The Internet & Its Uses

(Chapter 5)

Syllabus Content:

5.1 The internet and the world wide web	
Candidates should be able to:	Notes and guidance
1 Understand the difference between the internet and the world wide web	• The internet is the infrastructure • The world wide web is the collection of websites and web pages accessed using the internet
2 Understand what is meant by a uniform resource locator (URL)	• A URL is a text-based address for a web page; it can contain the protocol, the domain name and the web page/file name
3 Describe the purpose and operation of hypertext transfer protocol (HTTP) and hypertext transfer protocol secure (HTTPS)	
4 Explain the purpose and functions of a web browser	• The main purpose of a web browser is to render hypertext markup language (HTML) and display web pages • Functions include: – storing bookmarks and favourites – recording user history – allowing use of multiple tabs – storing cookies – providing navigation tools – providing an address bar

Syllabus Content:

5.1 The internet and the world wide web continued

Candidates should be able to:	Notes and guidance
5 Describe how web pages are located, retrieved and displayed on a device when a user enters a URL	• Including the role of: – the web browser – IP addresses – domain name server (DNS) – web server – HTML
6 Explain what is meant by cookies and how they are used, including session cookies and persistent cookies	• Cookies are used for functions, including: – saving personal details – tracking user preferences – holding items in an online shopping cart – storing login details

5.2 Digital currency

Candidates should be able to:	Notes and guidance
1 Understand the concept of a digital currency and how digital currencies are used	• A digital currency is one that only exists electronically
2 Understand the process of blockchain and how it is used to track digital currency transactions	• Blockchain, in its basic form, is a digital ledger, that is a time-stamped series of records that cannot be altered

5.3 Cyber security

Candidates should be able to:	Notes and guidance
1 Describe the processes involved in, and the aim of carrying out, a range of cyber security threats	• Including: – brute-force attack – data interception – distributed denial of service (DDoS) attack – hacking – malware (virus, worm, Trojan horse, spyware, adware, ransomware) – pharming – phishing – social engineering

Syllabus Content:

5.3 Cyber security continued	
Candidates should be able to:	Notes and guidance
2 Explain how a range of solutions are used to help keep data safe from security threats	• Including: – access levels – anti-malware including anti-virus and anti-spyware – authentication (username and password, biometrics, two-step verification) – automating software updates – checking the spelling and tone of communications – checking the URL attached to a link – firewalls – privacy settings – proxy-servers – secure socket layer (SSL) security protocol

5 The Internet & Its Uses

5.1 | The Internet & The World Wide Web

NOTE: The World Wide Web (WWW) is a newly added topic in the Computer Science (2210) syllabus for the session 2023–2025.

5.1.1 Differences Between Internet & World Wide Web (WWW):

Internet:

- The Internet is the massive network/global connection of interconnected computer networks.
- The Internet uses TCP/IP transmission protocols.
- The Internet stands for Interconnected Networks.
- The users can send and receive emails using the Internet and it also allows online chatting (via text, audio & video).

World Wide Web (WWW):

- The World Wide Web (WWW) is a collection of interlinked, hypertext documents/webpages/multimedia resources stored on websites.
- The World Wide Web is accessed over the Internet.
- WWW uses http protocols to transmit data.
- WWW is content from web servers organized as web pages which are written in HTML.
- The uniform resource locators (URLs) specify the location of the web pages.
- The web documents/resources are accessed using browsers.

A user sends emails from his webmail account (email account accessed through a website).

Is the user using the internet, or the World Wide Web (WWW), or both?

- The user is using both.
- He is using the Internet because he is sending data on the infrastructure.
- He is also using WWW because he is accessing a website (that is stored on a web server operated by webmail) that is a part of the WWW.

Exam Style Questions:

Question 1:

(b) The students use the network to access the Internet.

One student stated, '*The Internet and the World Wide Web are the same thing*'.

Tick (✓) **one** box to indicate whether this statement is true or false.

True	False

Justify your choice.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....[5]

Answer:

False because:

- The Internet is the infrastructure/global collection of networks.
- World Wide Web is the (multimedia web) pages/content.
- The World Wide Web is accessed over the Internet.
- Webpages are written in HTML.
- HTTP protocol used to transfer web pages.
- The Internet uses IP protocol.

Question 2:

(a) Explain the difference between the World Wide Web (WWW) and the Internet.

.....

.....

.....

.....[2]

Answer:

(a) **Two** from: **[2]**

- WWW is a collection of interlinked, hypertext documents/webpages/multimedia resources (accessed via the Internet) //WWW is content from web servers organised as web pages
- Internet is the global connection of interconnected computer networks
- The Internet uses TCP/IP protocol / WWW uses http protocols to transmit data

Question 3:

(d) Melinda sends emails from her webmail account (email account accessed through a website).

Explain whether Melinda is using the internet, or the World Wide Web (WWW), or both.

.....

.....

.....

.....

.....

..... [3]

Answer:

4(d)	**1 mark** for identifying that she is using both. **1 mark** per bullet point for justification • using internet because sending data on **the infrastructure** • using WWW because accessing a **website** (that is stored on a web server operated by the webmail) that is part of the WWW	**3**

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

5.1.2 Uniform Resource Locator (URL):

- A uniform resource locator (URL) is a text-based address for a web page.
- It contains the domain name, protocol used and the web page/file name.
- It is the website address that is typed into the browser's address bar used to access websites.
- It directs a browser to a specific page online called a web page.
- In essence, it's a set of directions and every web page has a unique one.

In a web browser, the address bar (also URL bar) shows the current URL. The user can either click on a link or type a URL into the bar manually to navigate to a chosen website.

It is typed into the browser address bar using the following format:

protocol://website address/path/file name

- The protocol is either http or https.
- The website address is:
  - domain host → www
  - domain name → website name
  - domain type → .com, .org, .net, .gov etc.
  - country code → .pk, .uk, .de, .cy etc.
- The path is the web page, which is often omitted and it then becomes the root directory of the website.
- The file name is the item on the web page.

For example, the web browser will break up the URL into three parts:

The first part: It is the access protocol used. It can only be either http or http**s**.

The second part: It is the domain name or also called web servers name.

The third part: It is the file name/web page.

Exam Style Questions:

Question 1:

(a) An example of a Uniform Resource Locator (URL) is:

http://www.cie.org.uk/index.htm

Part 1 Part 2 Part 3

Identify the **three** parts that make up this URL.

Part 1 .....

Part 2 .....

Part 3 .....

[3]

Answer:

Part 1 = access protocol **Part 2** = domain name **Part 3** = file name

Question 2:

(b) The website has a uniform resource locator (URL).

An example of a URL is given.

https://www.cambridgeassessment.org.uk/index.html

Complete the table to identify the name of each section of the URL.

URL section	Name
https	
cambridgeassessment.org.uk	
/index.html	

[3]

Answer:

https = protocol

cambridgeassessment.org.uk = domain name

/index.html = file name/web page

Question 3:

(b) Consider the URL:

http://cie.org.uk/computerscience.html

(i) Give the meaning of the following parts of the URL.

http .....

.....

.....

cie.org.uk .....

.....

.....

computerscience.html .....

.....

.....

[3]

Answer:

http = enables browser to know what protocol is being used to access information in domain

cie.org.uk = it is the domain name

computerscience.html = it is the actual web page / file being viewed

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

Question 4:

(b) The following URL is typed in:

http://www.cie.org.uk/ComputerSciencePapers

This URL is composed of three parts.

State the part of this URL that is the:

File name .....

Protocol .....

Web server name .....

[3]

Answer:

(b)

File name: ComputerSciencePapers

Protocol: http(://)

Web server name: www.cie.org.uk

[3]

Question 5:

(b) The URL for the music company's website is:

https://www.rockict.net/index.htm

Part 1 **Part 2**

(i) Identify what **Part 1** and **Part 2** represent in this URL.

Part 1 .....

Part 2 .....

[2]

Answer:

10(b)(i)	1 mark for each correct part – domain (name) – file name/webpage name	**2**

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

5.1.3 HTTP & HTTPs:

HyperText Transfer Protocol (http):

- It is the main protocol used by web browsers that governs the transmission of data using the Internet.
- HyperText Transfer Protocol (http) is a set of rules that must be obeyed when using the internet.
- It is an access/application-layer protocol for transmitting hypermedia documents, such as HTML.
- It is used for communication between web browsers and web servers.

The statements written above are for both http and https

HyperText Transfer Protocol Secure (https):

- It is a secure protocol and often indicated by a padlock sign in the status bar.
- It is a secure version of HTTP.
- It means that the website uses SSL/TLS (secure sockets layer/transport layer security).
- It means that the website uses encryption (data sent to and from the webserver is encrypted).
- It secures the website and the data being transmitted.
- It is slower to use as compared to http; and it is usually used when sensitive or private data is being transferred across the internet.

. HyperText Mark-up Language (HTML):

- It is used to create and develop webpages/websites (web authoring language).
- It uses both structure and presentation.
- It is translated by a browser to display webpages on screen.
- It uses opening and closing tags to display and format content (e.g. color, font, layout etc.).

Exam Style Questions:

Question 1:

(a) Explain what is meant by HTML.

.....

.....

.....

.....

.....

..... [3]

Answer:

- Hypertext Mark-up Language
- It uses both structure and presentation.
- It is used to create web pages/websites // web-authoring language.
- It is translated by a browser to display web pages.
- It uses (opening and closing) tags to display/format content e.g. colour/font/graphics/layout.

Question 2:

Give the meaning of the following terms.

HTML .....

.....

http .....

.....

https .....

.....

[3]

Answer:

- **HTML –** HyperText Markup Language / language used to create web pages.
- **http –** hypertext transfer protocol / protocol used by web browsers.
- **https –** hypertext transfer protocol secure / secure protocol used by web browsers.

Question 3:

(c) The website Gerald visits uses https.

Explain what is meant by https.

.....

.....

.....

.....

.....

..... [3]

Answer:

- Hypertext Transfer Protocol Secure.
- It is a protocol that is a set of rules/standards.
- It is a secure version of HTTP.
- It secures website/data.
- It uses TLS/SSL.
- It uses encryption.

5.1.4 Web Browsers:

- It is a software that renders the hypertext markup language (HTML) and display web pages.
- It translates the HTML code from websites and shows the result of translation (in the form of text, videos, images or sounds etc.).

Functions/features of browsers:

1) Stores bookmarks and favorites
2) Records user history
3) Allows use of multiple tabs
4) Stores cookies
5) Provides navigation tools
6) Provides an address bar

Role of the browser when accessing the Internet:

- It renders HTML and allows user to view web pages.
- It allows files to be downloaded from website/internet.
- It sends a request to the IP address/web server to obtain the contents of a web page.
- It sends URL to DNS.
- It manages HTTP/HTTPs protocol.
- It stores cookies.
- It allows user to bookmark/favorite web pages.
- It provides navigation features.
- It allows multiple tabs.
- It runs active script.
- It has a homepage and records the history of pages visited.

Role of browser in requesting and displaying the web pages for a website:

- It sends request to the webserver.
- It receives web pages back from the webserver.
- It converts HTML to display the web page.
- It manages protocols.

There are many more features/functions of browsers which are given in the answers to the exam style questions provided on the next page.

Exam Style Questions:

Question 1:

(c) Explain the function of a web browser.

.....

.....

.....

.....

.....

.....[3]

Answer:

(c) Any **three** from:
- displays web page
- interprets/translates the HTML document
- interprets/translates embedded scripting, for example JavaScript
- provides functions, such as bookmarks and history
- identifies protocols, such as https, SSL [3]

Question 2:

(b) State **three** functions of a browser.

1 .....

.....

2 .....

.....

3 .....

.....
[3]

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

Answer:

7(b)	**Three** from: • Display a web page • Sends a request to the web server • Receives data from web server • Translates HTML files • Processes client-side script, e.g. JavaScript • Store favourites • Store history • Navigation forward and backward • Check security • Store / access cookies • Find specific text within a web page • Downloading file from the web • Allows a homepage • Allows multiple tabs / web pages to be opened • Stores data in its cache	**3**

Question 3:

Meena uses a browser to research information for her business.

(a) Give **three** functions of a browser.

1 .....

2 .....

3 .....

[3]

Answer:

Question	Answer	Marks
5(a)	Any **three** from: – Convert HTML code – Display web pages – Check if a website is secure – Request web pages from a web server – Send URL/domain name – Runs active script – Store history/favourites/bookmarks – Create tabs	**3**

Question 4:

(c) Tammy uses a browser when accessing the Internet.

Describe the role of the browser.

.....

.....

.....

.....

.....

.....

.....

..... [4]

Answer:

Question	Answer	Marks
5(c)	Any **four** from: – Allows user to view web pages – Renders HTML – Allows user to bookmark/favourite web pages – Provides navigation features – Allows (multiple) tabs – **Stores** cookies – Records history of pages visited – Has a homepage – Runs active script – Allows **files** to be downloaded from **website/internet** – Sends a request to the **IP address/web server** (to obtain the contents of a web page) – Sends URL to DNS – **Manages** HTTP/HTTPS protocol	4

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

5.1.5 Retrieval, Location & Displaying Of Web Pages:

Domain Name Server (DNS):

- It is a system for finding IP addresses for a domain name given in a URL.
- It stores an index of URL and matching IP address.
- It searches for URL to obtain the IP address.
- The DNS process involves converting a URL (such as www.visionacademy.com.pk) into an IP address the computer can understand (such as 107.162.140.19).
- So, it basically translates domain names to IP addresses so browsers can load Internet resources.
- Therefore, the URL and domain name servers eliminate the need for a user to memorize IP addresses.

NOTE: The process of how web pages are located, retrieved, and displayed on a device when a user enters a URL including the roles of the web browser, IP address, DNS, web server & HTML involves using the same keywords for all kind of scenarios with little variations.

Therefore, a few examples according to questions asked in past examinations are given below for you to understand this important concept better and easily.

However, the basic keywords, reasoning and concepts remain fairly same for all questions.

Description of how Web Pages for a Website is requested and displayed on a user's computer:

- The browser sends URL to DNS (domain name server) using HTTP/HTTPS.
- The DNS finds matching IP addresses for URL and sends IP address to web browser.
- The web browser sends request to IP address/web server for web pages.
- The web server sends web pages back to browser.
- The browser renders/interprets the HTML to display web pages.
- Any security certificates are exchanged/authenticated.

How the web browser uses the URL to access the Web Pages:

- The web browser sends the URL to DNS (domain name server) to find the IP address.
- DNS stores an index of URL and matching IP address.
- DNS searches for URL to obtain the IP address.
- IP address is sent to the web browser, if found.
- It connects to the web server (using the IP address) using HTTP/HTTPS.
- Web server sends the web page to web browser.
- Web browser interprets/translates HTML code to display the web page.
- If URL is not found, DNS returns an error to the browser.

Explanation of role of browser when accessing the Web Pages:

- The web browser sends the URL to DNS (domain name server) to find the IP address.
- It connects to the webserver (using the IP address) using HTTP/HTTPS.
- It renders/translates HTML.
- It runs active/client-side scripts built into webpages.
- It manages SSL/TLS certificate process.
- It stores/retrieves cookies.

Exam Style Questions:

Question 1:

A company sells smartphones over the internet.

Explain how the information stored on the company's website is requested by the customer, sent to the customer's computer and displayed on the screen.

Requested:

- A web browser is used.
- The user enters the URL/web address (into the address bar) OR clicks a link containing the web address.
- The URL/web address specifies the protocol used e.g. Hyper Text Transfer Protocol (HTTP)/Hyper Text Transfer Protocol Secure (HTTPS).

Sent:

- The URL/web address contains the domain name.
- The domain name is used to look up the IP address of the company.
- The domain name server (DNS) stores an index of domain names and IP addresses.
- The web browser sends a request to the web server/IP address.

Received:

- The data for the website is stored on the company's web server.
- The web server sends the data for the website back to the web browser.
- The web server uses the customer's IP address to return the data.
- The data is transferred into Hyper Text Mark-up Language (HTML).
- HTML is interpreted by the web browser to display the website.

Question 2:

(d) Customers will use a web browser to access Victoria's website.

Victoria writes a paragraph of text to explain how the website will be displayed on a customer's computer.

Use the list given to complete Victoria's paragraph by inserting the correct **six** missing terms. Not all terms will be used.

- browser
- domain name
- firewall
- hexadecimal
- HTML
- https
- MAC address
- search engine
- Uniform Resource Locator (URL)
- web server

The user enters the website ..... into the address bar.

The protocol that is used is ..... . The URL contains

the ..... for the website. This is used to look up the

IP address of the company. A DNS server stores an index of IP addresses.

The browser sends a request to the ..... as this is

where the files for the website are stored. The files are sent back to the

..... as ..... files.

This is interpreted by the browser and the web page is displayed.

[6]

Answer (in correct sequence):

1. URL
2. https
3. Domain name
4. Web server
5. Browser
6. HTML

Question 3:

Alice enters a URL into a web browser to access a webpage.

(a) State what URL represents.

