

Being safe and legal online

You need to understand that:

- There are **risks and threats** involved in carrying out activities online and security is important. However, don't get this out of proportion; staying safe is mostly a question of **common sense**. You wouldn't give a copy of your front door key to anyone who asked for it!
- **Viruses** can damage your computer and security software should be used to prevent this.
 - ☺ A computer **virus** is a piece of computer code which is capable of copying itself and typically has a harmful effect, such as corrupting the system or destroying data.
- Your online activity produces a **permanent record** which could be accessed by others and used both now and in the future. Don't put anything online that might come back to haunt you!
- Others can **capture** and use your data maliciously e.g. for identity theft. You can protect and secure your personal data against such threats through privacy settings.
- You must not **share** other people's data, e.g. photos, online without their consent.
- It is important to keep your computer systems and security software **up to date**.
 - ☺ Software providers work constantly to improve their systems and to remove security loopholes. You will usually be prompted to install these **updates** and you should act accordingly.

Can you:

Set automatic updates in the settings menu for the computer operating system and security software?	
------------------------------------------------------------------------------------------------------------	--

☺ To make life even easier for you, some providers make it possible for updates to take place automatically when you are connected to the internet.

Keep secure the information you use to access your online accounts?	
----------------------------------------------------------------------------	--

☺ You should use different and secure **passwords** for your accounts and ensure that online login information is not shared with anyone.

Ensure your posts on social media are not offensive or inappropriate ?	
--------------------------------------------------------------------------------------	--

Ensure that nothing is posted on social media about others, including children, without their permission ?	
--------------------------------------------------------------------------------------------------------------------------	--

Identify secure websites by looking for the padlock and https in the address bar?	
--------------------------------------------------------------------------------------------------------	--

☺ **HTTPS (Hyper Text Transfer Protocol Secure)** is the secure version of the way by which data is sent between your browser and the website that you are connected to. It means all communications between your browser and the website are **encrypted** so that they cannot be read by anyone who intercepts them.

Create passwords which are difficult for others to guess?	
------------------------------------------------------------------	--

☺ See the section on **passwords**.

Set privacy settings on your social media and other accounts?	
----------------------------------------------------------------------	--

☺ Make sure that only those people that you want (e.g. friends or family) can see posts and shared content.

Respond to requests for authentication for your online accounts and email?	
-----------------------------------------------------------------------------------	--

☺ **Two-factor authentication** is a method of confirming your claimed identity by using a combination of two things:

- (a) something you **know** e.g. a password
- (b) something you **have** e.g. a bank card or mobile phone
- (c) something you **are** e.g. fingerprint or iris scan

A good example of two-factor authentication is the withdrawal of money from an ATM; only the correct combination of a PIN (a) and a bank card (b) allows the transaction to be carried out.

Often when changing a password you need the old password (a) and a onetime only code contained in a message sent to your mobile phone (b).

☺ **Useful web pages:** <https://www.getsafeonline.org/>
<https://www.ageuk.org.uk/>

Recognise suspicious links in email, websites, social media messages and pop ups?	
------------------------------------------------------------------------------------------	--

☺ Clicking on these links or downloading unfamiliar attachments could put you and your computer **at risk**.

Activate pop-up blockers on your web browser to reduce the threat from malicious sites?	
------------------------------------------------------------------------------------------------	--

☺ Pop-up ads or “pop-ups” are forms of online advertising on the Web. A pop-up is usually a small window, that suddenly appears ("pops up") in front of the window you are looking at on your device.

Ensure that any information or content is backed up frequently?	
------------------------------------------------------------------------	--

☺ **Backing up** means making a copy and storing it separately either in the cloud or on an external storage device.

Acknowledge that you cannot take and use content from the web that belongs to others without consent ?	
---------------------------------------------------------------------------------------------------------------	--

☺ Online material may be subject to **copyright** and intellectual property legislation.