Safe and Secure Online Awareness

How can you stay safe online?

- **Supported Operating Systems.** Ensure it is up to date and it's recommended that you have auto updates switched on.
- **Internet Security Software.** Any internet enabled device should have anti-virus installed, including Apple devices. Check that firewalls are enabled.
- **Anti-spyware & Malware Software.** Strongly advise to also have these installed on internet enabled devices.
- **Keep a safe backup.** Regularly create a backup of your important files (such as photos, documents and other files that cannot be replaced) on a USB stick, separate hard drive or cloud service.
- **Multifactor Authentication (MFA)** or 2fa two factor authentication is the process of using more than one way of securing an account, for example not just using a password but also maybe a Pin, passcode, smartcard or biometrics.

National Cyber Security Centre

www.ncsc.gov.uk

Passwords

- Current best practice advises **THREE RANDOM WORDS**. To add complexity, convert some letters to numbers and add special characters,
  For example : **gravitydecadetheatre**
  To add complexity : **Gra/1tyDe(ad3Th3atr3**
- Your single most important account and password is your email – effectively, anyone taking control of your email can then reset all your other passwords locking you out.
- Don't use words/names/information that may be in the public domain or easily worked out from social media content, such as Mother's maiden name; Date/Place of birth; pets names; children's names; teams you support etc.
- **Never** share passwords or disclose your password to anyone else
- **Always** change default passwords on **all** SMART devices/routers for your own unique one
- **ALWAYS** log out of sites – especially on shared/public devices/machines
- **NEVER** reuse passwords!
- Consider using a password manager and two factor authentication

Password managers store your login information for all the websites you use and help you log into them automatically. They encrypt your password database with a master password – the master password is the only one you have to remember.

How secure is your password?

www.howsecureismypassword.net

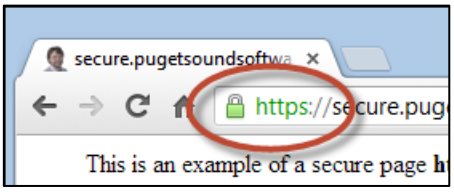
Beware RansomAware!

- Malicious software (malware) that attempts to extort money (tokens/bitcoins generally)
- The ransomware will either “lock” the computer to prevent usage, or will encrypt the files contained on it barring access to them
- Ransomware generally occurs when a link in an email and /or email attachment is opened allowing the malware to be installed
- Don’t pay extortion demands as this only feeds into criminals’ hands and there’s no guarantee that access to your files will be restored if you do pay. www.nomoreransom.org advice if you have been infected with ransomware.

Online Shopping Dangers.

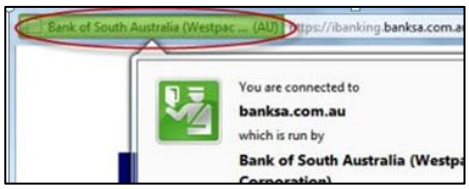
- Research your retailers and choose reputable sellers and buyers..
- Pay by credit card where possible, gives you more protection.
- Always read reviews and ratings
- Only use apps from authorised app stores and always log out of sites.
- Never send money by transfer to someone you don’t know and never transfer money for other people (Money Muling).
- Be aware when donating to charity, always check them out frst!
- Check the website is secure (below).

Make sure you’re on a secure website…



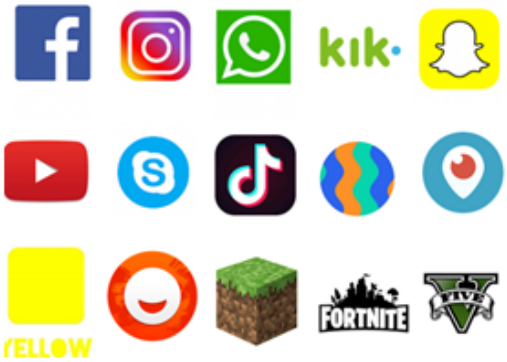
- Look out for the secure padlock symbol.
- The address in your address bar should begin https:// rather than http://. The S stands for secure.
- Part of your address bar might turn green. This depends on your browser and the website, but it’s generally a good sign. Clicking on it will give details of the site’s Security.

VPN (Virtual Private Network) =
allows you to create a secure connection to another network over the Internet. VPNs can be used to access region-restricted websites, shield your browsing activity from prying eyes on public Wi-Fi, and more.