U ..... R ..... L .....[1]

(b) Explain how the web browser uses the URL to access the webpage.

.....

.....

.....

.....

.....

.....

.....

.....[4]

Answer:

Question	Answer	Marks
8(a)	Uniform Resource Locator	1
8(b)	**Four** from: • The web browser sends URL to DNS • DNS stores an index of URL and matching IP address • DNS searches for URL to obtain the IP address • IP address sent to web browser, (if found) • Web browser sends request to IP of webserver • Webserver sends web page to web browser • Web browser interprets HTML to display web page • If URL not found DNS returns error	4

Question 4:

A music company has a website that allows users to stream music. The music is stored in sound files.

(b) Describe how the web pages for the website are requested and displayed on a user's computer.

.....

.....

.....

.....

.....

.....

.....

..... [4]

Answer:

7(b)	Any **four** from: – Browser sends URL to DNS – … using HTTP/HTTPS – IP address is found on DNS – DNS returns IP address to the browser – Browser sends request to web server/IP address – Web server sends web pages back to browser – Browser **interprets/renders** the HTML (to display web pages) – Security certificates exchanged	**4**

5.1.6 Cookies:

- They are small packets of data stored in a text file by a web browser which is downloaded to a user's computer when a website is visited.
- It is sent by a web server to a web browser every time the user visits the website.
- It collects and stores key information and data regarding user preferences.
- It is stored on a user's computer by a web browser.
- It is detected by the website when the user visits again.
- The use of cookies on a website can be determined by a message which is frequently displayed saying 'cookies are required to access this site' (or something equivalent).

Always remember that:

- They are not programs but simply pieces of data and so they can't actually perform any operations.
- They are not a form of virus/malware at all and do not corrupt or delete data on a user's computer.
- They are not a form of spyware at all and are just used to track the browsing of a user and then accordingly personalize/customize their experience.

There are two types of cookies:

1. session cookies
2. persistent (or permanent) cookies

A message is displayed to a user saying, "Set your browser to accept cookies". Why some websites make this request:

- They make this request to enable logon information to be kept on the user's computer.
- They provide pages customized for the user the next time he/she logs on.
- It allows websites to implement shopping carts and one-click purchasing.
- Moreover, cookies are used to be able to distinguish between new and repeat visitors to the website.

1) Session Cookies:

- They are stored in temporary memory on the computer and don't actually collect any information from the user's computer and doesn't personally identify a user.
- Session cookies are used, for example, when making online purchases.
- They keep a user's items in a virtual shopping basket.
- Hence, session cookies are deleted on a user's computer once the browser is closed, or the website session is terminated.

2) Persistent Cookies:

- They are stored on the hard drive of a user's computer until the expiry date is reached, or the user deletes it.
- Persistent cookies remember a user's log in detail (so that they can authenticate the user's browser).
- These cookies remain in operation on the user's computer even after the browser is closed or the website session is terminated.
- Their advantage is that they remove the need to type in login details every time a certain website is visited.
- Some websites use cookies to store more personal information or user preferences, but this can only be done if the user has provided the website with certain personal information and agrees to it being stored.
- Legitimate websites will always encrypt any personal information stored in the cookie to prevent unauthorized use by a third party that has access to your cookie folder.

Advantages of Persistent Cookies:

1. They are a very efficient way of carrying data from one website session to another, or even between sessions on related websites as they remove the need to store massive amounts of data on the web server itself.
2. Storing the data on the web server without using cookies would also make it very difficult to retrieve a user's data without requiring the user to log in every time they visit the website.

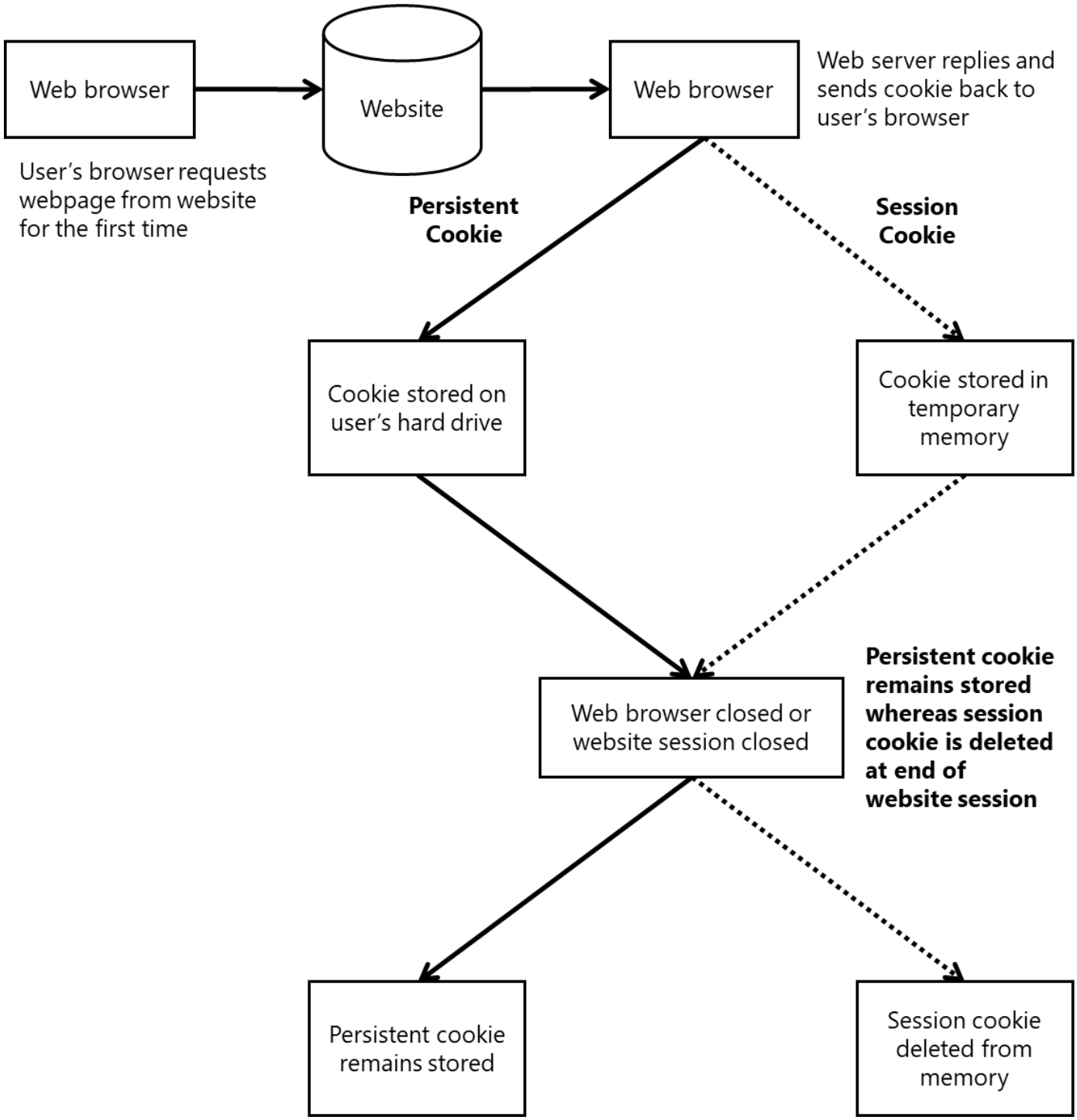
Uses of Persistent Cookies:

1. It is used to save personal details.
2. It is used to store login details.
3. It is used for tracking user preferences.
4. It is used to hold items in an online shopping cart.
5. It is used to track and save internet surfing habits.
6. It is used to carry out targeted advertising.
7. It is used to store payment/credit card details.
8. It is used to store user preferences and then accordingly customize/personalize a webpage.
9. It is used to store progress in online games or quizzes.

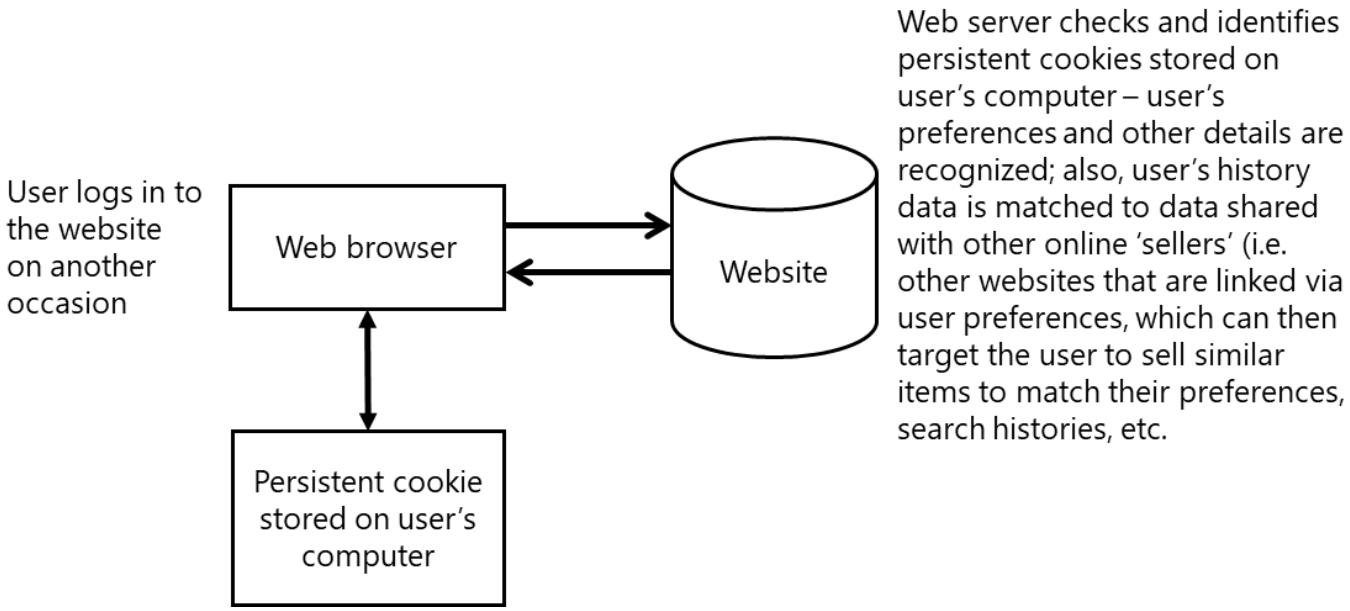
It is generally used to improve experience and speed up purchases and login.

The following diagrams summaries what happens when a website is first visited and then what happens in subsequent visits:

(i) The first-time user logs in to a website:



(ii) The user logs in to a website again (subsequent logins):



A cookie could be used to automatically enter a user's payment details when the user makes a purchase online.

How cookies can be used to store and automatically enter a user's payment details:

- The web server sends (cookie) file to the user's browser.
- The user's payment details are stored in an encrypted text file.
- The cookie file is stored by browser or stored on user's HDD/SSD.
- When a user revisits website, webserver requests cookie file.
- The browser sends cookie file back to web server to automatically enter the details.

Why a user may be concerned about their personal data and online browsing habits being stored in cookies:

- The user does not see what information is stored so the user may feel their privacy is affected.
- A profile could be built about the user that could expose a user's identity (lead to identity theft).
- Sensitive information stored in cookies could be intercepted in transmission.
- Other websites could gain access to the cookies stored on a user's computer.
- A computer could be hacked to obtain data stored in cookies so payment information could be stolen and used by a third party.

Exam Style Questions:

Question 1:

When a customer enters a music website, a message is displayed:

"RockICT makes use of cookies. By continuing to browse you are agreeing to our use of cookies."

Explain why the music company uses cookies. [2]

- To store items that a customer has added to an online shopping basket.
- To store a customer's credit card details.
- To store log-in details.
- To track what product a customer browses // Track music preference.
- Targeted advertising // making recommendations.
- Personalizes/customizes the experience.
- Shows who are new and returning customers.
- To speed up log-in times.
- To speed up/allow single click purchases.
- Improves the experience.

Question 2:

When customers access Victoria's website they will be given the message:

> This website uses cookies. An explanation of their purpose can be found in our cookies policy.

Explain why Victoria would use cookies as part of her website. [4]

- To store a customer's password.
- To store a customer's credit card details so they do not need to be re-entered in future.
- To track what the customer has viewed on the website so she can send them adverts that match their preferences.

Question 3:

Raj is using the Internet to do some online shopping. He visits a website that tells him that it uses cookies.

(a) Explain what is meant by the term **cookies**.

.....

.....

.....

.....

.....

.....

.....

.....[4]

(b) Give **two** examples of the use of cookies.

Example 1 .....

.....

.....

Example 2 .....

.....

.....

[2]

Answer:

5(a)	Any **four** from: • Data / files • Stored in a text file • Downloaded to a user's computer when a website is visited // webserver sends to web browser • Stored on a user's computer • Stored by a browser • Detected by the website when it is visited again	**4**
5(b)	Any **two** from: e.g. • To store personal information/data • To store login details • To save items in an online shopping basket • To track/save internet surfing habits // to track website traffic • To carry out targeted advertising • To store payment details • To customise a webpage // to store user preferences • Store progress in online games/quizzes	**2**

Question 4:

(a) Four statements about cookies are shown in the table below.

Study each statement.

Tick (✓) to show whether the statement is true or false.

Statement	True	False
they are a form of spyware		
they are used only in advertising		
they are used to track browser use		
they act in the same way as a virus		

[4]

Answer:

(a) 1 mark per correctly placed tick

Statement	True	False
they are a form of spyware		✓
they are used in advertising only		✓
they are used to track the browsing of a user	✓	
they act in the same way as a virus		✓

[4]

Question 5:

(c) Meena visits a website to buy products for her business.

The browser uses a small file to store the details of the products she views. This allows the website to display advertisements for other products she may like.

The small file also stores her log-in details.

Give the name of this type of file.

..... [1]

Answer:

- Cookies

Question 6:

(b) Priya uses cookies in her website.

Five statements are given about cookies.

Tick (✓) to show if the statement is **True** or **False**.

Statement	True (✓)	False (✓)
Cookies can be used to store a customer's credit card details		
Cookies can be used to track the items a customer has viewed on a website		
Cookies will corrupt the data on a customer's computer		
Cookies are downloaded onto a customer's computer		
Cookies can be deleted from a customer's computer		

[5]

Answer:

6(b)	1 mark per each correct row. **Statement** / **True (✓)** / **False (✓)** Cookies can be used to store a customer's credit card details — ✓ Cookies can be used to track the items a customer has viewed on a website — ✓ Cookies will corrupt the data on a customer's computer — ✓ Cookies are downloaded onto a customer's computer — ✓ Cookies can be deleted from a customer's computer — ✓	**5**

Question 7:

(a) Three statements about cookies are shown below.

Study each statement.

Tick (✓) to show whether the statement is true or false.

Statement	True	False
Cookies can destroy or modify data in a computer without the user's knowledge		
Cookies generate website pop-ups		
Cookies allow a website to detect whether a viewer has viewed specific web pages		

[3]

Answer:

(a)

Statement	True	False
Cookies can destroy or modify data in a computer without the user's knowledge		✓
Cookies generate website pop-ups		✓
Cookies allow a website to detect whether a viewer has viewed specific web pages	✓	

[3]

Question 8:

The table contains descriptions relating to web pages and the Internet.

Complete the table with the correct terms for the given descriptions.

Term	Description
	the language used to create a web page
	the type of software application used to display a web page
	an address given to a computer, by a network, to allow the computer to be uniquely identified
	a text file sent by a web server to collect data about a user's browsing habits
	the company that provides a connection to the Internet

[5]

Answer:

Question	Answer	Marks
11	One mark per each correct term.	5

Terms	Description
HTML	the language used to create a web page
Browser	the type of software application used to display a web page
IP address	an address given to a computer, by a network, to allow the computer to be uniquely identified
Cookie	a text file sent by a web server to collect data about a user's browsing habits
Internet Service Provider // ISP	the company that provides a connection to the Internet

5.2 | Digital Currency

NOTE: Digital Currency is a newly added topic in the Computer Science (2210) syllabus for the session 2023–2025.

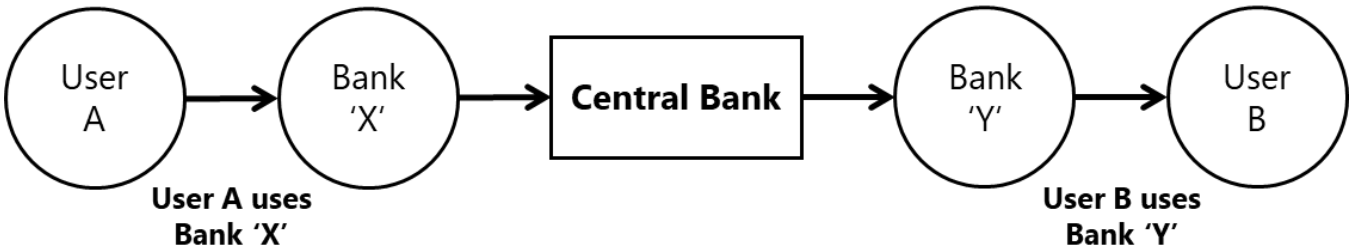
5.2.1 Digital Currency:

- Digital currency only exists electronically (in a digital format).
- It has no physical form unlike conventional fiat currency.
- Digital currency is an accepted form of payment to pay for goods or services as it can be transferred between various accounts when carrying out transactions.
- It has made it possible to bank online (for example, using PayPal) or via a smartphone app (for example, Apple Pay).

