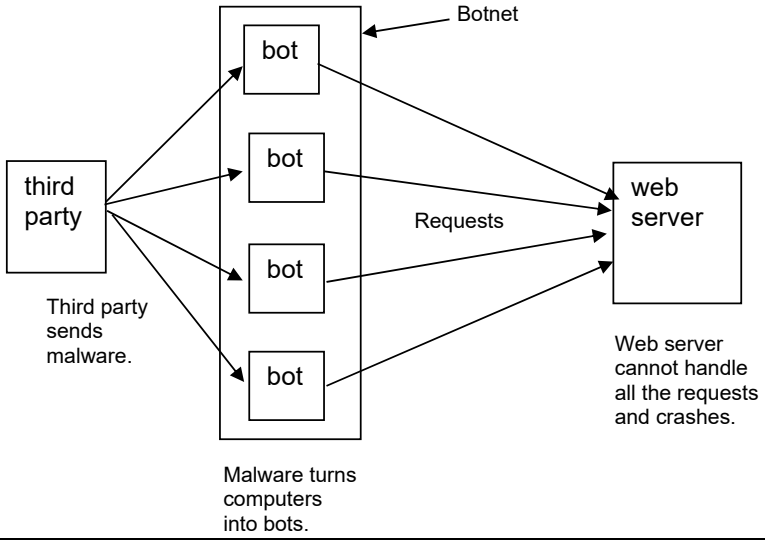
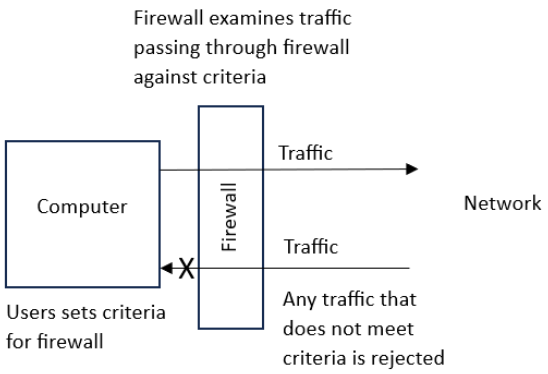
4(a)	Any **four** from: • A legitimate looking email is sent to the user • The user clicks a **link** in the email // the user **replies** to the email • The user is **directed** to a fake website • The user **enters** their **personal** data … • … that is stolen/used by a third party (for malicious purposes)
4(b)	Any **two** from: • Check the email address that the email has been sent from • Check the tone/spelling of the email • Check the URL that is attached to the link
4(c)	Any **three** from: For example: • Virus • Worm • Trojan horse • Spyware // keylogger • Ransomware • Adware
4(d)(i)	Any **one** from: • A language that uses English-like statements • It is a language that needs to be converted to machine code (to be processed by a computer) • It is a portable language (that can be used on any computer)
4(d)(ii)	Any **two** from: • Easy/quick to read/write/understand • Machine independent • Less likely to make errors • Programmer can focus on the problem instead of the manipulation of memory/hardware

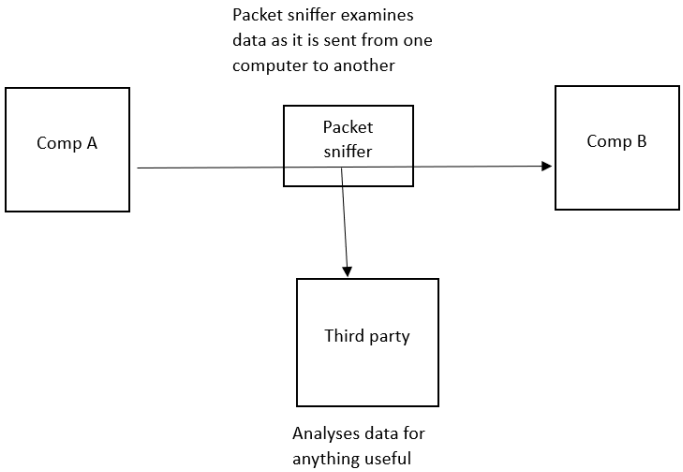
4(d)(iii)	Any **one** from: • Cannot directly manipulate the hardware • Takes **longer** to convert (than low level-language) • Cannot use specialised hardware • Uses more **memory** // less efficient **memory** use
4(d)(iv)	Any **three** from: • The code is translated and executed line by line • … stopping when an error is found (showing the error location) • … meaning errors can be corrected in real time • No need to retranslate each time an error is fixed • … making it easier to debug • Sections of code can be easily tested • … meaning the whole program doesn't need to be written for testing

