



The best in everyone™

KS 4

COMPUTER STUDIES

Knowledge Organiser

2026/27

How do I use my KO book for self-quizzing?



1) Write today's date and the **title** from the knowledge organiser



2) Write out the **keywords** you have been asked to learn leaving two lines between each word



3) Cover the definitions apart from the first: **read** it, **cover** it, **say** it in your head, **check** it



4) If you got it right, move on and **quiz yourself** on the rest in your head, one by one



5) Cover up **all** the definitions and write them out **from memory**



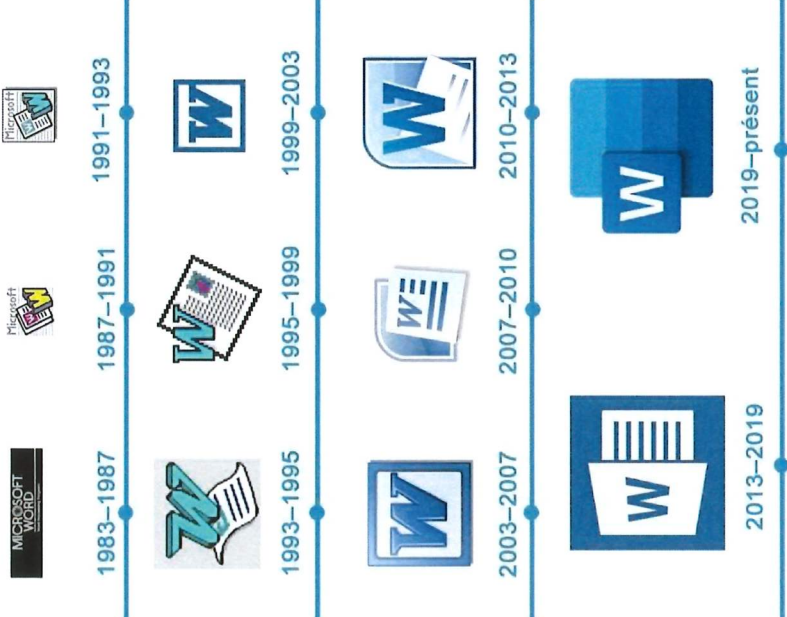
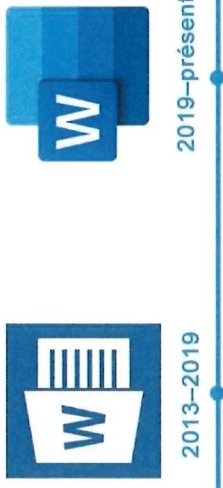
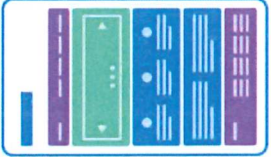
6) **Correct** your answers in green pen

7) Repeat the whole process

J836 – Cambridge Nationals Level 1/2 Information Technologies
R050 – IT in the Digital World
TA1: Design Tools

1.1. Types of design tools	
	Flow charts Shows the steps, decisions and outputs in a process. - Start point — End point — Decisions - Processes — Input/output - Connecting lines with directional arrows Can be useful for simple designs with a small number of tasks and decisions. — Does not need any specialist knowledge to understand the flow chart. — Can show sequences/steps that need to be followed in order. The processes and decisions are shown sequentially so does not show concurrent tasks. — Can become complicated if a lot of decisions need to be shown. — Cannot be used to create visual designs. <pre> graph TD PC[Previous consensus] --> ME[Make an edit] ME --> D1{Was the article edited further?} D1 -- No --> NC[New consensus] D1 -- Yes --> D2{Do you agree with the changes?} D2 -- Disagree --> SC[Seek the compromise] SC --> ME D2 -- Agree --> NC </pre>
	Mind maps To generate outline ideas or to present ideas to an audience. Types: - Library (sort/organise information) - Tunnel timeline (problem solving) - Presentation (present ideas). - Nodes — Sub-nodes — Connecting lines (branches) — Key words — Colours - Images Easy to add ideas at any time — Can help focus on the ideas and links between them — Show dependent ideas Can be difficult for others to understand The correct type of mind map needs to be used
	Visualisation diagrams Usually used when a static product is being created to show what the final solution will look like. Multiple images/graphics — Size and position of images/graphics — Position and style of text — Fonts — Labels/annotations — Colours — Themes Simple to produce — Non-technical so most people can understand them Ideas can be clearly shown — Can clearly show the layout of documents Can see if the layout will work before building a prototype Can lack detail — A lack of technical details can cause issues, confusion and misinterpretation