Problems of Digital Currency:

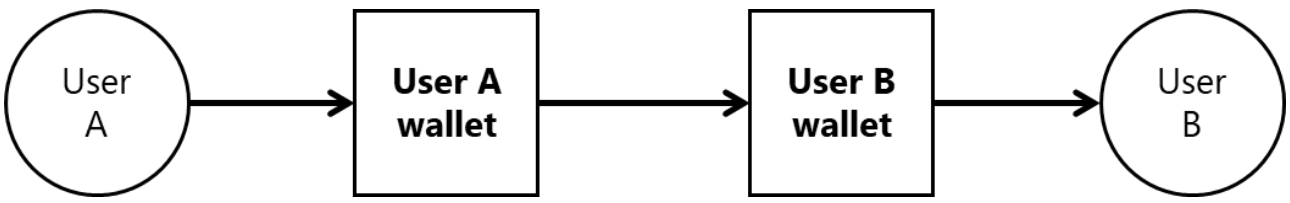
- The digital currency relies on a **central banking system**:

e.g. If User A wishes to send some money to User B:



- The problem with centralization is maintaining confidentiality and security.
- Traditional digital currencies are regulated by central banks and governments (in much the same way as fiat currencies) so all transactions and exchange rates are determined by these two bodies.

Solution: One example of digital currency, known as **Cryptocurrency**, was created to address the problems associated with the centralization of digital currency. It has essentially overcome these issues by introducing **decentralization**:

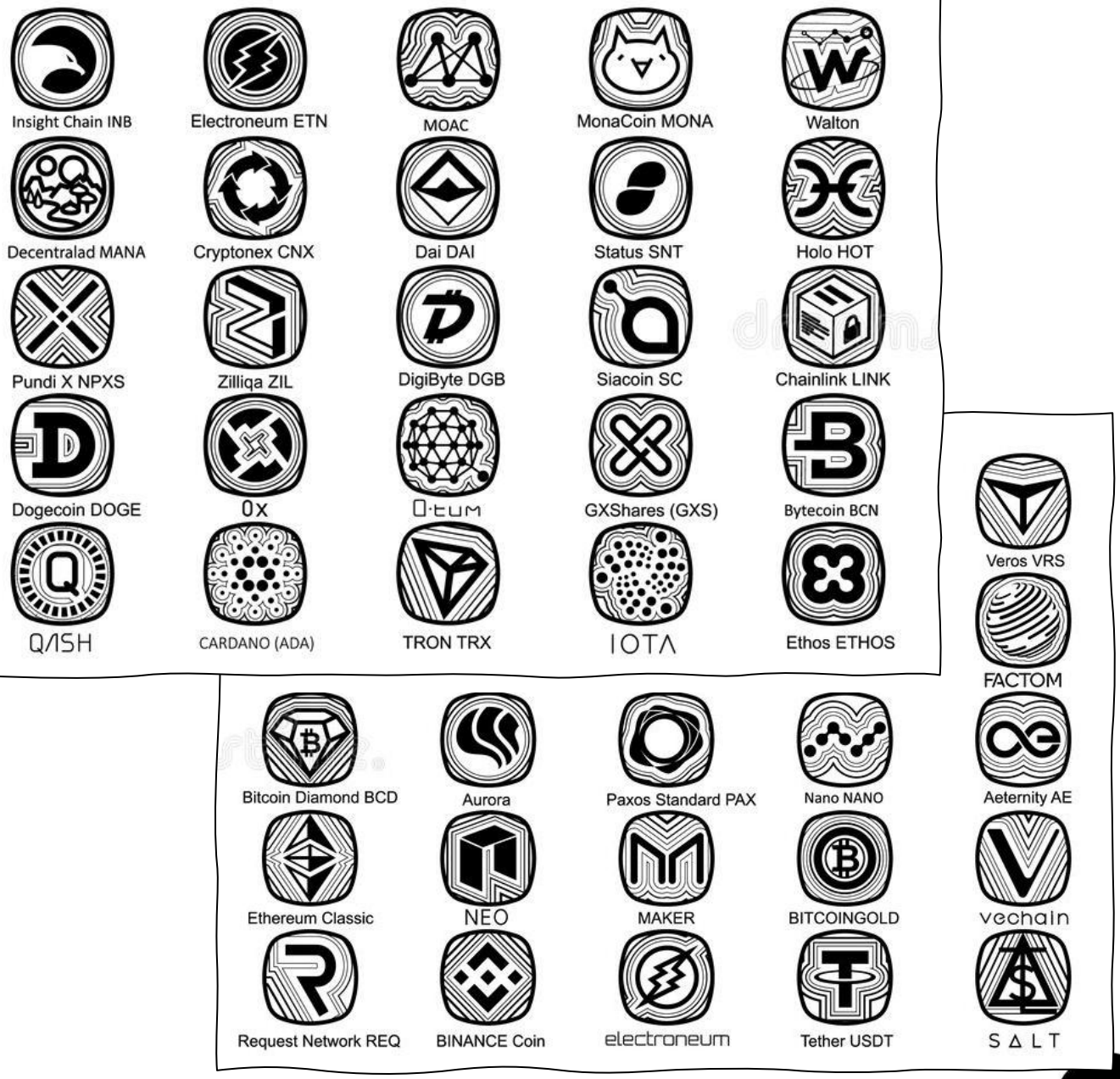


Cryptocurrency:

- Cryptocurrency uses cryptography to track transactions.
- Cryptocurrency has no state control (unlike traditional digital currency) and all the rules are set by the cryptocurrency community itself.
- Cryptocurrency transactions are publicly available and therefore all transactions can be tracked and the amount of money in the system is monitored.
- The cryptocurrency system works by being within a blockchain network which means it is much more secure.

A cryptocurrency, crypto-currency, or crypto is a digital currency designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it.

The following are some popular types of cryptocurrencies:



Sample Exam Style Questions:

NOTE: These questions are not actual examination questions. This new topic is recently introduced for 2023-2025 session and there are no either past paper questions or specimen paper questions available for this. These questions are not officially taken from any Cambridge examination or resource.

The following questions are just sample/model questions which you may expect in your upcoming examination, and they have been designed for your practice.

Question 1:

(a) What is meant by the term **digital currency**.

.....

.....

.....

..... [2]

(b) Outline the main differences between **digital currency** and **cryptocurrency**.

.....

.....

.....

.....

.....

..... [3]

Possible Answer:

Question	Answer	Marks
1(a)	Any **two** from: • Digital currency only exists electronically (in a digital format). • It has no physical form unlike conventional fiat currency. • Digital currency is an accepted form of payment to pay for goods or services as it can be transferred between various accounts when carrying out transactions.	**2**
1(b)	Any **three** from: • Digital currency relies on a centralized banking system whereas cryptocurrency uses decentralization. • The problem with digital currency is maintaining confidentiality and security whereas cryptocurrency uses cryptography to track transactions. • Digital currencies are regulated by central banks and governments whereas cryptocurrency rules are set by the cryptocurrency community itself. • Cryptocurrency transactions are publicly available and can be tracked unlike digital currency transactions. • The cryptocurrency system is more secure as it works in a blockchain network.	**3**

5.2.2 Blockchaining:

Blockchain:

- It is a digital ledger, that is a time-stamped series of records that cannot be altered.
- It facilitates the process of recording transactions and tracking assets in a business network.

Blockchain is used in many areas, such as:

1. cryptocurrency (digital currency) exchanges
2. smart contracts
3. research (particularly within pharmaceutical companies)
4. politics
5. education.

How is blockchain used to record digital currency transactions:

- The blockchain is a shareable ledger, a digital file that records all transactions.
- The ledger is distributed across several nodes, meaning the data is replicated and stored instantaneously on each node across the system.
- When a transaction is recorded in the blockchain, details of the transaction are recorded, verified, and settled across all nodes.
- The record of transactions cannot be modified or changed as each node has a full record of the data that has been stored on the blockchain since its formation.
- If one node has an error in its data, it can use the thousands of other nodes as a reference point to correct itself.

NOTE: Think of decentralization like the way Google Docs work. You can share a single document with multiple users and all users can view the changes simultaneously. A decentralized blockchain is similar except information in a blockchain once verified is very hard to change.

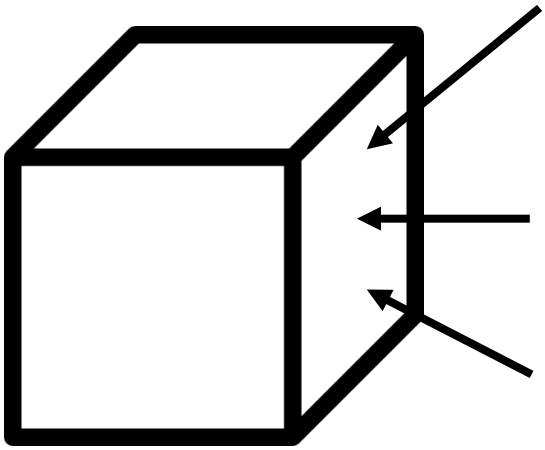
Process of blockchain and how it is used to track digital currency transactions:

- Blockchain is a decentralized database, and all the transactions of networked members are stored on this database.
- Whenever a new transaction takes place, a new block is created.
- The block consists of data, hash value and previous hash value (see diagram below).
- A new hash value is created each time a new block is created.
- This hash value is unique to each block and includes a timestamp, which identifies when an event actually takes place.
- The entire record is available to anyone in the decentralized system.
- The first block is known as the genesis block and all blocks are connected in a chain.
- Any changes to the data within a block in the chain will cause the value of the hash to change so all the remaining blocks will now be invalid since the chain was broken which prevents hacking.
- It uses proof-of-work to prevent tampering/hacking that makes sure it takes ten minutes for each block before it can be added to the chain.
- This is policed by miners.

Miners: They are special network users that get a commission for each new block created.

- It only takes one block to break the link for any transaction to be terminated.
- When a new block is created, it is sent to each computer in the blockchain and is checked for correctness before being added to the blockchain.

Diagram of a block in a blockchain:



Data – for example, name of sender & recipient, amount of money, and so on

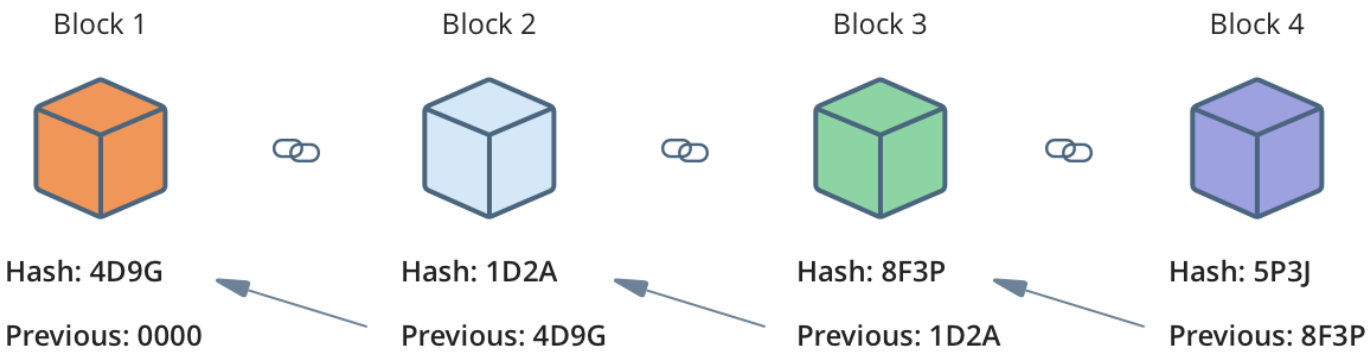
Hash Value – a unique value generated by an algorithm (usually a cryptographic algorithm called SHA 256), which acts as a fingerprint

Previous Hash Value – these points back to a previous block in the chain

Hacking of blockchains:

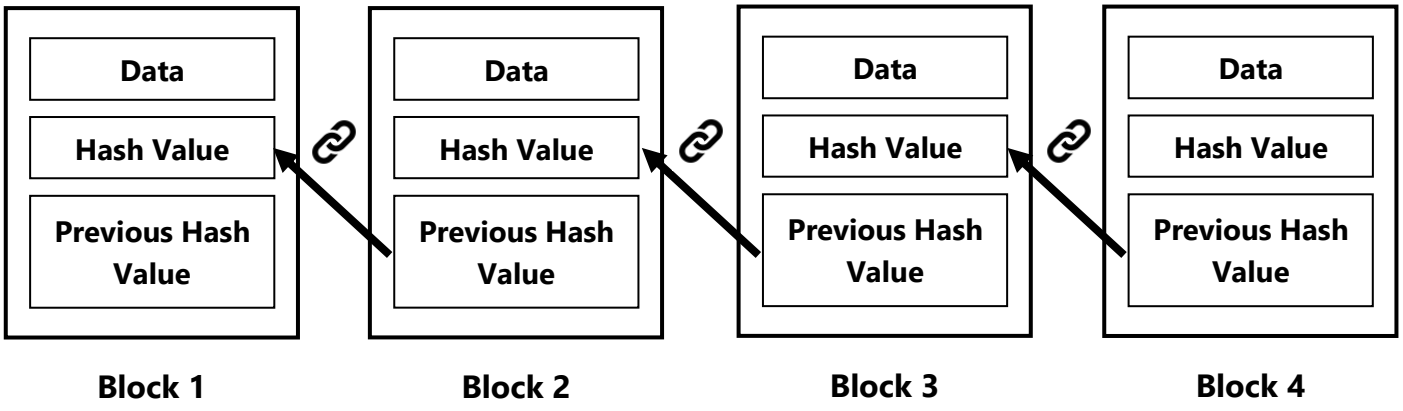
- It is almost impossible to hack into the blockchain since it would be necessary to attack every single block in the chain at the same time.
- Any changes to the data within a block in the chain will cause the value of the hash to change so all the remaining blocks will now be invalid since the chain was broken which prevents hacking.
- It only takes one block to break the link for any transaction to be terminated.
- It also uses proof-of-work to prevent tampering/hacking that makes sure it takes ten minutes for each block before it can be added to the chain.
- The whole process is also policed by miners.

Diagram of typical blockchain network (containing 4 blocks):



- Block 1 is known as the genesis block since it doesn't point to any previous block.
- All the blocks are connected in a chain network.

Simpler diagram of blockchain network to be drawn in CAIE Exam (if required):



Sample Exam Style Questions:

NOTE: These questions are not actual examination questions. This new topic is recently introduced for 2023-2025 session and there are no either past paper questions or specimen paper questions available for this. These questions are not officially taken from any Cambridge examination or resource.

The following questions are just sample/model questions which you may expect in your upcoming examination, and they have been designed for your practice.

Question 1:

Describe the process of **blockchain** and how it is used to track digital currency transactions.

.....

.....

.....

.....

.....

.....

.....

..... [4]

Possible Answer:

Question	Answer	Marks
1	Any **four** from: • Blockchain is a decentralized database, and all the transactions of networked members are stored on this database. • Whenever a new transaction takes place, a new block is created. • The block consists of data, hash value and previous hash value. • A new hash value is created each time a new block is created. • This hash value is unique to each block and includes a timestamp, which identifies when an event actually takes place. • The first block is known as the genesis block and all blocks are connected in a chain. • It uses proof-of-work to prevent tampering/hacking that makes sure it takes ten minutes for each block before it can be added to the chain. • This is policed by miners. • It only takes one block to break the link for any transaction to be terminated. • When a new block is created, it is sent to each computer in the blockchain and is checked for correctness before being added to the blockchain.	**4**

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

Question 2:

(a) A blockchain has **4 blocks**. Draw a diagram to represent how a blockchain network is created.

[4]

(b) Describe what would happen if **block 2** was hacked to change the sum of money in the transaction.

.....

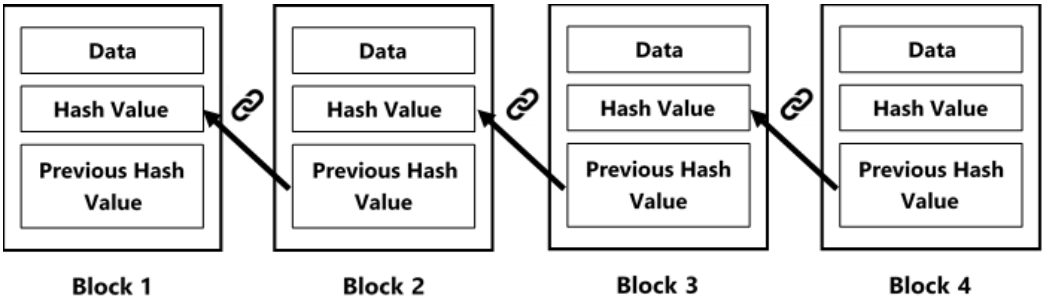
.....