4(a)	**One** mark for the security solution **Two** marks for a matching description • Strong/complex password • Requires a mixture of letters, number and symbols • Makes it very difficult for the hacker to guess • Limiting number of attempts for password • Cannot keep repeatedly guessing a password • Stops a brute-force attack being successful • Biometric device • Requires the hacker to have biometric data to access the data • It is very difficult to fake biometric data • Two-step verification // two-factor authentication • Requires the hacker to have additional data to access the data • The data is sent to the users registered device/account that the hacker would also need • Firewall • Examines **incoming** data/traffic • Can block any data that does not meet set criteria • Anti-spyware • Detects/removes any **spyware** present on the computer • Hacker cannot use **spyware** to get data to discover passwords
4(b)	**Two** marks for: • Involves manipulating/deceiving people • … with the aim of obtaining confidential/personal/valuable data Any **one** from: For example: • Phishing // by example • Baiting // by example • Shoulder surfing // by example
4(c)(i)	Any **one** from: • They are both small text files • They both store data about the user // by example • They are both **stored/managed** by the web browser • They are both downloaded on to a user's computer
4(c)(ii)	**Two** from (one mark for session, one mark for matching comparison to persistent): • Session cookies are deleted when the web browser is closed • … whereas persistent cookies are deleted by the user/expire after a certain time • Session cookies are only stored in RAM • … whereas persistent cookies are stored in the secondary storage

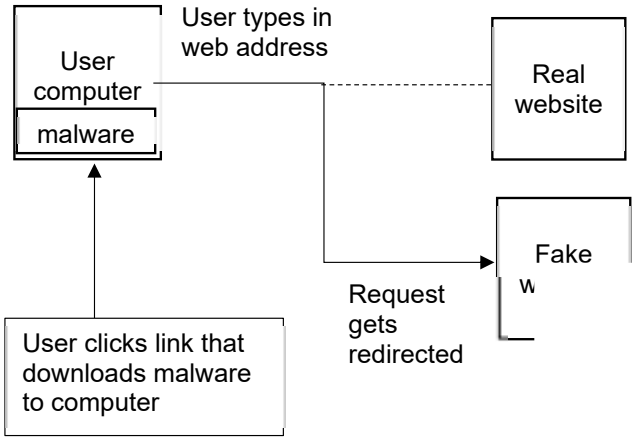
8(a)	**One** mark for each part of the diagram that shows: • A perpetrator/third party sending malware // user downloads/installs malware • Each computer is turned into a bot… • … to create a botnet • Third party initiates the attack • **All** the bots send a request at once to a **web server** • … crashing the webserver Example: 
8(b)	Proxy server

6	The diagram includes (any **four** from): – Traffic passing both ways through the firewall – An indication that criteria is set for the firewall – Traffic is compared to criteria – Traffic being rejected if it does/does not meet criteria – Traffic being accepted if it does/does not meet criteria e.g. 