Public Wi-Fi

- Any device connected to a Wi-Fi hotspot can view traffic sent & received by everyone else?
- A malicious hacker could sit in a coffee shop with a flat white and carry out all manner of attacks to intercept data as unsuspecting customers access online banking or chat on social media
- Enterprising criminals can even set up their own hotspots with the primary goal of capturing personal data.



App guide:
https://smartsocial.com/app-guide-parents-teachers/

Sites, apps & games (NSPCC):
https://www.net-aware.org.uk/networks

Gaming:
https://www.commonsensemedia.org/game-reviews

Apps and downloading.

- Only **download** apps from a **reputable** app store and read other users' reviews of apps.
- **Read** through an app's privacy policy to ensure that it will not share personal information.
- **Permissions** – Check to see exactly what the app is accessing on your device.
- **Never click** on unknown links.
- **Use** mobile anti-virus/malware products.

Securing your devices

Take time to make sure you're protected against the latest threats. Check these links to make sure your devices are secure:

Apple https://www.apple.com/uk/privacy/control/

Google https://safety.google/security/security-tips/ (android smartphones)

SAMSUNG https://www.samsung.com/global/galaxy/security/

Microsoft https://support.microsoft.com/en-ae/help/4013263/windows-10-stay-protected-with-windows-security

Looking after your personal information

- Limit the amount of information made publicly available – see how much information you can find on yourself online
- Check www.ukphonebook.com and www.192.com for your information – it may be a lot more than you realise, including DOB, occupation etc.
- Carefully read the options when subscribing for anything – they can be misleading. Ensure you opt OUT of sharing your information
- Have you opted to go on the edited Electoral Register so that your home details are not public?
- Make sure you back up your data (i.e. photos and contact details etc.) on all devices
- Consider installing or activating tracking software/apps in the event of loss or theft
- Be aware that your phone may be geo tagging your photos!
- Wherever possible, accept multi factor authentication for any apps or sites you log in to

Check to see if your email has been breached, if so, chance your password or delete your account if no longer needed.

Have you been owned? www.haveibeenpwned.com

How do I know what information is out there?

Quite simply, Google yourself! Also try searching yourself on www.pipl.com, www.yell.com or www.192.com.

Other steps to take :

- Change Facebook settings make old Timeline posts visible only to you
- Check that photos are not “publicly available”
- Opt to approve photos and posts by others before they appear on your timeline
- Delete any old social media accounts you no longer use
- Spring clean and remove any posts that may not show you in a positive way

Google Alerts is a great way to set up a virtual personal watchdog that will constantly look for attempts at identity theft. This is much better than checking these values by hand periodically, since Google Alerts lets you set it and forget it. You'll be notified as soon as a thief posts your data online for others to use.

www.google.co.uk/alerts

5 top tips….

Too much information.
Social networks let you post all kinds of information. The more information you put online the more people can find out about you. Some people might use this to bully you or contact you and lie about being into the same things as you.

- Don't post anything you don't want everyone to see
- Be aware and concerned about potential dangers
- Check your privacy settings
- Check your device settings

Digital footprints.
A trail of information that people leave online or using other communication devices. The problem is things you post on social networks can be difficult to delete – other people could have copied them or shared them. Will you want things you post today to be hanging around in a few years' time?

- Favourite apps
- Websites visited
- Messages sent
- Videos downloaded
- Pictures uploaded
- Music listened to
- Games played
- Comments posted

It's easy to lie online.
Some people set up fake profiles on social networks. They even pretend to be girls or boys your age when actually they're much older. It can be really hard to tell the difference between someone who's genuine and a fake.
Don't trust anyone! Liars…

- Are less likely to use "I"
- Often use negation (happy-not sad, exciting-not boring
- Tend to write shorter profiles
- Likely to avoid discussing their appearance

Anti-social networking.
Just as social networks can be used to share lots of great information about yourself and stay in touch with all your friends – they can also be used to share nasty things - embarrassing pictures, horrible comments, fake profiles – and say nasty things to people. Is your online life real?

I did NOT want to see that.
Anyone can post videos, pictures or ideas on social networks – nice or nasty. That means you might see things you wish you hadn't

- Child sexual abuse material
- Illegal hate speech / cyberbullying
- Incitement to terrorism
- Copyright infringement
- Consumer protection online

Stop! Block! Report! Tell!

Keeping children safe online - What can parents/guardians do?

- **Be aware of what your children are doing online**
  Show interest in their online activities and talk with them about what they do on the web. They might not tell you everything, but it doesn't mean you shouldn't ask. Spend time with them to understand what channels they are following on YouTube and other social media sites.

