CYBER DICTIONARY

What does that word mean???

Word	Meaning
Apps	Programs that run on devices
Automatic Updates	Updates that are installed automatically (by themselves) by devices
App Developer	A person who makes programs
Anti-virus	Software that looks for and remove viruses and malware (that attach your device - computer, tablet, phone)
Back-up	A back-up is a copy of important data (information) saved in a different location or spot, so that you can get it back if you delete it or it is corrupted. You should back-up your data regularly to protect it
Cyber Bullying	Cyberbullying is when someone uses the internet to be mean to a person (usually a child or young person) so they feel bad or upset. It can happen on a social media site, game, app, or any other online or electronic service or platform. It can include: posts, comments, texts, messages, chats, livestreams, memes, images, videos and emails. (Definition – Cyberbullying | eSafety Commissioner)
Cyber Criminal	These are people who use technology to commit crime on digital systems
Data	Data is any sort of information that is stored in a computer or device memory.
Email	Electronic mail (email) is a way of sending and receiving messages using electronic devices
Hacking	Is using computer skills to break into a device or computer network. Criminals do this to commit crimes. Hacking without permission is illegal. However, ethical hacking is hacking with permission and it can help a business find out how to improve their security

Word	Meaning
Identity Theft	When cyber criminals or another person accesses someone's personal information then pretends to be that person
Malware	Nasty software that can have a negative (bad) impact on devices or apps
Manufacturer	A company who makes devices (eg computers, phones, tablets)
One Time Password	Is a password that can be used once and then expires and are sometimes called OTP codes. A one-time password usually consists of an alphanumeric OTP codes (letters and numbers) and is made for a single login session
Operating System	Software that makes everything on devices work together
Password	Is a way to keep your information safe. Someone else can't get into your account unless they know your password or can crack it
Patches	Are software and operating system updates that fix weaknesses in the devices and apps. They fix security issues/problems and remove viruses and malware
Performance improvement	Irmprovements that make devices (or the apps that run on them) work better, or make them easier to use
Personal Information	This is information (data) that tells us who you are, for example your name, birthday and your email address
Phishing	Is a fake email from someone pretending to be a person or organisation they are not. The email could ask for personal information or have a link to a fake website
Ransomware	Is a type of malware (nasty software). It can spread by clicking a bad email link or opening an attachment. It locks you out of your data or device and demands money to unlock it
Remote Access Trojan (RAT)	A RAT may allow cybercriminals to watch and listen through the camera and microphone, record all your on-screen activity, alter your personal files and use your device to distribute malware to other computers
Security Features	Things that make it harder for cyber criminals to hack a device
Smishing	Is a fake text message from someone pretending to be a person or organisation they are not. The text message could ask for personal information or have a link to a fake website

Word	Meaning
Social Media	Social media is a form of electronic communication (such as websites and apps) that lets someone create and share content or to participate in social networking. Some examples of social media are Facebook, Twitter, Instagram, YouTube, TikTok, etc
Third Party Apps	Software that people can download (put on) their devices
Trojan	Trojan horse malware is a file, program, or piece of code that appears to be legitimate and safe, but is actually malware. Trojans are packaged and delivered inside real software (hence their name), and they're often designed to spy on victims or steal data. Many Trojans also download additional malware after you install them
Two-Step Verification (2SV)	2SV is a security method that uses two ways to prove who you are. For example a password and code sent to your phone
Updates	These are installed on devices to improve its performance or to increase security (make them work better and be safer)
Virus	A virus is a type of malware (nasty software). If you click on a bad link or attachment, it could be a virus. The virus copies itself onto your smartphone or computer. It can affect your apps. It might slow down your device, destroy data, or do other harmful things
Vishing	Is a phone call from someone pretending to be an organisation or a person. During the phone call you could be asked for personal information that can be used to pretend to be you or to hack your accounts
Web Browers	The program people use to access the internet (Chrome, Edge, Firefox, Safari
Website	A website is a set of webpages that are joined together. People look at websites with a computer or device of some kind, sometimes including mobile phones and televisions. The websites are kept on computers called web servers.
Worm	A computer worm is a type of malicious software that travels through network connections all over the world to find its targets. Worms are dangerous because they find a problem in a computer's security system to get inside a device. Once it's in there, it's really hard to stop.