.....

..... [2]

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

Possible Answer:

Question	Answer	Marks
2(a)	The diagram shows: • four blocks • contents of each block • the connection between the hash and previous hash value of each block • the connection between the blocks to represent a chain **For example:**  	**4**
2(b)	Any **two** from: • Any changes to the data within the block 2 in the chain will cause the value of the hash to change. • This means that block 3 and beyond will now be invalid since the chain was broken between block 2 and block 3. • The previous hash value of block 3 would no longer be valid therefore breaking the chain.	**2**

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

5.3 | Cyber Security

5.3.1 Cyber Security Threats (Internet Risks):

Data can be corrupted or deleted either through accidental damage or malicious acts. There are also many ways data can be intercepted leading to cyber security threats.

Brute-Force Attack:

- A brute-force attack is a hacking method that uses trial-and-error to crack passwords, login credentials, and encryption keys.
- It is an attempt to crack a password by systematically trying every possible combination of letters, numbers, and symbols until the hacker discovers the one correct combination that works.
- It basically consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly.
- The attacker systematically checks all possible passwords and passphrases until the correct one is found.

Ways of reducing the number of attempts needed to crack a password:

1. Try the most common passwords used. The five most common passwords are following:
    1. 123456
    2. password
    3. qwerty
    4. 111111
    5. abcl23
2. Start with a strong word list which is a text file containing a collection of words that can be used in a brute force attack and some programs will also generate a word list containing a million words.

    This is still a faster way of cracking a password than just total trial-and-error however it would still take several hours to find the correct password depending on the length of password and the variation of characters used.

Data Interception:

- It is a form of stealing data by tapping into a wired or wireless communication link to gain unauthorized access to personal data or to obtain confidential information.

In wired networks:

- It is carried out using a packet sniffer, which examines data packets being sent over a network.
- The intercepted data is sent back to the hacker.

In wireless networks (Wi-Fi):

- It is carried out using wardriving (or sometimes called Access Point Mapping).
- In wardriving, the data is intercepted using a laptop or smartphone (portable device), antenna and a GPS device (together with some software) outside a building or somebody's house.
- The intercepted Wi-Fi (wireless) signal can allow a hacker to steal personal data without the user's consent/knowledge.

Prevention methods:

1. It can be prevented by using wired equivalent privacy (WEP) encryption protocol.

Note: Encryption does not stop the data being intercepted but it will make the data meaningless to the hacker if they do not have access to a decryption key.

2. It can be prevented by using firewalls so that outside users cannot gain access.
3. It can be prevented by using complex passwords for wireless router/device.

Note: It is important not to use Wi-Fi (wireless) connectivity in public places (such as an airport) since no data encryption will exist and your data is then open to interception by anyone within the airport.

Distributed Denial of Service (DDoS) Attack:

Denial of Service (DoS) Attack:

- The web server is sent multiple requests at the same time from one computer.
- It is designed to flood a server with useless requests and deny people access to a website.
- The server is unable to respond to all the requests.
- As a result, the server fails/crashes/runs slowly.
- This prevents legitimate users from gaining access to a website/server.

Distributed Denial of Service (DDoS) Attack:

- It uses multiple computers as bots.
- It is designed to flood a server with useless requests and deny people access to a website.
- The web server is sent a large number of requests all at the same time from multiple computers.
- The server is unable to respond to all the requests.
- As a result, the server fails/crashes/runs slowly.
- This prevents legitimate users from gaining access to a website/server.

This attack may be able to prevent a user from:

1. accessing their emails.
2. accessing websites/web pages.
3. accessing online services (such as banking)

Purpose of a distributed denial of service (DDoS) OR denial of service (DoS) attack:

- The purpose is to disrupt the operation of a web server/network.

Why distributed denial of service (DDoS) OR denial of service (DoS) attack on a web server that hosts the website will prevent users from accessing the website:

- The web server has been flooded with traffic (it has been sent many requests at once)
- Therefore, the server crashes OR the server is brought to a halt.

Distributed denial of service (DDoS) attack on a user's emails account:

- An attacker sends out many spam messages to a user's email account.
- Internet Service Providers (ISPs) only allow a specific data quota for each user.
- Consequently, if the attacker sends out a very large number of emails to the user's account, it will quickly get clogged up and the user won't be able to receive legitimate emails.

Signs of distributed denial of service (DDoS) OR denial of service (DoS) attack:

1. The network performance is slow (accessing certain websites or opening files).
2. The user is unable to access particular websites.
3. There is a large amount of spam mail reaching the user's email account.

Security devices that can be used to help prevent a DoS or DDoS attack:

- A firewall OR proxy server

Prevention of distributed denial of service (DDoS) OR denial of service (DoS) attack:

1. It can be prevented using firewall.
2. It can be prevented using proxy server.
3. It can be prevented using an up-to-date malware/virus checker.
4. It can be prevented by applying email filters to manage or filter out unwanted traffic or spam emails.

Note: The principal difference between a DoS attack and a DDoS attack is that the DoS is a system-on-system attack whereas DDoS involves several systems attacking a single system.

In simpler words:

- DoS attack: a single system (one computer) targets the victim's system
- DDoS attack: multiple systems (multiple computers) attack the victim's system

Differences between DoS & DDoS Attacks:

Denial of service (DoS) attack	Distributed denial of service (DDoS) attack
Single system targets the victim system	Multiple systems attack the victims system
Victims PC is loaded from the packet of data sent from a single location	Victims PC is loaded from the packet of data sent from multiple locations
Can be blocked easily as only one system is used	Difficult to block this attack as multiple devices are sending packets and attacking from multiple locations
Only single device is used with DoS attack tools	Multiple bots are used to attack at the same time
Slower attack and easy to trace	Faster attack and difficult to trace
Lesser volume of traffic to victim's network	Massive volumes of traffic to victim's network

Hacking:

- It is the act of gaining unauthorized access to a computer system/data without the user's permission/knowledge.

Effects of Hacking:

1. This can lead to identity theft or gaining personal information.
2. The data can be deleted by the hacker.
3. The data can be corrupted by the hacker.
4. The data can be changed/altered by the hacker.

Prevention of Hacking:

1. It can be prevented using firewalls or proxy servers.
2. It can be prevented by using strong passwords and user ids.
3. It can be prevented by using biometrics.
4. It can be prevented by using two-step verification.
5. It can be prevented by using anti-hacking software.

Note regarding Encryption:

- The use of encryption won't stop hacking.

- The hackers can still access the data and corrupt it, change it, or delete it.
- The encryption simply makes data incomprehensible without decryption key/algorithm.

Ethical Hacking:

- Ethical hacking is when companies authorize paid hackers to check out their security measures and test how robust their computer systems are to hacking attacks.
- It is a legal act as long as it is done with the owner's permission to find loopholes in the system and offer solutions to improve it.
- Malicious hacking (described above) takes place without the user's permission, and it is always an illegal act.

Explanations of Methods used for Prevention of Hacking:

1. **It can be prevented by using firewalls.**

The firewalls monitor incoming and outgoing traffic. It allows the setting of a criteria (blacklist/whitelist). It checks that if the traffic meets the certain criteria set by the user and blocks access to signals that do not meet criteria (blacklist/whitelist). It sends signal to warn the user. It restricts access to specific applications. It blocks entry/exit by specific ports.

2. **It can be prevented by using proxy servers.**

The firewalls monitor incoming and outgoing traffic. It allows the setting of a criteria (blacklist/whitelist). It checks that if the traffic meets the certain criteria set by the user and blocks access to signals that do not meet criteria (blacklist/whitelist). It sends signal to warn the user.

3. **It can be prevented by using strong passwords.**

The user should create a strong password e.g., it must be long and contain 4 types of characters such as lowercase and uppercase letters, symbols, and numbers etc. User must change the password regularly on monthly basis. The user's system should lock out after a fixed number of wrong attempts have been made for password.

4. **It can be prevented by using biometrics.**

The biometrics rely on unique characteristics of human beings such as fingerprint scans, retina scans etc. Since this biological data required for entry is unique to the individual user, it is very difficult to replicate. The system should lock out after a fixed number of wrong attempts have been made for biometrics.

5. **It can be prevented by using two-step verification.**

The two-step verification allows user to sign in to their account in two steps using their password and device (phone). The additional data such as a pin code is sent to a device that is pre-set by the user, so it is difficult for hacker to obtain that specific device and therefore the pin code. Moreover, the data (pin code) has to be entered into the same system so if attempted from a different location, it will not be accepted.

Malware:

- It is a software program designed to damage data/disrupt the computer system.
- It replicates itself and fills the hard disk.
- It is one of the biggest risks to the integrity and security of data on a computer system.

Vulnerabilities that a Malware can exploit in computer systems:

1. A malware could be downloaded by opening an email attachment from unknown sources.
2. A malware could be downloaded if virus definitions are not updated which would allow for recently developed viruses to attack the computer system.
3. A malware could be downloaded by attaching a portable storage device.
4. A malware could be downloaded by accessing a suspicious website.
5. A malware could be downloaded if the Operating System is not up to date.
6. A malware could be downloaded by a file downloaded from the Internet.
7. A malware could be downloaded due to buffer overflow.
8. A malware could be downloaded through a software that is not up to date.
9. A malware could be downloaded if the anti-virus/anti-malware software is not up to date.
10. A malware could be downloaded if regular virus/malware scans are not performed.
11. A malware could be downloaded if a firewall is not set up correctly.

Methods that can be used to restrict the effect of Malware:

1. A malware can be restricted by an anti-malware software running in the background.
2. A malware can be restricted by using an up-to-date anti-virus software with updated virus definitions to quarantine viruses.
3. A malware can be restricted by logging off when not using a computer.
4. A malware can be restricted by not clicking on links in emails from unknown source to redirection to a fake/bogus website.
5. A malware can be restricted by ensuring the firewall is enabled to enforce rules for downloading data.
6. A malware can be restricted by using strong passwords.
7. A malware can be restricted by not sharing passwords.

There are many forms/types of malwares, and the following ones will be considered (according to syllabus):

1. Virus
2. Worm
3. Trojan horse
4. Adware
5. Ransomware
6. Spyware

1) Virus:

- It is a software that replicates (copies) itself and is designed to amend, delete, corrupt, or copy data and files on a user's computer without their consent/knowledge.
- The viruses need an active host program on the target computer or an operating system that has already been infected before they can actually run and cause harm.

Effects of Virus:

1. It can cause the computer to crash/run slow/generate errors.
2. It can delete (damage) files/data.
3. It can corrupt files/data.
4. It can fill up the storage space/hard disk with unnecessary data.
5. It can stop the hardware being able to communicate.
6. It can spread to other devices on the network.

Prevention of Virus:

1. It can be prevented by using an up-to-date anti-virus/anti-malware software.
2. It can be prevented by using a firewall or proxy server.
3. It can be prevented if the user does not download software or data from unknown sources.
4. It can be prevented if the user does not share external storage devices.
5. It can be prevented if the user is careful when opening emails/attachments from unknown senders.
6. It can be prevented if the user does not connect computer to network (use as stand-alone computer).
7. It can be prevented by limiting access to the computer.

Note regarding Back-ups:

- The backing up of files won't guard against viruses since the virus may have already attached itself to the backed-up files. However, the use of back-up may simply reinstall the virus.

Tasks carried out by Anti-Virus Software:

1. It scans files for viruses and detects/identifies a virus.
2. It can constantly run in the background.
3. It can run a scheduled scan.
4. It can automatically keep updating virus definitions.
5. It can quarantine a virus.
6. It can delete a virus.
7. It completes heuristic checking.
8. It checks data before it is downloaded and then accordingly either stops download or notifies the user of a possible virus.

Examples of when an Anti-Virus Software (Virus Checker) should perform a check:

1. It checks for boot sector viruses when the machine is first turned on.
2. It checks for viruses when an external storage device is connected.
3. It checks a file/web page for viruses when it accessed/downloaded

Different ways through which a malware/virus could be introduced to a computer system or a website/network:

1. A hacker hacked into the computer/network and downloaded the malware onto the computer/network.
2. The user clicked on a link or attachment from an email or web page and the malware could be embedded into the link or attachment.
3. The user downloaded a file from an email or web page and the malware could be embedded into the file.
4. The user opened an infected software package which triggered the malware to download onto the computer/network.
5. The user inserted an infected portable storage device which downloaded the malware onto the computer/network.
6. The firewalls were turned off and so the malware was not detected when it was entering the computer/network.
7. The anti-malware was turned off and so the malware was not detected when virus containing files were downloaded.

2) Worm:

- A standalone/independent piece of malicious software that can replicate/duplicate itself automatically using a network.
- They use networks to search for computers with weak security.
- They remain inside applications which allows them to move throughout networks.
- Unlike viruses, they don't need an active host program to be opened in order to do any damage.
- Worms replicate without targeting and infecting specific files on a computer and they rely on security failures within networks to permit them to spread unhindered.
- Worms frequently arrive as message attachments and only one user opening a worm-infested email could end up infecting the whole network.
- Worms tend to be problematic because of their ability to spread throughout a network without any action from an end-user; whereas viruses require each end-user to somehow initiate the virus.
- All of this makes them more dangerous than viruses.

Effects of Worm:

1. It can corrupt the user's computer.
2. It can delete files/data.
3. It can consume bandwidth.
4. It can overload web servers.

Prevention of Worm:

As with viruses, the same safeguards should be employed, together with the running of an up-to-date antivirus program.

1. It can be prevented by using an up-to-date anti-virus/anti-malware software.
2. It can be prevented by using a firewall or proxy server.
3. It can be prevented if the user does not download software or data from unknown sources.
4. It can be prevented if the user is careful when opening emails/attachments from unknown senders.
5. It can be prevented by keeping the softwares and the OS up to date.
6. It can be prevented if the user does not connect computer to network (use as stand-alone computer).

3) Trojan Horse:

- It is a malicious program often disguised as legitimate software but with malicious instructions embedded within it.
- They replace all or part of the legitimate software with the intent of carrying out some harm to the user's computer system.
- It is usually sent as an email attachment or downloaded from an infected website.
- It could be transmitted via a fake anti-virus program that pops up on the users screen claiming that their computer is infected, and an action needs to be taken.
- Once the user runs this fake program, the Trojan horse will give cyber criminals access to personal information on the computer, such as IP addresses, passwords, and other personal data.

Effects of Trojan Horse:

1. It can give cyber criminals access to users personal information.
2. It can export files, modify data, or even delete files.
3. It can lead to identity theft or stealing of personal data.

Prevention of Trojan Horse:

The Trojan horse relies on tricking end-users, and so firewall and other security systems are often useless since the user can overrule them and initiate the running of the malware themselves.

1. It can be prevented if the user does not download software or data from unknown sources.
2. It can be prevented if the user is careful when opening emails/attachments from unknown senders.
3. It can be prevented by keeping the softwares and the OS up to date.

Note regarding Trojan horse, Spyware, Adware & Ransomware:

- The spyware (including key logging software), adware and ransomware are often installed on a user's computer via Trojan horse malware.
- The Trojan horse malware tricks the end-users into downloading a fake program and then that fake program installs other types of malwares such as spyware, adware and ransomware.

4) Adware (advertising software):

- It is a type of malware that displays unwanted advertisements on an end-users computer or device.
- The advertisements are delivered through pop-up windows or a browser's toolbar.
- It could redirect a user's browser to a website that contains promotional advertising.
- It is commonly activated unknowingly when users are trying to install legitimate applications that adware is bundled with.
- It is hard to remove as it defeats most anti-malware software since it can be difficult to determine whether or not it is harmful.

It is not necessarily harmful, but it can be used for malicious purposes as well.

Effects of Adware:

1. It can highlight weaknesses in a user's security defenses.
2. It can hijack a browser and create its own default search requests.
3. It can slow down the user's computer/device and browser.
4. It can install viruses and/or spyware.
5. It can cause a program to crash or a device to freeze if too many ads show up.

Prevention of Adware:

1. It can be prevented by using an up-to-date anti-virus/anti-malware software.
2. It can be prevented by using a firewall or proxy server.
3. It can be prevented if the user does not download software or data from unknown sources.
4. It can be prevented if the user is careful when opening emails/attachments from unknown senders.
5. It can be prevented by not clicking on pop-up ads.
6. It can be prevented by keeping the softwares and the OS up to date.

5) Ransomware:

- It is a type of malware designed to encrypt data/files on a user's computer and hold the victims data/information at ransom (hold the data as hostage).
- The user's computer screen is locked, and this malware restricts access to the computer and encrypts all the data.
- The cybercriminal then demands ransom in exchange for decryption key.
- It can be installed on a user's computer by way of a Trojan horse or through social engineering.
- It not only targets home users, but businesses can also become infected with ransomware.