J836 – Cambridge Nationals Level 1/2 Information Technologies
R050 – IT in the Digital World
TA1: Design Tools

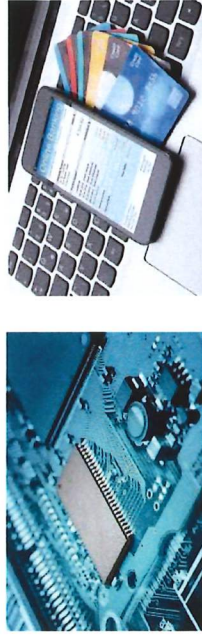
1.1. Types of design tools		1.1. Types of software used to create design tools	
Wireframes			
Purpose	Focuses on what the product will do, rather than what it will look like. Types: – Low-fidelity wireframe (uses basic shapes and image placeholders with limited specific details) – High-fidelity wireframe (shows actual content, fonts, colours, image, dimensions and branding)		
Components	Low-fidelity wireframe: – Boxes – Box labels – Image placeholders – Layout grids High-fidelity wireframe: – Branding – Colours – Fonts – Text – User interaction functionality – Information and graphical elements can be positioned and moved around – The size of the elements can be changed – The design can be finalised in a low-fidelity without the clutter of, for example, font types/colours – High-fidelity can be used in the testing process – Changes can be made efficiently		
Advantages			
Disadvantages	– Interactive features cannot be shown in low-fidelity – High-fidelity can become over designed		
		Desktop Publisher (DTP)	
Used to create:		– Visualisation diagram – Mind map – High-fidelity wireframe – The software allows elements from different files to be combined – Images can be imported from, for example, a scanner or a graphics package – Different elements can be grouped, which means that a group of elements can be moved as one – Elements can be positioned by using a 'drag and drop' feature which will enable precise positioning to be used	
Advantages			
		Word	
Used to create:		– Flow chart – Mind map – Low-fidelity wireframe – There are in-built tools and features which allow shapes and lines to be used to create these design tools	
Advantages			

J836 – Cambridge Nationals Level 1/2 Information Technologies R050 – IT in the Digital World

TA2: Human Computer (HCI) in everyday life

2.1. The purpose, importance and use of HCI in application

A well designed HCI will...	
Advantages	- Be clear in its layout: important information stands out, user interactions are clear - Be consistent in its layout: users know where to find things - Be simple: users can quickly learn how to use the HCI - Be user-controlled: which means the user decides the actions to be taken - Provides feedback: when a user makes an error, the messages should be clear and provide detailed feedback as to how to rectify the error



Embedded systems	
Advantages	- Greater flexibility in use compared to older devices - Ability to set preferences such as specific heating levels
Disadvantages	Limited number of functions/options for the user
Banking	
Advantages	- Increased security - A customer only has access to their own accounts - Can operate bank facilities without the need for bank staff - Flexibility in when and how to use bank
Disadvantages	- Cannot access accounts if the HCI fails - Incorrect programming could lead to incorrect accounts being shown

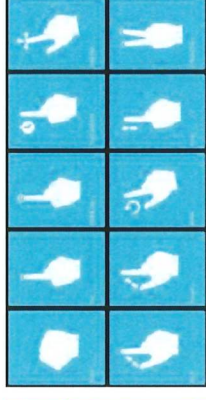


2.2. Hardware considerations	
Display	
Touch Screen	Allows the user to physical touch the screen as part of the interaction
LCD Screen	(Liquid crystal display) A type of display that uses a liquid crystal film sealed between glass plates
LED Screen	(Light emitting diode) A small device that emits light when an electric current is passed through it; lots of LEDs are used together to make self-illuminating displays
OLED Screen	(Organic light emitting diode) A type of display that produces its own light; it is flexible and can include a touch response layer
Resources	
Memory	To store HCI program, OS, applications and features/options
Processing power	The more options, and sub-option, an HCI has, the more processing power is needed to complete the requested tasks without being slowed down

