SKILLS FOR TOMORROW

Online safety - jargon buster

Boost your knowledge of common techy terms relating to online safety and harms. You'll build confidence and awareness to help protect yourself from getting caught out.

Words which appear in **bold like this** are also terms explained in the jargon buster.

If you are using this within a group, you might want to talk through the terms and meanings. You could then have a go at the **online safety word search** for a bit of fun!

Term	Meaning
Antivirus	Security software that helps protect your computer from online **viruses.**
Autofill	Autofill is a software function that automatically enters data in forms on websites and spreadsheets for you.
Bot	Is a type of software application that performs tasks over and over. You might come across a chatbot on a customer service site, or there are malicious bots that spread **spam** content.
Cloud	Allows us to save and access our files through the internet anywhere in the world on any device.
Cookie	A cookie is a small amount of data created by a website that remembers information about you.
Cyber attack	Is a digital attack that targets computer systems, networks, or personal devices, like your computer, tablet or smartphone.
Digital / Secure key	Often used for online banking as an extra level of security. Will give you added protection against the threat of **fraud**.
Email	A way of sending messages and files to someone electronically.
Encryption	Encoding data to make it more secure. It can help to prevent theft of your information by ensuring the data can only be accessed with a **digital key/ password.**
Firewall	A firewall is software that provides protection against external cyber attacks

Term	Meaning
Fraud	A crime in which someone tricks somebody else to get **personal information** or bank details unfairly or illegally. They often pretend to be from a company or business you may recognise.
Hacker	A hacker is someone who can gain access to other computers or online accounts without the owners permission.
HTTP / HTTPS	HTTP or HTTPS form part of a website address – having the '**S**' is one way to work out if the website is secure and safe to use, for example, http**s**://www.google.com
Junk / Spam folder	A folder in your email account for unwanted emails. Often your email account will have a filter that directs **spam** or marketing email automatically to this folder.
Link / Hyperlink	Often a picture or string of words, sometimes underlined or in a different colour. If you click on it, you will be taken directly to another website or other online content.
Malicious attack	An attempt by a **scammer** to install a virus on your computer. It can spread a code with the intention of stealing personal or financial information, sending **spam** or locking your systems down.
Malware	A term that describes all forms of malicious software designed to attack a computer. Common forms include: **viruses** and **ransomware**.
Padlock symbol	If you see a padlock sign on a website – it means you are on a safe connection, but not necessarily a safe website. Check for the '**S**' in **HTTPS** to make sure you are on a safe website.
Parental controls	Settings that let parents choose what content their children can see or access online. It helps protect them from unintended content such as gambling, online games and pornography.
Passcode	A passcode is a series of numbers to give access to either your device or an online account. It helps protect your device and helps keep your **personal information** safe.
Password	A secret word or phrase that you create when setting up a new online account. Usually made up of letters, numbers and sometimes symbols like **$??%.** The more varied it is, the more secure it is likely to be in keeping your **personal information** safe.
Personal data/ information	Information which is related to you. For example, your telephone number, credit card and bank details, address or passport information.
Phishing	**Scammers** may try to trick you be sending an email, sometimes containing a dodgy link, they enourage you to 'click' on. Don't. They will try and gain your **personal information** or encourage you to transfer money. They often pretend to be from a company or business you may recognise.

Term	Meaning
Privacy settings	You can change these setting on your device. They allow you to control and manage who sees or shares information about you.
Ransomware	A form of **malware** that prevents you from accessing files, until a ransom is paid.
Scam	Is when someone tries to cheat or trick you into giving away your **personal information** or bank details.
Scammer	A person who carries out a **scam** is called a scammer or cyber-criminal. They will try to trick you into giving away **personal information** or bank details.
Smart device	Could be your laptop, tablet or smartphone. It is the physical equipment used to access the internet.
Smishing	**Scammers** may try to trick you by sending a text (SMS), instant message or a link for you to click on. The scammer will try and gain your **personal information** or encourage you to transfer money.
Social engineering	Where a **scammer** will try and trick you through manipulation. They often play on your emotions and kindness, and may want you to act quickly. They will try to gain your trust, to access **personal information** or transfer money. If they ask you to buy things like gift cards, or transfer money to them for an emergency, be aware!
Software bug	If your device crashes or you see an error message, this is likely to be the result of a software bug. The software is no longer working properly. You may lose data or your device may fail completely. It's important to save or store your files in the **cloud**.
Spam	Spam is unwanted **emails** from untrusted sources.
Troll	A troll is someone who posts offensive, rude, or off topic comments online.
Username	A name that uniquely identifies someone on a computer system.
Virus	Just like a virus you might have when you are unwell. It can spread a code on your computer with the intentions to steal personal or financial information. The virus can also send **spam** from your computer or lock your system down.
Vishing	**Scammers** may try and reach you over the phone, maybe even using a recorded voice, called a 'bot'. They will try and get your **personal information** or encourage you to transfer money. They often pretend to be from a company or business you may recognise.

bt.com/skillsfortomorrow

Now that you're online why not check out the **helping others** page on the BT Skills For Tomorrow site. You'll find more creative and fun ways to make the most of being online.

Supported by Good Things Foundation