The payment of ransom does not guarantee the encrypted files will be released but it only guarantees that the cybercriminals receive the victim's money, and in some cases, their banking information.

In addition, decrypting files does not mean the malware infection itself has been removed

Effects of Ransomware:

1. It can cause temporary or permanent loss of sensitive information/data.
2. It can cause disruption to regular operations.
3. It can cause financial losses incurred to restore systems and files.
4. It can cause potential harm to an organizations reputation.

Prevention of Ransomware:

1. It can be prevented by using an up-to-date anti-virus/anti-malware software.
2. It can be prevented by using a firewall or proxy server.
3. It can be prevented if the user does not download software or data from unknown sources.
4. It can be prevented if the user is careful when opening emails/attachments from unknown senders.
5. It can be prevented by keeping the softwares and the OS up to date.
6. It can be prevented by regularly backing-up key files/data so the user can avoid having to pay a ransom.

Cyber Security Threats (Internet Risks) used to obtain personal data:

1. Hacking
2. Phishing
3. Pharming
4. Spyware (keylogger)

6) Spyware:

- It is a malicious software that monitors the user's activity by reading key presses on a user's keyboard.
- It tracks/records the key presses, and the data is relayed/sent to a third party/originator of the software.
- The collected data/key presses are analyzed to obtain sensitive data (e.g., passwords).
- It is also known as key logging software.

How Keylogging (Spyware) software can be used to gain unauthorized access to a user's account OR find out the username/password of a user (short description):

- The keylogger is downloaded without the user's knowledge.
- The keylogger records key presses/screen activity.
- The data is relayed back to a third party.
- The data is analyzed and common patterns in data could reveal log-in details.
- Those details can then be used to log into the user's account.

How Spyware can be used to obtain a user's password (detailed explanation):

- The user could have been sent an email with an attachment/link containing the spyware.
- The user could have clicked a link on an untrusted website.
- When the attachment/link was clicked the spyware was downloaded onto the user's computer without user's knowledge.
- The spyware records all the key logs/key presses from the user's keyboard.
- The recorded key logs/data is sent back to the creator of the spyware.
- The key logs/data is analyzed and common patterns in the key logs/data could have allowed a password to be identified/revealed.

Effects of Spyware:

1. It gives the originator access to all data entered using a keyboard on the user's computer.
2. It can lead to stealing of personal information as the originator can analyze the key presses to find sensitive data (e.g., passwords, credit card details, bank account numbers etc.).
3. It can install other spyware programs.
4. It can read cookie data.
5. It can change a user's default web browser.

Prevention of Spyware:

1. It can be prevented by using anti-spyware software.
2. It can be prevented by using virtual (onscreen) keyboard and drop-down boxes:
   This means keylogger cannot collect data.
3. It can be prevented by using a firewall or proxy server.
4. It can be prevented by using two-step verification:
   The extra data is sent to the device making it difficult for the hacker to obtain it.
   The data has to be entered into the same system and if attempted from a remote location, it will not be accepted.
5. It can be prevented by using a biometric device:
   The person's biological data such as their fingerprint is also required.
6. It can be prevented if only a part of the password is required:
   The hacker cannot get the full password.
7. It can be prevented if the user is alert and he/she looks out for clues that their keyboard activity is being monitored.

Tasks carried out by Anti-Spyware Software:

1. It scans the computer system for spyware.
2. It removes any spyware that is found.
3. It checks data before it is downloaded and then accordingly either stops download or warns the user if spyware is found.
4. It encrypts files to make the data more secure in case it is spied on.
5. It encrypts keyboard strokes to help remove the risk posed by the keylogging aspects of some spyware.
6. It blocks access to a user's webcam and microphone which can be used to collect information without the user's knowledge.
7. It scans for signs that the user's personal information has been stolen and warns the user if this has happened.

Purpose of drop-down boxes & virtual (onscreen) keyboards:

- These are used to defeat spyware/keylogging software.
- The keylogger records key presses and in the case of drop-down boxes or onscreen keyboards, there is no key pressed.
- It means keylogger cannot collect data and then relay it to the third party/originator.

Spyware & Virus:

Main Similarities between a Spyware & Virus:

1. Both are pieces of malicious software.
2. Both are downloaded/installed/run without the user's knowledge.
3. Both can pretend to be/are embedded in other legitimate software when downloaded.
4. Both try to avoid the firewall.
5. Both run in the background.

Main Differences between a Spyware & Virus:

1. The virus can damage computer data whereas spyware only records/accesses data.
2. The virus does not send data out of the computer whereas spyware sends recorded data to third parties.
3. The virus replicates itself whereas spyware does not replicate itself.

Virus, Spyware & Denial of Service (DoS):

The following table compares Virus, Spyware & Denial of Service (DoS):

Statement	Virus (✓)	Spyware (✓)	DoS (✓)
Captures all data entered using a keyboard		✓	
Can be installed onto a web server	✓	✓	
Prevents access to a website			✓
Is malicious code on a computer	✓	✓	
Is self-replicating	✓		
Damages the files on a user's hard drive	✓		

Phishing:

- It is a legitimate-looking email sent to a user.
- It encourages the user to click and open a link in the email or attachment.
- This link/attachment redirects the user to a fake website without their consent/knowledge.
- The user is encouraged to enter personal details into a fake website (e.g., financial information of user).
- It is designed to obtain/steal personal details from a user.

Spear Phishing:

- It is where the cybercriminal targets specific individuals or companies to gain access to sensitive financial information or industrial spying.
- The regular phishing is not specific regarding who the victims are.

Effects of Phishing:

1. The creator of the email can gain personal data such as bank account numbers from users when they visit the fake website.
2. This can lead to fraud or identity theft.

Prevention of Phishing:

1. It can be prevented by looking out for https and/or the green padlock symbol in the address bar (both suggest that traffic to and from the website is encrypted).
2. It can be prevented if the user does not open/click emails or attachments from unknown sources.
3. It can be prevented by using firewalls as some of them can detect fake/bogus websites.
4. It can be prevented by using an up-to-date browser, with all of the latest security upgrades, running, and run a good firewall in the background at all times.
5. It can be prevented by Internet Service Providers (ISPs) as some of them filter out phishing emails automatically.
6. It can be prevented if the user is always cautious when opening emails or attachments.

Note regarding Phishing:

- The legitimate looking emails often use large companies, such as well-known banks, to try to convince customers that the email is authentic.

Pharming:

- It is a malicious code/malware/software that is downloaded/installed on a user's computer without user's knowledge.
- It redirects the user from a correct URL to a fake/fraudulent website.
- The user is encouraged to enter personal details into a fake website (e.g., financial information of user).
- It is designed to obtain/steal personal details from a user.

Why does Pharming pose a threat to data security?

- It redirects users to a fake or malicious website set up by, for example, a hacker.
- The redirection from a legitimate website can be done using DNS cache poisoning.
- Every time a user types in a URL, their web browser contacts the DNS server.
- The IP address of the website is then sent back to their web browser.
- However, DNS cache poisoning changes the real IP address values to those of the fake website consequently, the user's computer connects to the fake website.

Effects of Pharming:

1. The creator of the code can gain personal data such as bank account numbers from users when they visit the fake website.
2. This can lead to fraud or identity theft.

Prevention of Pharming:

1. It can be prevented by using antivirus software, which can detect unauthorized alterations to a website address and warn the user.
2. It can be prevented by using anti-spyware software as some of them can identify and remove the pharming code from the hard drive.
3. It can be prevented by using modern web browsers that alert users to pharming and phishing attacks.
4. It can be prevented by trusting and using only secure websites (e.g., those with https protocol or those having a green padlock sign next to the website URL).
5. It can be prevented by checking and confirming that the URL exactly matches the intended site.
6. It can be prevented if the user is alert and he/she looks out for clues that they are being redirected to another website.

Phishing & Pharming:

Purpose of Phishing & Pharming:

- The purpose is to obtain a user's personal data.

Main Similarities between Phishing & Pharming:

1. Both are designed to steal/collect personal data.

2. Both pretend to be a real company/person.
3. Both use fake websites.

Main Differences between Phishing & Pharming:

1. Phishing involves the use of an email whereas pharming involves installing malicious code.
2. Phishing involves clicking a link or opening an attachment whereas pharming creates a redirection.

Social Engineering:

- It refers to all techniques aimed at manipulating a potential victim into revealing specific information or performing a specific action for illegitimate reasons.
- It occurs when a cybercriminal creates a social situation that can lead to a potential victim dropping their guard.
- It involves manipulation of people into breaking their normal security procedures and not following best practice.

It does not involve hacking since the user willingly allows the cybercriminal to have access to their computer for downloading malicious software or visits fake websites. The user is rushed into making rash decisions due to certain human emotions.

There are five types of threat that commonly exist:

1) Instant Messaging:

- The malicious links are embedded into instant messages.
- For example, a message of important software upgrade.
- This threat relies on the user's curiosity.

2) Scareware (fake anti-virus that looks real):

- It uses a pop-up message that claims that the user's computer is infected with a virus.
- The user is asked to download the fake anti-virus immediately.
- This threat relies on the user's fear.

3) Emails/Phishing Scams:

- The user is tricked by the apparent genuineness of an email and opens a link in the email.
- This link redirects the user's browser to a fake/bogus website.
- This threat relies on the user's trust of well-known companies.

4) Baiting:

- The cybercriminal leaves a malware-infected memory stick at a place where it can be found.
- The finder picks up the memory stick and plugs it into their computer and unwittingly downloads malicious malware.
- This threat relies on the user's curiosity.

5) Phone Calls:

- A so-called IT professional may call a user on their mobile claiming their device has been compromised in some way.
- The user is advised to download some special software that allows the cybercriminal to take over the user's device, giving them access to personal information.
- This threat relies on the user's fear.

The whole idea of social engineering is based on the exploitation of certain human emotions. The three most common ones to exploit are:

1) Fear:

- The user is panicked into believing their computer is in immediate danger and isn't given time to logically decide if the danger is genuine or not.

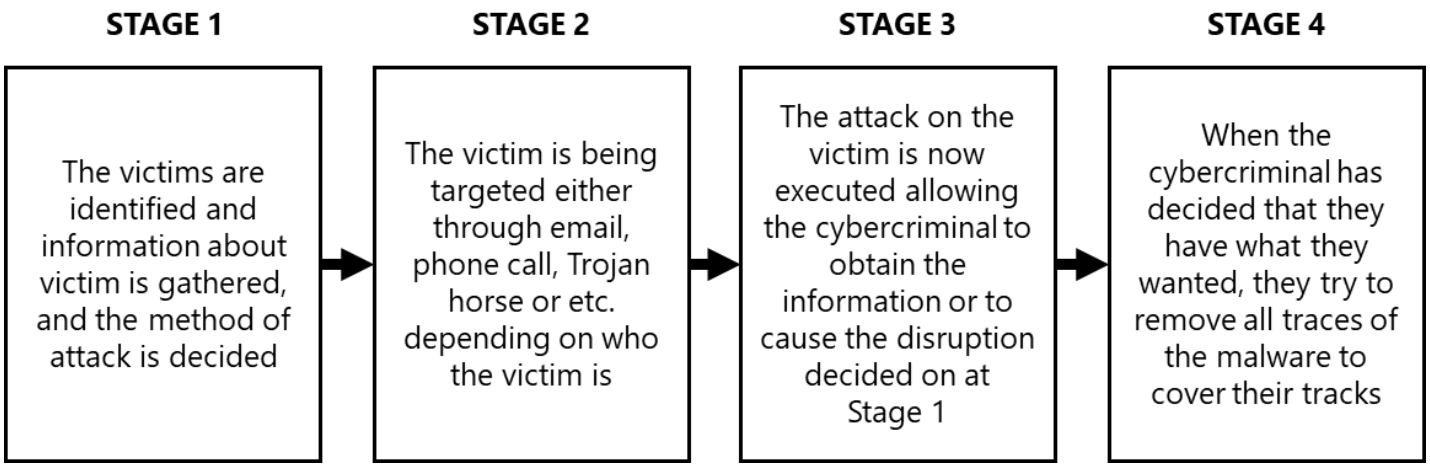
2) Curiosity:

- The user can be tricked into believing they have won a car, or they find an infected memory stick which increases curiosity of users.
- For the car, they give their details willingly to win the car which may involve credit card details to pay for delivery or road tax of the car.
- For the memory stick, the user may be curious to find who it belongs to and ends up plugging it into their computer without thinking clearly.

3) Empathy & Trust:

- It involves a real belief that all genuine-sounding companies can be trusted.
- The user responds to emails or phone calls coming from such companies on behalf of trust.

Stages involved in a typical Social Engineering Scam:



Exam Style Questions:

Question 1:

Two internet risks are phishing and pharming.

Describe what is meant by phishing and pharming.

Phishing .....

.....

.....

.....

.....

.....

Pharming .....

.....

.....

.....

.....

.....

[6]

Answer:

Question	Answer	Marks
4	Any **six** from: Phishing – Legitimate looking email sent to user – encourages user to **click a link** that directs user to a fake website – User encouraged to enter personal details into a fake website // designed to obtain personal details from a user Pharming – Malicious code/malware is downloaded/installed // software downloaded without users' knowledge – … that **re-directs** user to fake website (when legitimate URL entered) – User encouraged to enter personal details into a fake website // designed to obtain personal details from a user	**6**

Question 2:

Name **three** of these risks. For each, state why it is a risk and describe how the risk can be minimised.

Security risk 1 .....

Why it is a risk .....

.....

.....

How to minimise the risk .....

.....

.....

Security risk 2 .....

Why it is a risk .....

.....

.....

How to minimise the risk .....

.....

.....

Security risk 3 .....

Why it is a risk .....

.....

.....

How to minimise the risk .....

.....

.....

[9]

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

Answer:

1 mark for each risk + 1 mark for corresponding reason why it is a risk and 1 mark for method of minimisation

Risk:	hacking
Reason:	illegal/unauthorised access to data deletion/amendment of data
Minimised:	use of passwords/user ids use of firewalls encrypt data/encryption

Risk:	virus
Reason:	can corrupt/delete data cause computer to crash/run slow can fill up hard drive with data
Minimised:	use of /run anti-virus (software) do not download software or data from unknown sources

Risk:	spyware/key logging (software)
Reason:	can read key presses/files/monitors on a user's computer
Minimised:	use of/run anti-spyware (software) use data entry methods such as drop-down boxes to minimise risk

Risk:	phishing
Reason:	link/attachments takes user to fake/bogus website website obtains personal/financial data
Minimised:	do not open/click emails/attachments from unknown sources some firewalls can detect fake/bogus websites

Risk:	pharming
Reason:	redirects user to fake/bogus website redirection obtains personal/financial data
Minimised:	only trust secure websites, e.g. look for http**s** check the URL matches the intended site

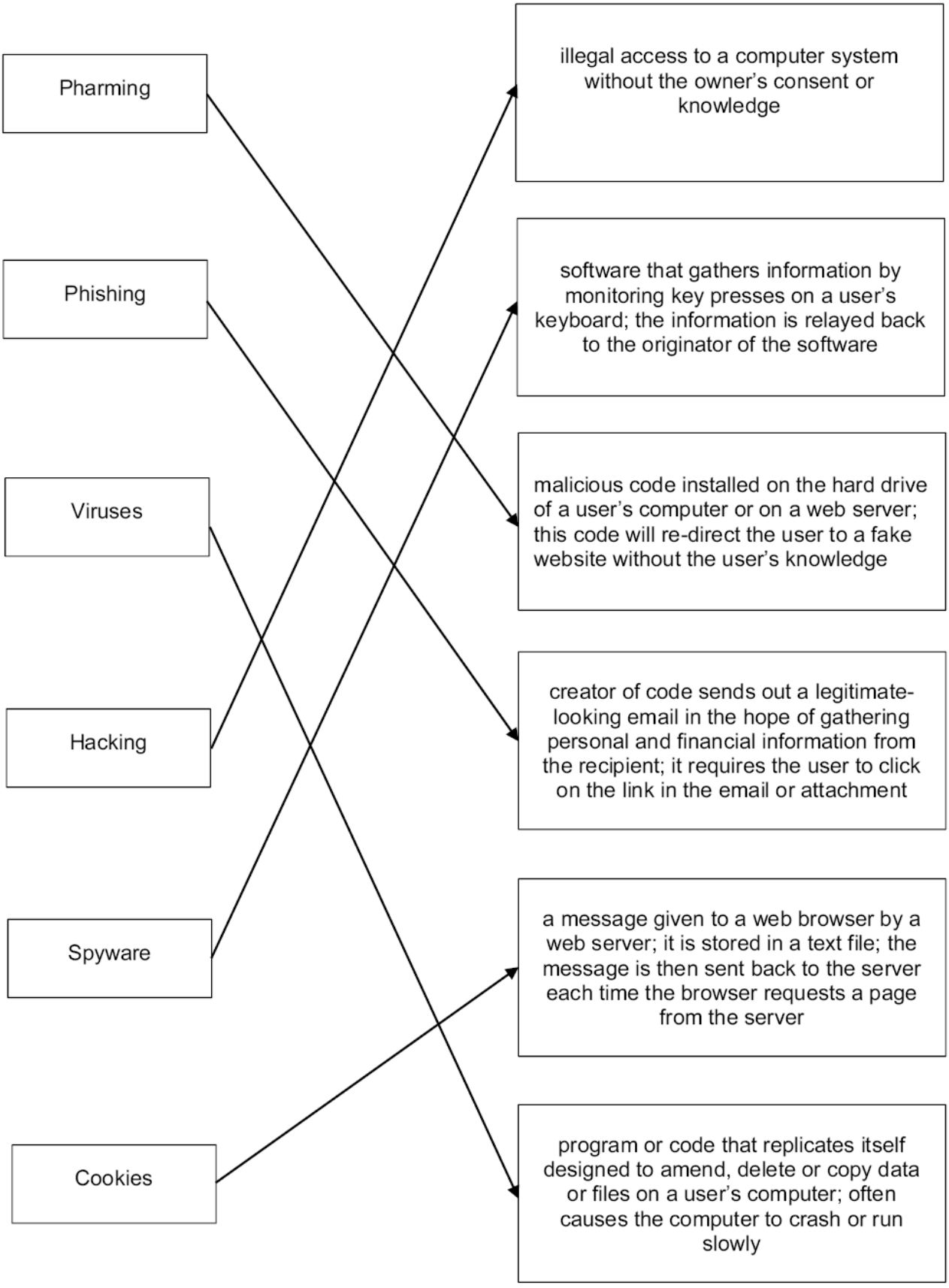
Risk:	credit card fraud/identity theft
Reason:	loss of money due to misuse of card/stealing data
Minimised:	set passwords encrypt data/encryption