TA2: Human Computer (HCI) in everyday life

2.3. Software considerations 2.3. Software considerations

Operating system (OS)	
The operating system allows the hardware to communicate with the different applications that the device has. OS can be GUI or CLI based. OS can also be proprietary or open source.	
Windows	Mainly PCs, laptops and tablets
Mac OS/iOS	Apple-based devices including Mac desktops and laptops, iPhones and iPad tablets
Android	Used on mobile devices such as tablets and smartphones
Chrome	Used on Chromebook laptops and smartphones
Ubuntu	Mainly PCs but can also be used on a server
Linux	Mainly PCs and laptops but can also be used on, for example, cars, smartphones, web servers and networking hardware
Unix Unix	Can be used on devices ranging from supercomputers to mobile devices



Graphical User Interface (GUI)	
Purpose	A visual interface made up of icons and menus which can be selected. E.g. Click on an icon to open the program.
Used by OS:	– Windows – Mac OS/iOS – Android – Chrome – Ubuntu – Linux – Unix
Advantages	– A help feature is usually included – The same data can be shared between different software applications with the results seen as WYSIWYG – Complicated commands do not have to be learnt or remembered – Intuitive and easy to use
Disadvantages	– Very experienced programmers can find these slow to use and select the options needed – The file size is large which means more storage is needed – A large amount of memory and processing power are needed to handle all the graphics and commands
Command Line (CLI)	
Purpose	Uses text to give the device instructions. E.g. Opening software using a keyboard.
Used by OS:	– Chrome – Linux – Unix
Advantages	– Limited memory and processing power are needed – An experienced user can quickly interact using the correct commands – Does not need a GUI to run
Disadvantages	– Commands have to be spelt and typed precisely for the operating system to react – There are a large number of commands which need to be learnt and remembered by users

2.4. User interaction methods

Touch and gesture

Advantage	The HCI can be less cluttered as fewer buttons will be needed
Disadvantage	Users need to learn, remember and accurately execute touch commands and gestures

Keyboard and mouse

Advantage	Many people are familiar with the layout
Disadvantage	It is a slow method when you need to write a long piece of writing

Voice

Advantage	Benefit to those who need assistive technology due to a disability as there is little physical interaction needed to interact with the HCI
Disadvantage	Noisy environments, accents and multiple speakers may degrade results

J836 – Cambridge Nationals Level 1/2 Information Technologies

R050 – IT in the Digital World

TA3: Data and testing

3.1. Information and data	
Data	Raw facts and figures before they have been processed
Information	= data + [structure] + [context] + meaning
The relationship between data and information:	
- Information is in context, while data has no context - Information is data that has been coded/structured - Data must be processed to become information	
Example:	
Data	01/01/2023
Structure	NN/NN/NNNN
Context	A UK date
Meaning	New year's day in 2023



3.2. Data use: Data types	
Alphanumeric	Any combination of letters, symbols, spaces or numbers. E.g. Qw3r!y
Boolean	There are only two choices. E.g. 1 or 0
Date	There are different formats of date that can be used. E.g. 01/01/2023
Currency	Shows data in a format of money. Can show currency signs and decimals. E.g. £1.09
Decimal	A number format that shows an exact number using a decimal point. E.g. 1.1
Integer	Whole numbers. E.g. 2023
Percentage	A number format that includes decimal places and a % sign and can include decimals. E.g. 19%, 20.23%
Real	Any number, with or without decimal places. E.g. 1, 2.23
Text	Any character. E.g. Ab1£;

3.2. Data use: Validation	
- Checks that the data being entered into a digital system is sensible and reasonable - Does not check that the data is correct - Checks the data against pre-set rules - Is usually carried out by the digital system at the point at which the data is being entered - Is usually set as part of the creation of a solution	
Validation tools	
Data type check	Checks that the data entered is one of the required type. E.g. Price is in currency format.
Input mask Format check	Makes sure that the data is in a specific format. E.g. UK postcode is in LLNN NLL format.
Length check	Sets the length of the data entry. E.g. Mobile number has to be 11 integers in length.
Limited choice	Provides users with a limited choice to select for data entry. Includes drop-down lists, radio buttons and tick lists. E.g. Drop-down list to select month.
Lookup	Looks up acceptable values in a list. E.g. Checks that a postcode is valid by looking up the data in a list.
Presence check	Checks that the data has been entered into a specific field. E.g. Checks that the postcode has been entered for delivery.
Range check	Sets an upper and lower boundary for data entry. The entered data must be between these values. E.g. Secondary school year group entered can only be between 7-11.

