Year 9 Computer Science Cyber Security Knowledge Organiser

Key Word	Definition
Data	Raw facts and figures.
Information	Created when that data has been processed and becomes meaningful.
Cybersecurity	The application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber attacks.
Cybercriminals	A person who engages in criminal activity by means of computers or the internet.
Profiling	The process of construction and application of user profiles generated by computerized data analysis.
User Behaviour	The way in which a person uses a service or product, and whether they are likely to be a repeat user.
Privacy Policy	A statement that explains in simple language how an organisation or agency handles user personal information.
Data Protection	A set of strategies and processes users can use to secure the privacy, availability, and integrity of their data.
Data Subject	The identified or identifiable living individual to whom personal data relates.
Data Portability	Allows individuals to obtain and reuse their personal data for their own purposes across different services.
Malware	Any intrusive software developed by cybercriminals to steal data and damage or destroy computers and computer systems.
Social Engineering	A set of methods used by cybercriminals to deceive individuals into handing over information that they can use for fraudulent purposes.
Phishing	The victim receives an email disguised to look as if it has come from a reputable source, in order to trick them into giving up valuable data.
Shouldering	An attack designed to steal a victim's password or other sensitive data. It involves the attacker watching the victim while they provide sensitive information, for example, over their shoulder.
Blagging	The perpetrator invents a scenario in order to convince the victim to give them data or money.

Year 9 Computer Science Audio Visual Representation Knowledge Organiser

Key Word	Definition
Name Generator Attack	The victim is asked in an app or a social media post to combine a few pieces of information or complete a short quiz to produce a name.
Scam	A dishonest scheme carried out over the internet. The goal is to defraud potential victims and generate financial gain for the perpetrator.
Cyberthreats	The possibility of a malicious attempt to damage or disrupt a computer network or system.
Hacking	Gaining unauthorised access to or control of a computer system.
Ethical Hacking	An authorised attempt to gain unauthorised access to a computer system, application, or data.
Penetration Testing	Paying people to legally hack into computer systems with the sole purpose of helping a company identify weaknesses in their system.
Brute Force Attack	A form of attack that makes multiple attempts to discover something (such as a password).
Script Kiddies	Hackers (not necessarily kids) who use tools downloaded from the internet that allow them to hack with little technical knowledge
DoS (Denial of Service)	A cyberattack where the criminal makes a network resource unavailable to its intended users by flooding the targeted machine or website with lots of requests in an attempt to overload the system.
DDoS (Distributed Denial of Service)	This uses the same concept as a DoS attack, but this time it is multiple computers making the attacks at the same time.
Computer Misuse Act (1990)	The main legislation that criminalises unauthorised access to computer systems and data, and the damaging or destroying of these.
Ransomware	Locks a computer, encrypts files, and therefore prevents the user from being able to access the data. The attacker will demand that a ransom be paid before they decrypt the files and unlock the computer.
Virus	A malicious form of self-replicating software. Once on a computer or network, a virus will replicate itself by maliciously modifying other computer programs and inserting code.

Year 9 Computer Science Audio Visual Representation Knowledge Organiser

Key Word	Definition
Trojan	A piece of software that appears to perform a useful function (such as a game) but unbeknown to the user it also performs malicious actions, e.g. open a 'back door' to give an attacker remote access to your computer.
Worms	Replicate themselves but do not attach themselves to files as a virus does, but cause problems by using up network bandwidth and therefore slowing down the network significantly.
Adware	Infects a computer and causes it to download or display malicious adverts or pop-ups when the victim is online.
Spyware	Unwanted software that monitors and gathers information on a person and how they use their computer.
Bots	Automated programs that perform tasks repeatedly.
Botnet	A large collection of malware-infected devices (zombies). An attacker ('bot herder') chooses when to 'wake' the zombies to perform an attack.
Anti-Malware	Software that scans any file that is able to execute code to check for malicious content.
Firewall	Checks incoming and outgoing network traffic and scans the data to make sure it doesn't contain anything malicious and that it follows the rules set by the network.
End-User Authentication	Techniques used to ensure that the end user is authorised to use the product or service they are trying to access.
Folder Permissions/Privileges	Define what a user can and cannot do with a file or folder.
Biometrics	A type of digital security used to prevent data breaches by making use of individual characteristics such as fingerprints.
Two-Factor Authentication (2FA)	An identity and access management security method that requires two forms of identification to access resources and data.

Key Word	Definition
CAPTCHA	A type of challenge–response test used in computing to determine whether the user is human in order to deter bot attacks and spam.
Blagging	The perpetrator invents a scenario in order to convince the victim to give them data or money.
Firewall	Checks incoming and outgoing network traffic and scans the data to make sure it doesn't contain anything malicious and that it follows the rules set by the network.
Backups	The process of backing up data from multiple devices into a centralized storage device or location.
Internet Service Provider (ISP)	A company that provides access to the internet.
Auto-Updates	The process in which your software applies critical updates without seeking confirmation from a user.

LIVE CYBER THREAT MAP
2,729,792 ATTACKS ON THIS DAY

Malware   Phishing   Exploit

Snapchat
ncce.io/snapchatprivacy

Instagram
ncce.io/instagramprivacy

Google
ncce.io/googleprivacy

Facebook
ncce.io/facebookprivacy

Your Data ☑
Your Rights

1. Unauthorised access to data

2. Unauthorised use of a computer to commit or facilitate another offence

3. Unauthorised acts with intent to impair, or with recklessness as to impairing the operation of a computer

Learning Graph

Explain the difference between data and information

Identify what happens to data entered online

Explain the need for the Data Protection Act

Recognise how data breaches are caused by humans

Define hacking in the context of cybersecurity

Explain how a DDoS attack can impact users of online services

Explain the need for the Computer Misuse Act

Question how malicious bots can have an impact on societal issues

Examine how different types of malware cause problems for computer systems

Compare security threats against their probability and potential impact on organisations

Explain how networks can be protected from common security threats

Identify the most effective methods to prevent cyberattacks

Identify strategies to reduce the chance data being accessed by unauthorised bodies

Key:

Concept

Skill