Question 3:

Security issue	Description
Pharming	illegal access to a computer system without the owner's consent or knowledge
Phishing	software that gathers information by monitoring key presses on a user's keyboard; the data is sent back to the originator of the software
Viruses	malicious code installed on the hard drive of a user's computer or on a web server; this code will re-direct the user to a fake website without the user's knowledge
Hacking	creator of code sends out a legitimate-looking email in the hope of gathering personal and financial information from the recipient; it requires the user to click on the link in the email or attachment
Spyware	a message given to a web browser by a web server; it is stored in a text file; the message is then sent back to the server each time the browser requests a page from the server
Cookies	program or code that replicates itself; designed to amend, delete or copy data or files on a user's computer; often causes the computer to crash or run slowly

[7]

Answer:



[5]

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

Question 4:

(c) Security of data is very important.

Three security issues are viruses, pharming and spyware.

Explain what is meant by each issue.

Viruses: .....

.....

.....

.....

Pharming: .....

.....

.....

.....

Spyware: .....

.....

.....

.....

[6]

Answer:

(c) **2** marks for each term described

Viruses:
- program/software/file that replicates (copies) itself
- intends to delete or corrupt files//fill up hard disk space

Pharming:
- malicious code stored on a computer/web server
- redirects user to fake website to steal user data

Spyware:
- monitors and relays user activity e.g. key presses//key logging software
- user activity/key presses can be analysed to find sensitive data e.g. passwords [6]

Question 5:

Name each of the potential security issues described in the **five** statements below:

Statement	Security issue
The act of gaining unauthorised access to a computer system	.....
Program code that can replicate itself with the intention of deleting or corrupting files stored in a computer	.....
A small file sent by a web server to a web browser; every time the user visits the website, data about user preferences is collected	.....
The act of illegally changing the source code of a program so that it can be exploited for another use	.....
Malicious code installed on a user's hard drive or a web server which redirects the user to a fake website without their knowledge	.....

[5]

Answer:

- Hacking
- Virus
- Cookies
- Cracking
- Pharming

[5]

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

Question 6:

A company discovers malware on its network.

Explain **two** ways that the malware could have been introduced to the company's network.

.....

.....

.....

.....

.....

.....

.....

..... [4]

Answer:

Question	Answer	Marks
8	**Four** from: • A hacker could have hacked the network … • … and downloaded the malware onto the network • Clicking a link/attachment/downloaded a file from an email/on a webpage … • … the malware could have been embedded into the link/attachment/file • Opening an infected software package … • … this would trigger the malware to download onto the network • Inserting an infected portable storage device … • … when the drive is accessed the malware is downloaded to the network • Firewall has been turned off … • … so malware would not be detected/checked for when entering network • Anti-malware has been turned off … • … so malware is not detected/checked for when files are downloaded	**4**

Question 7:

Hans has a website selling comic books. Customers can create an account to buy the comic books.

Customers enter a username and password to log in to their account.

(a) Customers may worry about keylogging software being used to gain unauthorised access to their account.

(i) Describe how keylogging software can be used to gain unauthorised access to a customer's account.

.....

.....

.....

.....

.....

.....

.....

..... [4]

(ii) Identify a feature that Hans can add to the website to limit the threat of keylogging software.

..... [1]

Answer:

Question	Answer	Marks
7(a)(i)	Any **four** from: – Keylogger is downloaded without knowledge (by example) – Keylogger records key presses – Data is relayed back to third party – Data is analysed // Patterns in data could reveal log-in details … – … details can then be used to log into the account	4
7(a)(ii)	Any **one** from: – Use drop-down boxes for password – Two-step verification (by example) – Partial password requests – Onscreen / virtual keyboard	1

Question 8:

(c) The company is concerned about a distributed denial of service (DDoS) attack.

(i) Describe what is meant by a DDoS attack.

.....

.....

.....

.....

.....

.....

.....

..... [4]

(ii) Suggest **one** security device that can be used to help prevent a DDoS attack.

..... [1]

Answer:

2(c)(i)	Any **four** from: • multiple computers are used as bots • designed to deny people access to a website • a large number / numerous requests are sent (to a server) … • … all at the same time • the server is unable to respond / struggles to respond to all the requests • the server fails / times out as a result.	**4**
2(c)(ii)	firewall **OR** proxy server	**1**

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

Question 9:

Spencer finds out that his online music account has been accessed by an unauthorised person.

He believes his personal details for the account were obtained using phishing.

(a) Explain how the personal details could have been obtained using phishing.

.....

.....

.....

.....

.....

..... [3]

(b) Give **two** other Internet security risks that could have been used to obtain the personal details.

1 .....

2 .....

[2]

Answer:

Question	Answer	Marks
4(a)	– Legitimate looking/fake email sent to user – … that contains a link to a fake website – User **clicks link** and enters personal details (into fake website)	**3**
4(b)	Any **two** from: – Pharming – Spyware – Hacking/cracking	**2**

Question 10:

Clive has a laptop computer that he uses for his business. He enters a username and password to log in to his laptop.

Clive is worried about spyware being used to find out his username and password.

(a) Describe how spyware could be used to find out Clive's username and password.

.....

.....

.....

.....

.....

.....

.....

..... [4]

(b) The threat of spyware makes Clive concerned about typing a password to log in to his laptop.

Give an example of how Clive could log in securely without typing a password.

..... [1]

Answer:

Question	Answer	Marks
10(a)	Any **four** from: – Example of spyware e.g. Keylogger is used – Spyware is downloaded without knowledge (by example) – Spyware records key presses / screen clicks / screen activity – Data is relayed back to third party – Data is analysed // Patterns in data could reveal log-in details … – … details can then be used to log into the laptop (remotely)	4
10(b)	– Biometric device – Two step authentication	1

5.3.2 Solutions of Cyber Security Threats:

There are many solutions to keep data safe from cyber security threats.

Access Levels:

- It involves having different levels of access for different people by using a username and password.
- The different access rights are set up for individuals/group of users.
- It allows specific people to have access to certain data.
- It restricts actions of specific users such as read, write, and delete data.
- This stops users from reading/editing data they are not permitted to access.

Most systems have access levels depending on a person's level of security. The levels of access are particularly important when:

using Databases:

- It is essential to determine who has the right to read, write and delete data.
- The different views of data tables allow different users to only have access to certain data.

using Social Networks (e.g., Facebook):

There are four access levels:

1. Public access (this refers to the data anyone from the general public can access).
2. Friends (only people identified as 'friends' by the owner of the data can see certain data).
3. Custom (this allows the user to further refine what data can be seen by 'friends' allowing them to exclude certain content from selected people).
4. Data owner (this is the data only the owner of the data can see).

The social networking applications allow the users to use privacy settings rather than passwords to decide the level of access.

Anti-Malware:

The two most common types of anti-malware are anti-virus and anti-spyware:

Anti-Virus Software:

- It scans files for viruses and detects/identifies a virus.
- It can constantly run in the background.
- It can run a scheduled scan.
- It can quarantine a virus.
- It can delete a virus.
- It completes heuristic checking.
- It checks data before it is downloaded and then accordingly either stops download or notifies the user of a possible virus.

Examples of when an Anti-Virus Software (Virus Checker) should perform a check:

1. It checks for boot sector viruses when the machine is first turned on.
2. It checks for viruses when an external storage device is connected.
3. It checks a file/web page for viruses when it accessed/downloaded

Anti-Spyware Software:

- It scans the computer system for spyware.
- It removes any spyware that is found.
- It checks data before it is downloaded and then accordingly either stops download or warns the user if spyware is found.
- It encrypts files to make the data more secure in case it is spied on.
- It encrypts keyboard strokes to help remove the risk posed by the keylogging aspects of some spyware.
- It blocks access to a user's webcam and microphone which can be used to collect information without the user's knowledge.
- It scans for signs that the user's personal information has been stolen and warns the user if this has happened.

Authentication:

- It is the process of determining whether somebody/something is who/what they claim to be.
- It is frequently done through log on passwords, biometrics & two-step verification.
- It helps to prevent unauthorized access to data.

Authentication Methods/Techniques:

1. Usernames and Passwords
2. Biometrics (fingerprint scanner, retina scanner, face recognition, voice recognition)
3. Two-step Verification

Methods that can be used to prevent confidential data being viewed:

1. Encryption
2. Password
3. Adding a biometric device to the computer system
4. Using two-step verification/two-factor authentication
5. Physically locking the computer away in a secure place

1) Usernames and Passwords:

- The user has a username and password which are checked/matched against a secure file to allow a user to gain access to, for example, a bank website.
- If either is incorrect or does not match up, then access is denied.
- The passwords should be strong to prevent unauthorized access to data or systems.
- The passwords should be updated on a regular basis in case they have been seen by someone else, illegally, or accidentally.
- This is to ensure that a system cannot be accessed without a valid username and password therefore preventing unauthorized access to the system.

The Usernames and Passwords are frequently used when accessing email accounts, carrying out online banking or shopping or accessing social networking sites

The Passwords must be protected by:

1. running anti-spyware software to make sure that password is not being relayed back to the originator of the spyware.
2. changing passwords on a regular basis in case they have been seen by someone else, illegally, or accidentally.
3. Using strong passwords which are not easy to guess or crack.

The strong Passwords should contain:

1. at least one capital letter
2. at least one numerical value
3. at least one other keyboard character (such as @, *, &)

Example of a strong password: Sy12@#TT90kj=0
Example of a weak password: GREEN

Forget/Reset Password:

- If a user forgets their password or they need to reset it, they will be sent an email.
- The email contains a link to a web page where they can reset their password.
- This is done as an added precaution in case an unauthorized person has tried to change the user's password.

2) Biometrics:

- The biometrics relies on the unique characteristics of human beings.
- These are the unique features of individuals that cannot be guessed.

Why modern smartphones are secured with a biometric system:

- It adds extra level of security
- The biometric device requires properties unique to an individual.
- It allows quicker access as there is no need to remember or input a password.

Biometric Methods/Techniques:

i. Fingerprint scans
ii. Retina scans
iii. Face recognition
iv. Voice recognition

(i) Fingerprint Scans:

- The images of fingerprints are compared against previously scanned fingerprints stored in a database.
- The system compares patterns of 'ridges' and 'valleys' of a finger which are fairly unique.
- If they match, then access is allowed; otherwise denied.
- The accuracy of the scan is about around 1 in 5000.

Benefits of Fingerprint scanning:

1. The fingerprints are unique and very difficult to replicate, therefore it can improve security.
2. The other security devices such as magnetic cards to gain entry to a building can be lost or stolen which makes them less effective.
3. It would be impossible to 'sign in' for somebody else since the fingerprints would match with only one person on the database.
4. The fingerprints cannot be misplaced unlike other security devices as the user always has them.

Drawbacks of Fingerprint scanning:

1. It is relatively expensive to install and set up fingerprint scanners.
2. If a user's fingers are damaged through an injury, then it can affect the scanning accuracy.
3. Some people may regard any biometric device as an infringement of civil liberties.

(ii) Retina Scans:

- It uses infra-red to scan the unique pattern of blood vessels in the retina (at the back of the eye).
- It requires a person to stay still for 10 to 15 seconds while the scan takes place.
- It is very secure since nobody has yet found a way to duplicate the blood vessels patterns.
- If the blood vessel patterns match, then access is allowed; otherwise denied.
- The accuracy of the scan is about 1 in 10 million.

(iii) Face Recognition:

- It maps facial features from a photograph or video.
- The features are compared with the information stored in a database of known faces to find a match.
- The key parts of the face such as distance between eyes, width of nose etc. are compared.
- If the key parts/features of face match, then access is allowed; otherwise denied.

(iv) Voice Recognition:

- The system takes input of user's voice and then converts it into digital form.
- A few words spoken produce a digital wave pattern.
- The system compares this wave pattern to wave patterns stored in database to see if they match.
- If the wave patterns match, then access is allowed; otherwise denied.

Text-based & Biometric Password:

Text-based Password:

- It is a minimum number of characters that can be typed on a keyboard.
- It is set and can be changed by the user.

Biometric Password:

- It is a stored physical measurement such as a fingerprint.
- It is compared to a previously scanned human measurement.

Differences between Text-based & Biometric Password:

1. The text-based passwords are easier to hack than biometric passwords.
2. The biometric passwords are unique to that person and cannot be shared.

The following table compares the benefits and drawbacks of four common biometric techniques:

Biometric Technique	Benefits	Drawbacks
Fingerprint Scans	It is one of the most developed biometric techniques It is very easy to use It has relatively small storage requirements for the biometric data created	It is very intrusive for some people since it is still related to criminal identification It can make mistakes if the skin is dirty or damaged (e.g., skin cuts)
Retina Scans	It has very high accuracy There is no known way to replicate a person's retina	It is very intrusive It can be relatively slow to verify retina scan with stored scans It is very expensive to install and set up
Face Recognition	It is a non-intrusive method It is relatively inexpensive technology	It can be affected by changes in lightning, the persons' hair, change in age, and if the person is wearing glasses
Voice Recognition	It is a non-intrusive method The verification takes less than five seconds It is relatively inexpensive technology	A person's voice can be easily recorded & used for unauthorized access It has low accuracy An illness such as a cold can change a person's voice making absolute identification difficult or impossible

3) Two-step Verification:

- It allows the user to sign into their account in two steps using their username and password along with device.
- The user enters their username and a password.
- The pin code (OTP) is sent to an email or a text message on the device that is pre-set by the user, so it is difficult for hacker to obtain that specific device and therefore the pin code.
- The pin code has to be entered into the same system so if attempted from a different location, it will not be accepted.
- It is used predominantly when a user makes an online purchase using a credit/debit card as payment method.

Automatic Software Updates:

- It is keeping the software on computers and mobile phones/tablets up to date.
- It is applying patches to update the software security for protection against malware and improving software performance by removal of bugs and addition of new features.
- It helps in finding, fixing, and preventing security vulnerabilities in any installed application.
- The update may potentially disrupt the device following installation and the user might have to wait for another patch to make that right.
- The software updates are sometimes done overnight or when you log off the device.

Checking the Spelling & Tone of Communications & the URL attached to a link:

- It involves checking the spellings in the email and in the links and carefully checking the tone used in the communication.
- A professional, genuine organization will not send out emails which contain spelling or major grammatical errors such as amazzon.com
- If the email is rushing a user into doing something or if the language used seems inappropriate or incorrect then it could be a phishing email or worse.

The following five things must be looked out for:

1. **The email address itself:**

   No legitimate company will use an email address such as @gmail.com.
   The part of the address after '@' symbol should match the company's name.

   For example: account-update@amazon.com

2. **The tone of the email & bad spelling of words is a clear indication of a potential scam:**

   An email may look official but many spelling mistakes, grammatical errors and the domain name in the email address shows it didn't come from a legitimate company.
   The email may contain a 'LOG IN HERE' box and if the user clicks this box, they will reveal passwords and other key information since the user will be sent to a fake website.