3.2. Data use: Verification	
- Checks to see whether the data being entered into a digital system is identical to the source from which it came - Can be carried out manually - Can be carried out by the digital system	
Verification tools	
Double entry	- Entering the data twice - Data entered is checked by comparing it with another set of data to make sure they are the same - If any difference is found between two sets of data, then the user is alerted by an error message - Comparison can be done manually by a person or through a check by the digital system E.g. Setting or resetting a password as the password needs to be entered twice. The second entry is checked against the first entry to make sure they are the same.
Manual checking	- Proofreading - Visually comparing the source data with the data entered into the digital system - Involves a person being able to follow two sets of data and identify any differences E.g. Entering data from a paper-based survey



J836 – Cambridge Nationals Level 1/2 Information Technologies
R050 – IT in the Digital World
TA3: Data and testing

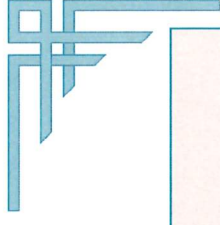
3.3. Data collection methods

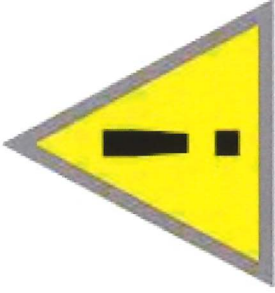
	Primary	Secondary	Email	
Meaning	Research that collects first-hand or fresh data for a specific purpose	Research that uses data and information that has already been collected	Advantage	Can be sent to many people at the same time
Based on	Raw data and information	Analysed and processed data and information	Disadvantage	Can be diverted into spam/junk folders by the email provider
Carried out by	The researcher	Someone else	Advantage	Interview Questions can be modified based on previous answers given
Data	Specific to the purpose	May not fully meet the specific needs	Disadvantage	Can be time consuming and costly to carry out
Process	Very involved	Quick and easy	Advantage	Online questionnaire and survey Cheaper than interviews for large number of people
Cost	High	Low	Disadvantage	Technology and a stable connection is required to complete it
Time	Long	Short		
			Books and magazines	Can be used to collect historical data
			Advantage	Can be biased to the viewpoint of the author(s) or contributors
			Disadvantage	Government statistics Readily available statistics from a trusted source
			Advantage	Can be difficult to collect the exact data needed in large datasets
			Disadvantage	Websites The data has already been collected, and possibly processed, and readily made available for the public
			Advantage	It is not always possible to tell if the site is genuine or real

3.4. Storage of collected data

Logical location		Physical (internal) location	
	Cloud		Physical (external) location
Advantage	Can be accessed through a web browser or app	Primary hard drive	Portable solid-state drive (SSD)
Disadvantage	No or unstable/slow internet connection can make the files, softwares and apps inaccessible	Network drive	Advantage
			Fast reading and writing of data times
			More vulnerable to abrupt power loss and electromagnetic fields
			Portable USB flash drive
			Advantage
			Portable, small and lightweight
			Disadvantage
			Constant plugging into a device can degrade the USB port or the connector
			Network-attached storage (NAS) device
			Advantage
			Files can be between users and devices
			Disadvantage
			Requires some network knowledge to install and configure
			Portable wireless drive
			Advantage
			Has own battery/power source
			Disadvantage
			Can be discoverable by other devices if security protection methods not used





