3 NCSC Cyber Career (National Cyber Security Centre)

CyberFirst courses - NCSC.GOV.UK

4.4 Young Scot

https://young.scot/campaigns/national/digi-know-learning-opportunities

4.5 FutureLearn

Cyber Security Careers Advice (futurelearn.com)

https://www.futurelearn.com/courses/introduction-to-cyber-security

https://www.futurelearn.com/courses/cyber-security-landscape