For example:

From: PayPal <paypal@customer-notice55.com>
To: PayPal user 551-121-998
Sent: Feb 1st 2023 @ 10:55
Subject: Compremised Account [CaseID Nr: KX-003-551-121-998]

Dear Customer

We need you help to resolve issue with account. We have temporarily stop account due to problem's.
Unusual account activity on PayPal account means action need be taken immediately. If your not sure this was you, an unauthorized user might be trying to access your accounts. Please to log in here to change your password:

LOG IN HERE

This email contains many spelling mistakes, grammatical errors and the wrong domain name in the email address shows it didn't come from the legitimate PayPal company.
All these errors have been underlined for you to understand and notice.

3. **The misspelling of domain names in a link are very common errors found in emails sent by scammers and fraudsters:**

   This is known as typo squatting where names close to the genuine/original names are used to fool/trick a user.

   For example: www.gougle.com
   www.amozon.com

4. **The suspicious links:**

   The destination addresses should match the rest of the email.
   If an email is claiming to be from a company but when you hover over the link in the email the destination is a website with a different address where there is no mention anywhere of that company in the URL.
   It is a very high chance that it is a scam to try and collect the user's personal details.

   For example: An email from Netflix with the destination address such as:
   http://www.billing.com/id1234121XA3
   where there is no mention of Netflix anywhere in the URL

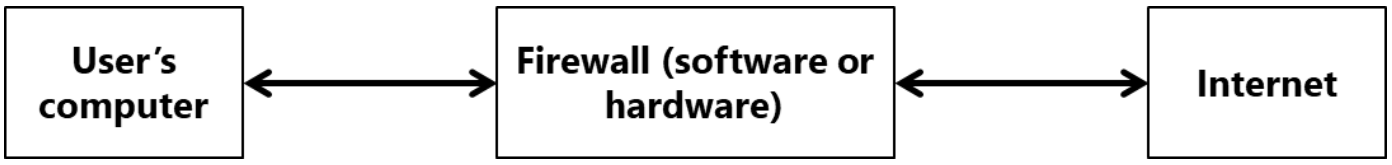
5. **The other errors like plain spelling mistakes, the access protocol & domain type:**

   The spelling of the address should match with the company name.
   If the company involves online payments, then it should be very secure with the https access protocol.
   If the company is a large and global one, then it should use '.com' domain type.

   For example: An address from TKMaxx company:
   http://www.tkmax.co.ie
   The spelling of the company is incorrect using 'tkmax' instead of 'tkmaxx'.
   The company involves online payments and so it's very likely to use secure links therefore, https protocol should be used instead of http.
   It is more likely to use '.com' since they are a large company instead of '.co'

Firewalls:

- It can be software installed on a computer or in some cases; it is a part of the operating system.
- It can be hardware interface which is located somewhere between the computer and the internet connection. In this case, it is referred to as a Gateway.
- It is used between the user's computer and an external network (e.g., the Internet) to examine the data traffic and filter information in and out of the computer to make sure it meets certain criteria.



It helps protect a computer system from hacking, malware (viruses & spyware), phishing and pharming.

Tasks carried out by a Firewall:

- It examines/monitors traffic going to and from a user's computer and a network/internet.
- It allows a user to set criteria/rules for the traffic (blacklist/whitelist).
- It checks whether incoming and outgoing traffic meets a given set of criteria/rules.
- It blocks/filters any traffic that doesn't meet the criteria/rules and gives the user a warning that there may be a security issue.
- It logs all incoming and outgoing traffic so that it can be later examined by the user.
- It can prevent viruses or hackers gaining illegal/unauthorized access.
- It blocks/filters access to specified IP addresses/websites set by the user and keeps a list of these IP addresses OR it maintains a blacklist/whitelist of IP addresses.
- It restricts access to specific applications and blocks entry/exit by specific ports.

It basically warns a user of any unauthorized software, unauthorized outgoing traffic or attempted unauthorized access to the computer system.

Note regarding Firewalls:

- It can be software and/or hardware.
- It does not act as intermediary servers like proxy servers do.
- It does not encrypt any data that is transmitted around a network.
- It cannot automatically stop all malicious traffic.
- It stops unauthorized access/hackers gaining access to computer network.
- It stops malware (viruses and spyware) reaching a computer.

Certain circumstances where the Firewall cannot prevent potential harmful traffic:

1. It cannot prevent individuals, on internal networks, using their own modems to bypass the firewall.
2. It cannot control employee misconduct or carelessness (for example, control of passwords or use of accounts).
3. It cannot prevent users on stand-alone computers who have disabled the firewall, leaving their computer open to harmful 'traffic' from the internet.

All of these issues require management control or personal control (on a single computer) to ensure that the firewall is allowed to do its job effectively.

How a Firewall helps keep data safe:

- It helps prevent hackers trying to gain unauthorized access to the system.
- It can monitor incoming and outgoing traffic.
- A user can set criteria or rules for traffic (blacklist/whitelist).
- It can check whether the traffic meets or defies the criteria rules.
- It can reject/block any traffic that does not meet or defies the criteria and sends signal to warn the user.
- It restricts access to specific applications and blocks entry/exit by specific ports.
- It blocks any unacceptable data and allows acceptable data to be sent into the system.
- It acts as a filter for incoming and outgoing data.

Applications of Firewalls in various scenarios:

Example 1:

A company is concerned that its employees are being distracted by using gaming websites at work.

How a firewall could help prevent this distraction:

- The company could use the firewall to set criteria.
- The gaming websites can be listed as blocked websites (ports can be blocked).
- The firewall would examine any traffic leaving the network.
- If it detects traffic requesting a listed website, it will block access to it.
- It keeps a log of all attempts to access blocked websites.

Example 2:

A parent is using a firewall to help prevent his children from accessing websites that he does not want them to see.

How the firewall helps prevent his children from accessing these websites:

- It examines outgoing traffic to check what is being requested.
- It examines incoming traffic to check the content of what is being received.
- The parent can set rules/criteria for websites that cannot be accessed (create a blacklist).
- The firewall checks if the traffic meets the rules/criteria.
- If it does not meet the criteria, the access to the website is denied.

The following tables contain True & False statements regarding Firewalls:

(i) Table 1:

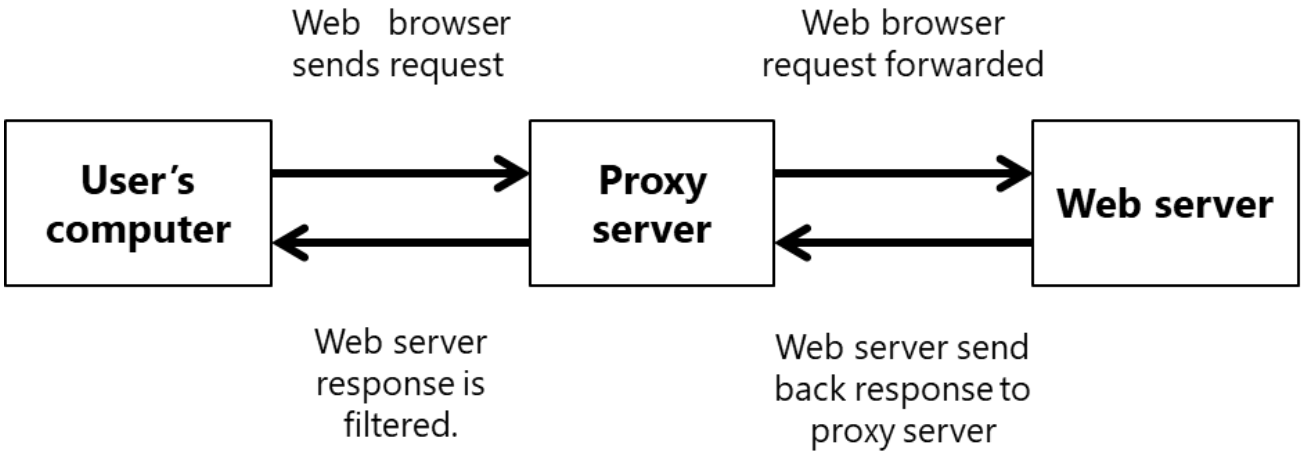
Statement	True (✓)	False (✓)
Firewalls can monitor incoming and outgoing traffic.	✓	
Firewalls operate by checking traffic against a set of rules.	✓	
Firewalls cannot block access to a certain website.		✓
Firewalls can be software and hardware.	✓	
Firewalls can act as intermediary servers.		✓
Firewalls can block unauthorized traffic.	✓	

(ii) Table 2:

Statement	True (✓)	False (✓)
Firewalls are only available as hardware devices.		✓
Firewalls allow a user to set rules for network traffic.	✓	
Firewalls will automatically stop all malicious traffic.		✓
Firewalls only examine traffic entering a network.		✓
Firewalls encrypt all data that is transmitted around a network.		✓
Firewalls can be used to block access to certain websites.	✓	

Proxy Servers:

- It is a dedicated computer or a software system running on a computer.
- It acts as an intermediate between the user and a web server:



- It sits between the user and a webserver and prevents direct access to the webserver.
- If an attack is launched, it hits the proxy server instead and so it helps prevent hacking of the webserver or denial of service attack etc.

Tasks carried out by a Proxy Server:

- It acts as a firewall.
- It monitors/filters/examines incoming and outgoing traffic.
- The rules/criteria for the traffic can be set by a user.
- It is used to direct invalid traffic away from the webserver.
- If the traffic is valid then the data from the webserver will be obtained by the user.
- It blocks any traffic that does not meet criteria and can send a warning message to the user.
- It stops the website failing in a Denial of Service (DoS) attack as the DoS attack hits the proxy server and not the webserver.
- It blocks/filters access to specified IP addresses/websites set by the user and keeps a list of these IP addresses.
- It speeds up the access to web pages/information from a web server by using a cache.
  The cache stores the website home page after it has been accessed for the first time. When the user next visits the website, it now goes through the proxy server cache instead, giving much faster access.
- It keeps the user's IP address secret which clearly improves security.

Note regarding Proxy Server:

- It does not encrypt any data that is transmitted around a network.
- It helps prevent hacking of user's computer/data.
- It does not help prevent malware, including viruses, from entering a user's computer.

Role of a Proxy Server in a security system:

- It sits between the user and a webserver and prevents direct access to the webserver.
- If an attack is launched, it hits the proxy server instead and so it helps prevent hacking of the webserver or denial of service attack etc.
- It is used to direct invalid traffic away from the webserver.
- It examines and filters the traffic.
- If the traffic is valid then the data from the webserver will be obtained by the user.
- If the traffic is invalid, then the request to obtain data is declined.
- It can block requests from certain IP addresses specified by the user.

Firewalls & Proxy Servers:

The following table compares Firewalls & Proxy Servers:

Statement	Firewall (✓)	Proxy Server (✓)
Speeds up access of information from a web server by using a cache		✓
Filters all Internet traffic coming into and out from a user's computer, intranet, or private network	✓	✓
Helps to prevent malware, including viruses, from entering a user's computer	✓	
Keeps a list of undesirable websites and IP addresses	✓	✓

Privacy Settings:

- These are the controls available on web browsers, social networks, and other websites.
- They are designed to limit who can access and see a user's personal profile.

The privacy settings can refer to:

1. A 'do not track' setting:
   It stops websites collecting and using browsing data which leads to improved security.
2. A check to see if payment methods have been saved on websites:
   It is a useful safety feature which prevents the need to type in payment details again as every time the user types the financial details, there will be a risk of data interception.
3. A safer browsing:
   An alert is given when the browser encounters a potentially dangerous website, and the undesirable website will be in a blacklist stored on the user's computer.
4. The web browser privacy options (e.g., storing browsing history, storing cookies etc.)
5. The website advertising opt-outs:
   A website may be tracked by any number of third parties who gather information about the user's browsing behavior for advertising purposes.
6. The applications (apps):
   For example, the sharing of location data in map apps can be switched off.

Secure Socket Layer (SSL) Security Protocol:

The protocol is a set of rules used by computers to communicate with each other across a network when using the Internet. This allows data to be sent and received securely over the Internet.

- It is a security protocol used for secure transmission of data between devices and users when communicating over the internet.
- It encrypts data being transmitted and uses public and private keys so only the user's computer and the web server are able to make sense of what is being transmitted.
- It provides a secure connection between web browsers and websites allowing secure transmission of private data over the internet.
- A user will know if SSL is being applied when they see access protocol 'https' or the small padlock in the status bar at the top of the screen.

The address window in the browser when https protocol is being applied, rather than just http protocol, is quite different:

using https:		**https**://www.xxxx.org/documents
using http:		**http**://www.yyyy.co.uk/documents

How SSL protocol secures the data/helps keep data safe for transmission:

- It uses symmetric, asymmetric or both type of encryption which makes use of public and private keys.
- It enables an encrypted link between the browser and the webserver based on the authentication of an SSL certificate.
- It makes the data meaningless without a decryption key even if intercepted.

Benefit of using an SSL connection:

- If the data is intercepted, it still cannot be understood as the data is encrypted.
- The data is scrambled through encryption and it requires keys to decrypt the data.

Ways that a user can identify if a website is secure OR a website uses secure data transmission by looking at the web address:

- The user can check that the URL begins with HTTPS protocol.
- The user can check that the padlock symbol is locked (green padlock).
- The user can check that the website SSL certificate is valid.

How a browser checks that a website is secure:

- The browser requests the web server to identify itself.
- The web server sends a copy of its digital SSL certificate to the browser.
- The browser checks if the SSL certificate is authentic/trustworthy.
- The browser sends a signal back to webserver that the certificate is authentic/trustworthy.
- The webserver then starts to transmit data once the connection is established as secure.

Process of SSL and how it provides a secure connection:

- The SSL is a security protocol used for secure transmission of data.
- It encrypts any data that is sent.
- It uses and sends digital certificates.
- The digital SSL certificates are requested from web server by user's browser (asking web server to identify itself).
- The web server sends the digital SSL certificate to the user's browser as requested.
- The user and server agree on encryption method to use that contains the server's public key.
- The digital certificate can be used to authenticate the web server.
- Once the certificate is authenticated by the browser, the session key is generated, and the browser sends signal to server to start transmission.
- The encrypted data transmission begins between the browser and server.

Examples of where SSL would be used:

1. Online banking & all online financial transactions
2. Online shopping/commerce
3. Sending & receiving emails
4. When making use of a social networking site
5. Voice over Internet Protocols (VoIP) when carrying out video chatting and/or audio chatting over the Internet
6. Intranet/extranet (as well as Internet)
7. Used in instant messaging/chatting
8. Using cloud storage facilities

The following stages take place when a user wants to access a secure website OR the stages a web browser goes through to detect whether a website is secure:

The web browser attempts to connect to a website which is secured by SSL.

↓

The web browser requests the web server to identify itself.

↓

The web server responds by sending the web browser a copy of its digital SSL certificate which is used to authenticate a website.

↓

The web browser checks whether the SSL certificate is authentic as it contains the public key that can be used to authenticate the web server.

↓

If the digital certificate is authentic then the web browser sends a message back to web server.

↓

The web server will then send back some form of acknowledgment to allow the SSL encrypted session to begin after secure connection is established.

↓

The encrypted data is then shared securely between the web browser and the web server.

↓

If the website is not secure, then the browser will display an open padlock or a warning message.

The following table shows potential threats to a company's web server, the different impacts each threat could have on the company & the software the company can use to help limit each threat:

Threat	Impact on Company	Software
Denial of Service	• Users cannot access the website • Loss of sales for company • Loss of reputation for company	Proxy/Firewall
Virus/Malware	• Data on the server may be deleted/ changed • Website may be deleted/changed • Server may be filled with data and crash	Anti-Virus
Hacker (unauthorized access)	• Data could be deleted/stolen/changed	Proxy/Firewall

Exam Style Questions:

Question 1:

(a) State what is meant by the term SSL.

.....

.....

.....[1]

(b) The following stages take place when a user wishes to access a secure website.

Put each stage in sequence by writing the numbers 1 to 6 in the column on the right. The first one has been done for you.

Stage	Sequence number
the encrypted data is then shared securely between the web browser and the web server	
the web browser attempts to connect to a website which is secured by SSL	**1**
the web server sends the web browser a copy of its SSL certificate	
the web browser requests the web server to identify itself	
the web server will then send back some form of acknowledgement to allow the SSL encrypted session to begin	
the web browser checks whether the SSL certificate is trustworthy; if it is, then the web browser sends a message back to the web server	

[5]

Answer:

(a) Any **one** from:

- secure sockets layer
- encrypts data being transmitted
- use of http**s**
- use public and private keys

[1]

(b) 1 mark for each number in the correct order, next to the correct stage.

Stage	Sequence number
the encrypted data is then shared securely between the web browser and the web server	**6**
the web browser attempts to connect to a web site which is secured by SSL	***(1)***
the web server sends the web browser a copy of its SSL certificate	**3**
the web browser requests the web server to identify itself	**2**
the web server will then send back some form of acknowledgement to allow the SSL encrypted session to begin	**5**
the web browser checks whether the SSL certificate is trustworthy; if it is then the web browser sends a message back to the web server	**4**

[5]

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

Question 2:

A company has a number of offices around the world.

(a) Data is transmitted between the offices over the Internet. In order to keep the data safe the company is using Secure Socket Layer (SSL) protocol and a firewall at each office.