3.5. Application of testing to a range of contexts: Testing and test data		
Testing - The process of checking that a solution, the final product, meets the needs of the end users and is fit for purpose - There are two types of testing: Technical testing and User testing		Test Data Extreme data - A data value that is on the boundary between valid and invalid data - This type of data will not cause an error - A passenger can take between 0-3 suitcases. Test data used: 3 - A new secondary pupil has joined the school and will be placed in a year group between 7 and 11. Test data used: 7
		Invalid (erroneous) data - A data value that will cause an error - This will be unacceptable but could also be incomplete or not meet the validation - A password has been set as having 8 characters including 1 capital letter and 1 number and 1 symbol Test data used: pa55w0rd - A postcode has been set in the format LLNN NLL. Test data used: 12QW E34
		Valid data - A data value that is acceptable, sensible and reasonable - This type of data will not cause an error - A postcode has been set in the format LLNN NLL. Test data used: QW12 3ER - A password has been set as having 8 characters including 1 capital letter and 1 number and 1 symbol Test data used: P@55w0rd
Advantages - The final solution will be fit for purpose - The final solution will be of high quality - Testing will have covered all functions and features so all errors should have been identified and rectified - Technical testing means that the solution will have been tested on a range of digital devices and operating systems - User testing will ensure the user journey is error free and intuitive to use - Carrying out testing can ensure the reliability and robustness of the solution		Definition - A data value that is acceptable, sensible and reasonable - This type of data will not cause an error - A postcode has been set in the format LLNN NLL. Test data used: QW12 3ER - A password has been set as having 8 characters including 1 capital letter and 1 number and 1 symbol Test data used: P@55w0rd
		Disadvantages - Creating a full and complete test plan can be time consuming - If the solution is complex then many people may need to test it, meaning a large number of resources in terms of time, people and money may be needed - If the test plan is not full and complete then errors may not be identified if the tests are not specifically detailed - The planned tests must cover all functions and features of the solution - Full and complete testing can take a long time - If testing does not identify errors at the testing stage, then the completion of the solution may be delayed as errors may be identified later in the process
		Examples - A data value that is acceptable, sensible and reasonable - This type of data will not cause an error - A postcode has been set in the format LLNN NLL. Test data used: QW12 3ER - A password has been set as having 8 characters including 1 capital letter and 1 number and 1 symbol Test data used: P@55w0rd

J836 – Cambridge Nationals Level 1/2 Information Technologies
R050 – IT in the Digital World
TA3: Data and testing

3.5. Application of testing to a range of contexts: Types of testing

Technical testing		User testing	
Definition	Checking the functionality of the solution, including, on a range of digital devices, different OS and, if connectivity is needed, that it works on a range of connectivity methods – Links on a web page or a mobile app to take the user to the intended internal or external page – Testing an HCI to make sure the buttons and macros work as intended – How a solution loads on opening on a range of digital devices and operating systems – Calculations used in a spreadsheet solution – How an AR product loads on a range of digital devices – User interaction in an AR project – Output including the contents and layout – Data validation on a form – The solution will be fit-for-purpose and error free – The solution will have been tested on a range of digital devices – All functionalities will work as intended – It can be time consuming to carry out full and complete technical tests – If all functionality is not tested, the product will have errors on release – It may not be possible to test on a range of digital devices and operating systems – It can be expensive in terms of time and money	Definition	User testing is carried out by a range of users who are likely to use the solution to identify errors or changes required which can be resolved before it is released
Test can cover:		Test can cover:	– Data entry including validation – Whether it is intuitive with informative error messages – Different user interaction methods – Functionality of an HCI – Output format – Ease of use
Advantages		Advantages	– The development team can observe where users get stuck or muddled – A range of user demographics can be used to test the product – An increased confidence in the product from users – Real users will interact with the product, following a complete user journey
Disadvantages		Disadvantages	– Only a small group of users can test the product – If the incorrect demographic users are selected, their user journey may not be indicative of the actual or target demographic group – It can be expensive in terms of time and money



J836 – Cambridge Nationals Level 1/2 Information Technologies
R050 – IT in the Digital World
TA4: Cyber-security and legislation

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		
Social engineering	The art of manipulating people so that confidential information can be found out		
Cyber Security Threat Levels:		Social engineering	
Baiting	Tries to get victims to give cybercriminals the information they need with promises of goods in return.	Phishing	Tries to get users to input their credit or debit card numbers, or security details or log-in details, into a fake website.
Shoulder surfing	Aims to steal data or information by oversteering what an individual is viewing/typing.	Scareware	Tries to scare people into downloading and buying useless software.
		Quid pro quo	Tries to disable anti-virus software so that software updates, usually malware, can be installed to gain access to a digital system.
		Pretexting	A cybercriminal lies to get data or information.

