eSafety

When we are online you can easily share personal information with other people but you need to be careful. You need to watch out for spam emails and protect your private information.

The internet
Be careful when sharing personal information online. Only use websites you trust. Personal information includes:

- full name
- date of birth
- address

This information can be used to steal your identity or to find you in the real world. Identity theft is where someone pretends to be you. They might shop online spending your money, or take out loans in your name.

Status updates, comments and photos
Where possible, limit access to your social media profiles to family and friends. Do not post inappropriate status updates, comments or photos online. You might not want certain people, such as potential employers, to gain access to them.
Social networking sites also frequently change their privacy policies. This means that the way your information is used can change, a danger which often draws criticism.

False information and unsuitable content
The internet is a great source of information but some of it is incorrect, out of date or **biased**. Always check multiple sources, ie other websites or written material, to confirm what you've read is correct.

No one is in charge of the internet so anyone can post or publish anything to it. Some content may be unsuitable. Websites that you can trust include those from:

- the Government – if the address has 'gov.uk' in it, it's a UK Government website
- the National Health Service (NHS) – if the address has 'nhs.uk' in it, it's an NHS website
- the Police – the official website is www.police.uk
- the BBC – all of the BBC's websites have 'bbc.co.uk' in their address

Wikipedia

Wikipedia is an online encyclopaedia that anyone can edit. It has its pros and cons. It's full of useful, up-to-date information, but because anyone can edit it, it's easily abused.

Know who you're talking to

Email, instant messaging, social networking sites and video chat are great for keeping in touch with family and friends, but make sure you know who you're talking to. People may not be who they claim to be. They might try to get personal information from you or ask you to do something that makes you uncomfortable. Others may try to wind you up or be unnecessarily aggressive. This is called trolling and flaming.

Ignore emails and friend requests from people you don't know and never meet up with someone you don't know.

File sharing, cyberbullying and smartphones

File sharing

File sharing is very popular but beware of fake files, **malware** and **copyrighted material**. Internet service providers (ISPs) may reduce your internet speed or disconnect you entirely if you repeatedly download files protected by copyright. They are able to track what you download using your **IP address**. Every computer has a unique IP address.

Cyberbullying

Using technology to bully someone is called cyberbullying. Cyberbullying can involve one or more of the following:

- sending offensive texts or emails
- posting lies or insults on social networking sites
- sharing embarrassing videos or photos online

If you're being bullied, tell someone. For more advice visit **Think U Know**.

Smartphones and mobile devices

These allow for photos, videos and your location to be shared instantly on the internet. Be careful what you get up to in public as anyone might have a smartphone pointed at you. Do not post photos or videos of other people online without their permission.

Location-aware applications

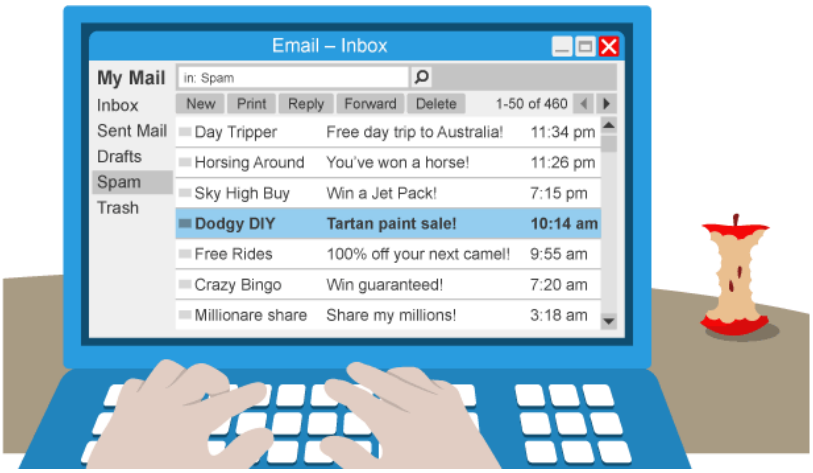
There are many websites and **mobile applications** that share your location. Some of the popular ones include:

- Facebook
- Foursquare
- Twitter

It's wise not to share your location. Especially on websites that are accessible by anyone.

Spam email and phishing

Nearly everyone has an **email address**. Email is a useful tool at home and in work but spam and junk mail can be a problem. Spam emails offer all kinds of things like money, prizes and very low prices for products that are normally very expensive. They can contain **malware** too.



Spam is very difficult to avoid but there are ways to reduce it:

- Use a spam filter – most email clients try to stop spam from reaching you by using a spam filter. It recognises common spam emails and stops them from getting through. Check your spam email regularly as sometimes real emails are mistaken for spam.
- Do not give your email address out – if you don't trust the website or if supplying your email address is optional, don't give it to them.
- Keep an eye out for tick boxes – when you sign up to a website, it might try to sign you up to its **newsletter**. Read the small print next to the tick boxes carefully.

Phishing

Trying to trick someone into giving out information over email is called 'phishing'. You might receive an email claiming to be from your bank or from a social networking site. They usually include a link to a fake website that looks identical to the real one. When you log in it sends your username and password to someone who will use it to access your real accounts. They might steal your money or your identity.

Your bank will never send you an email asking for your personal information or your username and password.

Malware and security

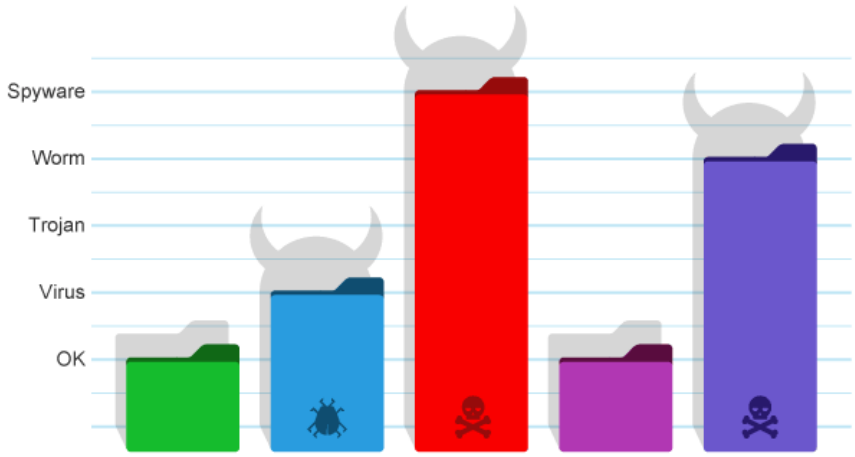
Malware is a general term that describes lots of different programs that try to do something unwanted to your computer. Anti-virus software prevents malware from attacking your computer or mobile device. There are free anti-virus applications available:

- AVG
- Avast!
- Microsoft Security Essentials

There are also applications that you have to pay for:

- Norton
- McAfee
- Sophos

There are many types of malware:



- A **virus** harms your computer in some way, usually by deleting or altering files and stopping programs from running.
- A **trojan** starts by pretending to be a trusted file, but gives **unauthorised access** to your computer when you run it.
- **Worms** are difficult to get rid of. They copy themselves over networks to **external storage devices**
- **Spyware** collects information from your computer and sends it to someone.
- **Scareware** tricks you into thinking it's software that you need to buy.

Firewall

A firewall monitors connections to and from your computer. If it spots something suspicious, it closes the connection or disconnects it. Most operating systems include a firewall and it should be turned on by default.

Hackers, people who try to gain access to your computer without your permission, will have a harder time if your firewall is enabled.