Explain how SSL protocol and a firewall will keep the company's data safe.

SSL protocol .....

.....

.....

Firewall .....

.....

.....

[4]

(b) A company stores personal details of its customers on a computer system behind a firewall.

Explain, with reasons, what else the company should do to keep this data safe.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....[6]

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

Answer:

Question	Answer	Marks
8(a)	2 marks for SSL, 2 marks for Firewall **SSL protocol** **Two** from: • uses encryption • encryption is asymmetric / symmetric / both • makes use of (public and private) keys • data is meaningless (without decryption key / if intercepted) **Firewall** **Two** from: • helps prevent unauthorised access // helps prevent hacking • checks that data meets criteria // identifies when data does not meet criteria • acts as a filter for (incoming and outgoing) data // blocks any unacceptable data //allows acceptable data through	**4**
8(b)	**Six** from: Encrypt the data … … so it cannot be understood by those not entitled to view it Password protected / biometrics … … to help prevent unauthorised access Virus checking software … … helps prevent data corruption or deletion … identifies / removes a virus in the system … scans a system for viruses Spyware checking software … … helps prevent data being stolen/copied/logged … scans a system for spyware Drop-down input methods / selectable features … … to reduce risk of spyware / keylogging Physical method e.g. locked doors / CCTV timeout / auto log off … to help prevent unauthorised access Network / company policies // training employees … to educate users how to be vigilant Access rights … … allows users access to data that they have permission to view … prevents users from accessing data that they do not have permission to view	**6**

Question 3:

An art gallery uses secure socket layer (SSL) to provide a secure connection when selling art on its website.

Describe the process of SSL and explain how it provides a secure connection.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

..... [6]

Answer:

Question	Answer	Marks
10	**Six** from: • SSL is a (security) protocol. • It encrypts any data that is sent. • It uses/sends digital certificates … • … which are sent to the (buyer's/user's) browser // requested by the (buyer's/user's) browser • … that contains the gallery's public key • … that can be used to authenticate the gallery. • Once the certificate is authenticated, the transaction will begin.	**6**

Question 4:

RockICT is a music business that has a website to allow customers to view and buy the products it sells.

The website consists of web pages.

(d) The music company is concerned about the security of its website.

The company uses a proxy server as part of its security system.

Describe the role of a proxy server in the security system.

.....

.....

.....

.....

.....

.....

.....

.....

[4]

Answer:

Question	Answer	Marks
10(d)	Any **four** from: – Prevents direct access to the **webserver** // Sits between **user** and **webserver** – If an attack is launched it hits the proxy server instead // can be used to help prevent DDOS // help prevent hacking of **webserver** – Used to direct invalid traffic away from the webserver – Traffic is examined by the proxy server // Filters traffic – If traffic is valid the data from the webserver will be obtained by the user – If traffic is invalid the request to obtain data is declined – Can block requests from certain IP addresses	**4**

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

Question 5:

(a) Identify **three** security issues that can put a computer system at risk.

Security issue 1 .....

Security issue 2 .....

Security issue 3 .....

[3]

(b) Explain how a firewall can help to protect a computer system from security issues.

.....

.....

.....

.....

.....

.....

.....

.....[4]

Answer:

Question	Answer	Marks
4(a)	**Three** from: • Malware • Virus // No antivirus • Denial of service • Spyware // No antispyware • Phishing // opening unknown links/emails • Pharming // opening unknown links/emails (only award once for this alternative) • Hacking/cracking/unauthorised access // No/weak password // No/weak firewall • Downloading/Using unknown software • Not updating software • Physical issue e.g. computer/door left unlocked	3
4(b)	**Four** from: • It examines/monitors/filters traffic into **and** out of a computer • It allows a user to set criteria/rules for the traffic • It checks whether the traffic meets the criteria/rules • It blocks any traffic that does not meet the criteria/rules // Blocks unauthorised access • It warns a **user** of any unauthorised software/access/unauthorised outgoing traffic • It keeps a log of all traffic (that can be examined)	4

Question 6:

A firewall can be used to help keep the data secure that is stored on a computer.

(a) The given paragraph describes how the firewall operates to help keep the data secure.

Complete the paragraph using the most appropriate terms from the given list. **Not** all of the terms on the list need to be used.

- Accept
- Criteria
- Hacking
- Input
- Network
- Outgoing
- Output
- Processor
- Reject
- Software
- Store
- Storage

A firewall can be ..... or hardware based. It monitors traffic between the computer and the ..... The user sets ..... for the traffic. The firewall will ..... or ..... the traffic based on this. It can help prevent ..... and malicious software that could be a threat to the security of the data.

[6]

(b) Identify **three** other methods that could be used to keep the data secure.

Method 1 .....

Method 2 .....

Method 3 .....

[3]

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

Answer:

3(a)	One mark per each correct term in the correct order. – Software – Network – Criteria – Accept // reject – Reject // accept – Hacking	**6**
3(b)	Any **three** from: – Password – Biometrics (device) – Encryption – Physical methods (e.g. locks) – Two-factor authentication // Two-step verification – Anti-viruses	**3**

Question 7:

Explain the differences between a *text-based password* and a *biometric password*.

.....

.....

.....

.....

.....

.....

.....[4]

Answer:

9	Any **four** from, must include at least **one** difference: Text based password • (a minimum number of) characters that can be typed at a keyboard • set / can be changed by the user Biometric password • a stored physical measurement e.g. fingerprint • that is compared to a previously scanned human measurement Difference • text based passwords are easier to hack than biometric passwords • biometric passwords are unique to that person/cannot be shared	**4**

Question 8:

(e) Modern smartphones can be secured with a biometric system that is built into the phone.

(i) Identify **two** biometric systems that would be suitable for securing a smartphone.

1 .....

2 .....

[2]

(ii) Explain why modern smartphones are secured with a biometric system.

.....

.....

.....

..... [2]

Answer:

1(e)(i)	Any **two** from: – Fingerprint scanner – Voice recognition – Retina/iris recognition – Facial recognition	**2**
1(e)(ii)	Any **two** from: – Adds extra level of security – Biometric device requires properties unique to individual – Allows quicker access as no need to input password // don't need to remember password	**2**

Question 9:

David has installed anti-virus software on his computer.

(a) State **three** tasks carried out by anti-virus software.

Task 1 .....

.....

Task 2 .....

.....

Task 3 .....

.....

[3]

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

(b) David is still concerned that his computer might get infected by a computer virus.

State **three** other ways in which David can reduce the risk of his computer getting a computer virus.

1 .....

.....

2 .....

.....

3 .....

.....

[3]

Answer:

Question	Answer	Marks
2(a)	Any **three** from: Scans files for viruses // detects/identifies a virus Can constantly run in background Can run a scheduled scan Can automatically updating virus definitions Can quarantine a virus Can delete a virus Completes heuristic checking Notifies user of a possible virus	3
2(b)	Any **three** from: Use a firewall Use of a proxy server Do not use / download software / files from unknown sources Do not share external storage devices / USB pens Do not open / take care when opening attachments / link Do not connect computer to network / use as stand-alone computer Limiting access to the computer	3

0335-1400368 @gilanihaseeb Syed Haseeb Bari Gilani CS/IT - O/A Level

Applications of Cyber Security Threats & Their Solutions:

NOTE: This topic is no longer a part of the Computer Science (2210) syllabus for the session 2023–2025.

However, it is provided here for completeness and additional knowledge.

Online banking and shopping are all at risk from many of the security issues described earlier on.

We will now consider some of the ways banks protect their customers from online fraud. The following notes are in addition to safeguards such as encryption, SSL, virus scanners and many of the other ways described in the earlier part of this chapter and refer to additional features you might see as part of a bank's security system.

When a customer logs on to a banking website and carries out a transaction, encryption is used to protect the customer's personal details.

However, banks carry out a number of other procedures to give additional protection. The following notes give some idea of the type of safeguards that might be encountered when a customer logs on to a bank's website:

1. Many banks use a 10 or 12 digit code which is unique to the customer.
2. You may then be asked to input three random numbers from a four-digit PIN and/or three characters from a 10-character password (this will vary from bank to bank, of course).
3. Some systems use a hand-held device into which a customer inserts their card and then enters pin. The device generates an 8-digit code to be typed in on the web page of bank. The code is valid for a few minutes, and it helps defeat hackers and spyware.
4. Some banking systems ask the customer to key in parts of their password using drop-down boxes. This is an attempt to defeat spyware/key-logging software as the use of a keyboard is eliminated.
5. Once all these stages have been passed, some systems then ask for personal data, such as:

    - 'You last logged into the system on 15th September 2015. Is that correct?'
    - 'Your mobile phone number is: 9777 111 2222. Is that correct?'
    - 'What is your mother's maiden name?'

Exam Style Questions:

NOTE: The following are a few past paper questions that have been asked over the recent years from the section 'Application of the Security Methods'.

Thoroughly reading these questions and their answers will provide you with a clear vision of how the knowledge mentioned in the whole chapter is applied to real-life scenarios.

Though the requirement of the questions below are around mentioning, describing, or explaining 1, 2, 3 or maximum 4 security methods only (as can be seen from the number of marks) but all possible answers to these questions have been stated below to enhance and improve your knowledge along with demonstrating the type of questions to expect in exam.

Question 1:

An online bank requires a client to supply an 8-digit code each time they wish to access their account on the bank's website.

Rather than ask the client to use a keyboard, they are requested to use an on-screen keypad (shown on the right) to input the 8-digit code.

The position of the digits on the keypad can change each time the website is visited.

The client uses a mouse or touch screen to select each of the 8 digits.

2	5	1
6	8	3
9	0	4
	7	

(i) Explain why the bank has chosen to use this method of entering the 8 digits. [2]

- The bank has chosen this method to defeat the spyware/key logging software as it can only pick up key presses.
- There will be no key presses to log, if either a mouse or a touchscreen as above is used.
- Moreover, the numbers on the keypad are in random format, which makes them more difficult to interpret.

(ii) Name and describe another measure that the bank could introduce to improve the security of the website. [2]

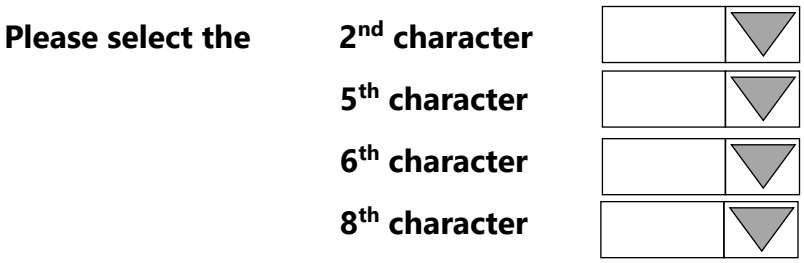
1. The bank could use a chip and PIN reader. Only the user and the bank will know which codes can be generated.
2. The bank could request a username from the person. It will ensure additional security together with password/PIN.
3. The bank could use anti-virus. It will scan and remove a potential virus threat so that it cannot be passed on to customers.

4. The bank could use firewall. It will help protect bank computers from virus threats and hacking by filtering/blocking harmful traffic.
5. The bank could use encryption. It will protect customer's data by making any hacked information meaningless/unreadable.
6. The bank could use a security protocol such as SSL. It will govern the secure transmission of data over the internet.
7. The bank could use biometric. It will involve recognizing the user through the use of e.g., facial/retina/fingerprint. This biological data is highly unique and difficult to replicate.
8. The bank could alert or warn the customers. The users IP/MAC address will be registered and the user will be alerted through, e.g. SMS if his/her account is accessed through an unregistered address.

Question 2:

A bank offers an online service to its customers. The bank has developed a "*SafeToUse*" system that asks each customer to enter four randomly chosen characters from their password each time they log in.

The customer selects these four characters from drop-down boxes. For example:



(i) Explain why it is more secure to use drop-down boxes rather than entering characters using a keyboard. [2]

- Drop-down boxes are used to protect against key logging software/spyware as it can stop key presses being recorded and then relayed.
- Moreover, drop-down boxes can be placed in different location on the screen each time to overcome the screen capture issue.

(ii) Give a reason why the system asks for four characters chosen at random. [1]

- The hacker never finds all characters on the first attempt to hack.
- It makes it more difficult for hackers to find the order of the characters.
- The hacker needs to hack the system several times to gain the whole password.
- Shoulder surfing will not give another person the full password.

Question 3:

The Henslow Diner stores personal data on a computer. This computer is connected to the Internet to allow the data to be backed up.

There is currently one security method in place to protect the data on the computer from unauthorized access. This is a password.

Give two other security methods that could be added to improve the security of the data.

Describe how each method will keep the data safe. [4]

1. Encryption:
   If the data is accessed or stolen, it will be meaningless.
2. Biometric device:
   It can help prevent unauthorized access to the system since biometric device takes input of biological data which is unique and difficult to replicate/fake.
3. Firewall:
   It can alert to show unauthorized access attempt on the system and therefore help protect against viruses and malware entering the system. It can also help prevent unauthorized traffic and access to the system.
4. Anti-spyware:
   It can stop the keys being logged that, when analyzed, would reveal the password used to store the data.

Question 4:

A company stores personal details of its customers on a computer system behind a firewall.

Explain, with reasons, what else the company should do to keep this data safe. [6]

1. The company should encrypt the data so it cannot be understood by those not entitled to view it.
2. The company should use password or biometrics which are unique and help prevent unauthorized access to the system.
3. The company should use virus checking software which helps prevent data corruption or deletion. It will scan the system for viruses and then accordingly remove them.
4. The company should use spyware checking software which helps prevent the keys being logged that, when analyzed, would reveal the password used to store the data. It will scan the system for spyware and accordingly remove it.
5. The company should use drop-down input methods to reduce risk of spyware (keylogging).
6. The company should use physical security methods such as locked doors, CCTV camera, security guards or auto log off to help prevent any unauthorized access and theft of the data.
7. The company should train employees and educate them on how to be vigilant.
8. The company should use access rights, so it only allows those users access to data that have permission to view and therefore prevents those from accessing data without permission.

Question 5:

Online banking is increasing in popularity.

Online banking can be a risk as it can raise a number of security issues. SSL can be used as a security method to make online banking safer.

Identify and describe three other security methods that could be used to make online banking safer. [6]

1. It can be made safer by using strong password which makes it difficult to hack an account.
2. It can be made safer by using biometric devices which take input of biological data which is unique and difficult to replicate/fake.
3. It can be made safer by using encryption as it will make data meaningless if intercepted.
4. It can be made safer by using anti-spyware software which will find and remove any spyware thereby stop key loggers recording any key presses.
5. It can be made safer by using firewalls as it will prevent unauthorized access to an account and block/filter any requests that do not meet the criteria/rules.
6. It can be made safer by using two-step verification as it will add another level of identification of the user.
7. It can be made safer by using drop-down boxes which will prevent key loggers from recording the key presses.
8. It can be made safer by using proxy servers as they will divert an attack away from the main system.

Question 6:

A law company holds a lot of sensitive data about its clients.

It currently requires employees to enter a username and a password to log-in to an account. Each password must be 8 letters.

The company wants to increase the security of the log-in system.

Identify two improvements the company could use to make the log-in system more secure.

Explain how each improvement increases security. [4]

- The company should make the password require more characters than 8 so it will be difficult for the hacker to crack or guess the password due to multiple possible combinations of password.
- The company should use a biometric device as it takes input of biological data which is unique and difficult to replicate/fake.
- The company should use a two-step verification method which adds an additional level in the process of hacking.
- The company should use drop-down boxes to prevent passwords being obtained using key logger.

- The company should request random characters from the user so that it won't reveal the entire password.
- The company should set up a number of password attempts so that the account will lock itself if someone takes more than the limited attempts in guessing the password. This will also stop brute-force attacks.

Question 7:

A music company wants to send a new music file to many radio stations. It will send the music file the day before the release date so that the radio stations can store the file ready for release.

The music company does not want the radio stations to be able to open the music file until 09:00 on the release date.

Identify two security measures and describe how each measure can be used to make sure the music file cannot be opened until the release date. [4]

- The file should be protected by a password. This password should be released on the release date of the music file.
- The file should be protected by encryption, so the data is meaningless. The encryption key should be released on the release date of the music file.

Question 8:

Companies can use a range of security methods to keep their data secure.

Identify two security methods that a company can use to keep their data secure and explain how each method can keep the data secure. [6]

1. The company can use firewalls which will monitor the traffic and then block any traffic that doesn't meet the criteria/rules.
2. The company can use strong passwords which are difficult to crack/guess and so prevent unauthorized access.
3. The company can use biometric devices as it takes input of biological data which is unique and difficult to replicate/fake.
4. The company can use encryption so that the data will be meaningless if intercepted. A key will be required to decrypt the data.
5. The company can use physical security methods such as locked doors, CCTV camera, security guards or auto log off to help prevent any unauthorized access and theft of the data.
6. The company can use anti-spyware software which will scan and remove any spyware from the system thereby preventing data being relayed to a third party.