Types of threats		4.1. Threats	
Cyber-security	The practice of defending digital devices, including computers, servers, mobile devices, electronic systems, networks and data, from malicious attacks	Black Hat Hacking	The hacker hacks into the computer system with malicious intent. The intent can include theft, exploiting the data stolen or seen, and selling the data on. Black hat hackers carry out illegal hacking activities and can be prosecuted.
DoS	(Denial of Service) An attempt to make a digital system, for example a network or website, unavailable to its users by flooding it with network traffic.	Grey Hat Hacking	The hacker hacks into the computer system for fun or to troll but does not have malicious intent towards the computer system. If they find a vulnerability, they offer to fix it – but for a fee. They can manipulate rankings of website in a search engine.
Hacking	Hacking means finding a weakness in an established system and exploiting them	White Hat Hacking	The hacker is given permission to hack into systems to identify any loopholes or vulnerabilities. White hat hackers are motivated to keep the computer systems as safe as possible from malicious hacking attempts.
Malware	(Malicious Software) Malware is installed on a computer system and collects information about users without their knowledge		

R050 – IT in the Digital World

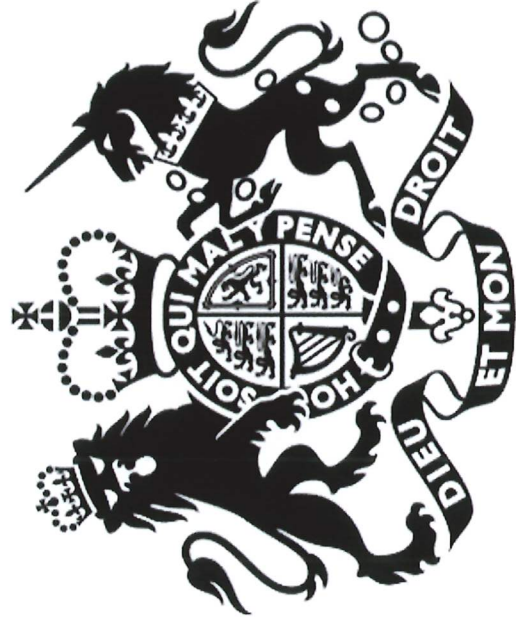
TA4: Cyber-security and legislation

4.2. The impacts of a cyber-security attack on individuals and/or organisations	
Data Destruction	Data is destroyed by a cyber-security attacker and no longer exists. E.g. Attacker deletes customers' orders.
Data Manipulation	Data is edited, usually to meet the needs of the cyber-security attacker. E.g. Attacker changes the data in a news feed on social media platforms.
Data Modification	It changes data to meet the needs of the attacker. However, the attacker usually has different aims and the crime may not be found for a long time. E.g. Attacker changes the amount of money in a bank account and the increased amount of money.
Data Theft	Cyber-attacker steals computer-based data from a person or organisation, with the intent of compromising privacy or obtaining confidential information. Can occur when the data is at rest or in transit.
Data at rest	The data is not moving from device to device or network to network. The data is stored on, for example, a hard drive, laptop, flash drive or archived by an organisation.
Data in transit	The data is being sent to two or more authorised users, or moving, from one location to another, for example across the internet or through a private network.
Identity theft	When personal details are stolen.
Identity fraud	When personal details are stolen and used to commit fraud. E.g. Take out a loan in someone else's name.

4.3. Prevention measures	
Physical prevention measures	
Usually hardware based. The aim is to stop unauthorised access to digital devices, and the data and information stored on them.	
Biometric devices	Devices which use a physical characteristic of the user, such as a fingerprint, eye scan or voice, which needs to be positive match before the device can be accessed.
Keypads	A type of lock where the correct code must be inputted before the lock opens.
RFID	(Radio-frequency Identification) Access badges or tags that use radio frequency to transfer data from the tags to a digital system, for example to allow access to a room.
 	
Logical prevention measures	
Software based techniques used to authenticate a user.	
Access rights and Permissions	Control over who has access to a digital system, folder, files, data and/or information.
Anti-virus/malware software	A set of attributes that can be set to determine what a user can do with files and folders. E.g. read, write, edit, delete.
Manual updates	Security software which are designed to prevent, detect and remove viruses and other malware.
Automatic updates	Users manually prompt for the update to occur.
Username and passwords	Some software updates occur automatically. This process is usually completed in real time.
2FA	The username acts as authorisation whilst the password acts as authentication. Without both parts being correct, access will be denied.
Encryption	The process of encoding files or data.
Asymmetric encryption	(Public key encryption) The encryption key is available to anyone to encrypt data but only the person who receives the data receives the decryption key.
Symmetric encryption	This is when the encryption and decryption keys are the same.
Firewalls	A security device that mitigates against threats by examining data packets. Can be a hard/software - both work in the same way.
Secure backups	A copy of the data/files that are currently in use. Backups are made regularly and stored away from the digital system, preferably in another building in a secure place.