- **Discuss the internet**
  Explain to your young people what you consider to be an appropriate use of the internet, which will help you support the reasons that they are online, Expression, Creativity, Problem solving, Education, Entertainment

- **Make a clear set of rules**
  Make house rules relating to some technology you may have, e.g. no phones at the dinner table, no devices before bedtime etc. Consider writing them down and displaying them close to a computer they may use. Why not challenge them to a duel; If your young people like playing console or online games, ask if you can play too. When you respect their interests they're more likely to respect your rules.

- **Teach the importance of being cautious**
  Particularly when they are chatting or corresponding with people they don't know./ Discuss with them that all they are told and read online may not be true! (fake news)

- **Be sure they understand 'personal information'**
  Be clear that they understand what information is inappropriate to be sharing online, like their name, home address, dob, school name, contact numbers, passwords.

- **Invent an online nickname**
  Explain that they should use this nickname rather that their real name when they are playing game, using virtual worlds or on sites where they may be chatting with people online.

- **Emphasise 'never meet someone they've met online'**
  They should never arrange to meet with someone they met online and that they should let you know if someone online tries to arrange a meeting with them.

- **Make sure they know where to go for help and support**
  Be clear that yourselves, other relatives, teaches etc. are here to help. Schools promote CEOP reporting tools and childline (www.childline.org.uk) can offer them support. Get them to understand that somethings they may see or that happens online maybe difficult to talk about but there are people to talk.

NSPCC www.nspcc.org.uk/keeping-children-safe/online-safety

internet matters.org www.internetmatters.org/schools-esafety/primary/parent-support

Phishing emails

- From your 'bank' asking you to update your information or your account will be closed
- From a well-known software company asking you to update your account details or install a programme on your computer
- An email saying you have won some kind of lottery or inherited a large amount of money
- An email supposedly from someone that you may know asking for money because they are stranded somewhere or need medical assistance

Internet/Online Scams

There is a huge crossover between Fraud and Cyber crimes!

http://www.derbyshirescamwatch.org.uk/

CHECKLIST

- ❒ Check Operating Systems are supported and running the latest version (Windows 9 & above!) If you are still using Windows Vista or XP, you must upgrade as a matter of urgency!
- ❒ Check Firewalls, Antivirus, Antimalware and Antispyware installed up to date and running
- ❒ Check your passwords are secure enough and not used across platforms
- ❒ Check your digital footprint
- ❒ Check UK Phonebook & 192.com for entries in your name – request removal
- ❒ Check your social media settings
- ❒ Check your email address with www.haveibeenpwned.com
- ❒ Ensure your home router has a password set, if the original default, change it
- ❒ Don't use public Wi-Fi for sensitive transactions such as banking/social media/email unless you're using a VPN (Virtual Private Network). Alternatively, revert to 3G/4G/5G on your device

If you think you're a victim: Report it to Action Fraud by calling 0300 123 2040 www.actionfraud.police.uk.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

www.saferderbyshire.gov.uk/MOT

Online safety on all areas for everyone :

GetSafeOnline	www.getsafeonline.org

CEOP online safety for under 18s, parents and schools :

CEOP (report online grooming)	www.ceop.police.uk
ThinkUknow	www.thinkuknow.co.uk

Online safety for under 18s, parents and schools :

UK Safer Internet Centre	www.saferinternet.org.uk
Know the Net	www.knowthenet.org.uk
NSPCC	www.nspcc.org.uk
	www.net-aware.org.uk

Action Fraud	www.actionfraud.police.uk
Advice on fraud and scams	www.takefive-stopfraud.org.uk/

Victim support/services

Derbyshire Victim Service	www.derbyshirevictimservices.co.uk
Got Your Back (under 18)	www.gotyourback.tv

Have you been pwned?	www.haveibeenpwned.com
Pipl (people search)	www.pipl.com
Internet Watch Foundation	www.iwf.org.uk

(report child sexual abuse and non-photographic child sexual abuse images)

If you need further advice or guidance:

James Land –
Cyber Prevent & Engagement Officer (Digital PCSO)

james.land.4513@derbyshire.pnn.police.uk

www.derbyshire.police.uk/cybercrime

Advice/info.: www.bit.ly/digitalpcso

#protect yourself online

safe & secure
#DerbyshireOnline

@DigitalPCSO

DERBYSHIRE ALERT **www.derbyshirealert.co.uk**