1(a)	– A
1(b)	Any **one** from: – Spyware // Keylogger – Adware – Trojan horse
1(c)	– Anti-malware

8(a)	The diagram demonstrates (**One** mark for each part of the diagram): – Data is being sent from one device to another – The data is being examined **during transmission** – Packet sniffer is used – Intercepted data is reported to a third-party **during transmission** … – … and analysed for anything useful – Connection hacked to spoof destination address e.g. 
8(b)	– Encryption … – … if the data is intercepted it will be **meaningless** (because they do not have the decryption key)

8(a)	**Three** from: • Trial and error to **guess** a **password** • **Combinations** are repeatedly entered … • … until correct password is found • Can be carried out manually or automatically by software
8(b)(i)	Any **two** from: e.g. • Steal/view/access data • Delete data • Change data • Lock account // Encrypt data • Damage reputation of a business
8(b)(ii)	Any **three** from: e.g. • Virus • Worm • Trojan horse • Spyware • Adware • Ransomware
8(c)	Any **two** from: • Two-step verification//Two-factor authentication//by example • Biometrics • Firewall // Proxy-server • **Strong/complex** password // by example • Setting a limit for login attempts • Drop-down boxes • Request for partial entry of password

10(a)	• To obtain **personal** data/details // by example
10(b)	**One** mark for each correct part of the diagram. Diagram shows: • User clicks/opens attachment/link that triggers download • Malicious software downloaded onto user's computer • User enters website address • User is **redirected** to fake website e.g. 
10(c)	**Two** from: Displays web pages … by rendering HTML
10(d)	Any **three** from: e.g. • Storing bookmarks/favourites • Recording user history • Allowing use of multiple tabs • Providing navigation tools // by example • Providing an address bar • Managing protocols // by example // checking digital certificate • Send URL to DNS • Sends a request to the **IP address/web server** (to obtain the contents of a webpage) • Runs active script/JavaScript/client-side script • Allows **files** to be downloaded from **website/internet**
10(e)	Any **four** from: • Session cookies are stored in memory/RAM • … whereas persistent cookies are stored on the hard drive/secondary storage • When the browser is closed a session cookie is lost • … whereas a persistent cookie is not lost • … until deleted by the user/they expire

1(a)	D
1(b)	**One** mark for identification. E.g. **One** mark per bullet for description to **max two** each. Virus • Software/code that replicates • …when the user runs it // with an active host • Deletes/damages/corrupts data/files // takes up storage/memory space Worm • Software/code that replicates itself on a **network** • …without user input // without active host • Takes-up bandwidth • Deletes/damages/corrupts data/files // takes up storage/memory space • Opens back doors to computers over the network • Used to deposit other malware on networked computers Trojan horse • Software/code that is hidden within other software // Software that is disguised as authentic software • …when **downloaded/installed** the other **malware**/**by example** it contains is **installed** Adware • Software/code that generates/displays (unwanted) adverts on a user's computer • Some may contain spyware/other malware • Some when clicked may link to viruses • Reduces device performance // reduces internet speed • Redirects internet searches/user to fake websites Ransomware • Software/code that stops a user accessing/using their computer/data • …by encrypting the data/files/computer • A **fee** has to be paid to decrypt the data // A **fee** has to be paid to 'release' the computer/device/data

1(c)	**One** mark for each similarity to **max two**. **One** mark for difference (both sides needed unless clearly and accurately implied). Similarities e.g. • Check incoming and outgoing signals // filter traffic • Store whitelist/blacklist • Block incoming/outgoing signals • Both block unauthorised access • Keep a log of traffic • Both can be hardware or software (or both) Differences e.g. • Proxy can hide user's IP address, firewall does not hide the user's IP address • Proxy intention is to divert attack from server, firewall is to stop unauthorised access • Proxy protects a server, firewall protects individual computer • Proxy examines/processes requests for a website but a firewall does not (checks type of signal) // Proxy **processes** client-side requests whereas firewall **filters** packets • Proxy transmits website data to the user, but a firewall does not (it allows valid signals) • Proxy allows faster access to a web page using cache, but a firewall does not (allow faster access or have cache) • Proxy can hide internal network from internet, but a firewall cannot