J836 – Cambridge Nationals Level 1/2 Information Technologies
R050 – IT in the Digital World
TA4: Cyber-security and legislation

4.3. Prevention measures	
Secure destruction of data	
Data sanitation	The process of deliberately, permanently and irreversibly removing or destroying the data stored on a storage device to make the data unrecoverable. <i>E.g. Data erasure, Magnetic wipe, Physical destruction.</i>
Data erasure	Software used to overwrite the data on a storage device.
Magnetic wipe	When the magnetic field part of a storage device is removed. This makes all the data stored on the storage device unreadable.
Physical destruction	Physical destruction of a storage device is the most secure. The device is so thoroughly destroyed that the data cannot be retrieved. Methods can include: hard drive shredder, steamroller, burning, drill through or hammer on the device.



4.4. Legislation related to the use of IT systems			
Computer Misuse Act (CMA)		Data Protection Act (DPA)	
Purpose	Protect data and information that is held on computer systems. The CMA relates to illegal access to files and data stored on digital systems.	Purpose	Attempts to control how personal data and information are used by organisations and the UK Government. The Act also gives data subjects control of their personal data.
Main parts to the act:	1. Unauthorised access to computer material 2. Unauthorised access with intent to commit or facilitate the commission of further offences 3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of a computer 4. Making, supplying or obtaining any articles for use in a malicious act using a computer 5. Unauthorised acts causing, or creating risk of, serious damage	Main principles:	1. Used fairly, lawfully and transparently 2. Used for specified, explicit purposes 3. Used in a way that is adequate, relevant and limited to only what is necessary 4. Accurate and, where necessary, kept up to date 5. Kept for no longer than is necessary 6. Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage
Copyright, Designs and Patents Act (CD&PA)		Health and Safety (H&S) at Work Act	
Purpose	Establishes copyright to protect the creative work of individuals or businesses. The CD&PA aims to protect intellectual property.	Purpose	Provides guidance to employers and employees about health and safety at work. The part of the act that applies to people working with digital systems is the Health and Safety DSE Regulations.
Main parts to the act:	1. Illegal download of video/audio files 2. Software piracy, wither by illegal download or illegal distribution 3. Theft of intellectual property, for example text/written work, including on websites 4. Use of software without the relevant license 5. Using/downloading images without permission of the copyright holder	Main tasks:	1. Analyse workstations and assess and reduce risks 2. Plan work so that there are breaks or changes of activity 3. Arrange and pay for eye tests and glasses (if special ones are needed) 4. Provide health and safety training and information
Freedom of Information Act (Foi)			
Purpose	The Act deals with access to official information and people being able to find out any information on any topic from any public authority, i.e. right of access.	Provides access to:	1. Official information 2. Any information on any topic from any public authority (except for information regarded as "exceptions")

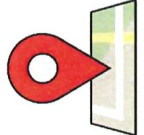
5.1. Types of digital communications		
Audio		
Advantage	It is more accessible to those with hearing impairments	Disadvantage It can only be heard within a short distance
Collaboration tools		
Advantage	People can work from any location where there is an internet connection	Disadvantage If there is no internet connection, then collaboration cannot take place
Leaflets		
Advantage	It can be target at one, or more, demographic group	Disadvantage It can be easily ignored or recycled without being read
Infographics		
Advantage	It can explain a complex topic in a simple way	Disadvantage It can simplify a complex topic too much
Newsletters		
Advantage	A house style can be used to provide recognition and consistency	Disadvantage May not be read so important information could be missed
Presentations		
Advantage	The contents can be presented by a speaker or automatically with no human involvement	Disadvantage Effects such as animations and transitions between slides can become distracting
Reports		
Advantage	A range of elements, for example a table of contents and graphs/charts, can be included	Disadvantage If the information does not 'flow' then the user may become confused
Social media		
Advantage	Posts can be uploaded which can be seen by many people	Disadvantage Negative posts can be seen by many people and shared
Video		
Advantage	It can be uploaded to social media, AR experiences and websites	Disadvantage It can take a long time to create



5.2. Software	
DTP	
Main features	– Pre-defined templates – Frames – Drag and drop – WYSIWYG
Can be used for:	– Infographics – Leaflets – Newsletters
Word processing	
Main features	– Format text – Spelling and grammar – Tables – Insert elements from different applications
Can be used for:	– Infographics – Leaflets – Newsletters – Letters (inc. mail merge) – Reports
Spreadsheet	
Main features	– Calculations – Graphs and charts – Modelling – Format cells
Can be used for:	– Creating elements to be used in other digital communications – Graphs and charts – Data manipulation
Database	
Main features	– Records – Fields – Tables – Queries – Validation tools – Verification tools – Relationships between tables
Can be used for:	– Creating elements to be used in other digital communications – Mail merge – Data manipulation
Presentation	
Main features	– Slides – Slide master – Animations – Transitions – Speaker notes
Can be used for:	– Slideshows
Collaboration tool	
Main features	– Voice calling – Video calling – Chat – Access rights
Can be used for:	– Recording meetings – Sharing screens – Sharing documents

J836 – Cambridge Nationals Level 1/2 Information Technologies
R050 – IT in the Digital World
TA5: Digital communications

5.3. Digital devices		
Digital communication needs digital devices so that the communication can be seen, heard or accessed.		
Smartphones	Can be classed as mobile devices.	
Tablets	They can be easily moved and are portable. It can usually be used on the go.	
Laptops		
Smart TVs	TVs that connect to the internet. The TV includes software that allows the user to access a wide range of apps: streaming services, web browsing, catch-up TV, games etc.	
PCs	Used for tasks such as, using standard office applications to create and edit digital content and using the internet.	
Projected smartboards	Allows images from a computer screen to be displayed onto the smartboard using a digital projector.	
Television-style smartboards	Uses the same technology as a smart TV. The smartboard is connected to the internet so files stored in the cloud can be accessed and edited. There is no connection via a projector to a source digital device.	

5.5. Audience demographics			
The factors which should be considered when selecting the type of digital communication and the distribution channel			
			
Age	Location	Gender	Accessibility

5.4. Distribution channels					
Distribution channels			Distribution channel connectivity methods		
Cloud	Advantage	Files are stored off-site so can be used as a backup	4G/5G	Advantage	Increased bandwidth for all users which means faster transfer speed
	Disadvantage	Must have internet access to be able to download stored files		Disadvantage	Possible less coverage as more transmitter masts will be needed to provide the increased bandwidth
Email	Advantage	Communications can be sent with attachments	Bluetooth	Advantage	No cables are needed so paired devices can be moved
	Disadvantage	Can go into junk/spam folder so may not be seen		Disadvantage	The range between the paired devices is relatively low, about 10 meters
Messaging	Advantage	All users in a group will receive the message	Mobile Wi-Fi hotspots	Advantage	Will allow multiple devices to connect to the same hotspot wherever it is needed
	Disadvantage	This service needs to be monitored to make sure any posts meet the rules		Disadvantage	Some mobile data charges may be applied by the internet service provider (ISP)
Mobile apps	Advantage	Features can be included in the data/information to increase user interaction	Wi-Fi	Advantage	Increased mobility as devices can be moved and still be connected to the WAP
	Disadvantage	Apps need to be constantly monitored and updated to continue providing their service		Disadvantage	The more devices connected, the slower the data transfer
Multimedia	Advantage	Can include a range of elements such as text, graphics and sound	Wired	Advantage	Lack of interference from , for example, walls and closed doors, meaning the signal is stable
	Disadvantage	The message given through multimedia can be lost if too many elements are used		Disadvantage	Devices cannot be moved as device needs to remain connected via a cable
VoIP	Advantage	Features such as call forwarding, group calls, call waiting and voicemails can be used			
	Disadvantage	May have lag or distortion if the connection degrades			
Websites	Advantage	Communications can be uploaded and kept for access			
	Disadvantage	Some indication of where the communication is located needs to be provided			

