1. State **two** issues with only using usernames and passwords in an authentication system.

(Total 2 marks)

2. Describe **one** security measure that could be used, in addition to a password, to make sure that a user is who they are claiming to be.

(Total 2 marks)

3. State **two** reasons why automatic software updates provide better security than manual software updates.

(Total 2 marks)

4. Explain what penetration testing is.

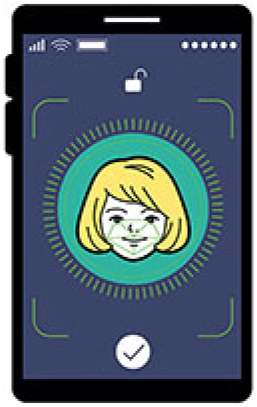
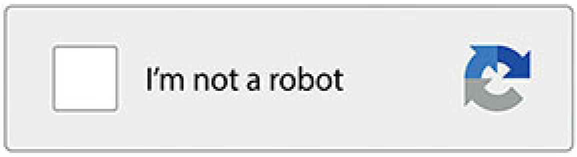
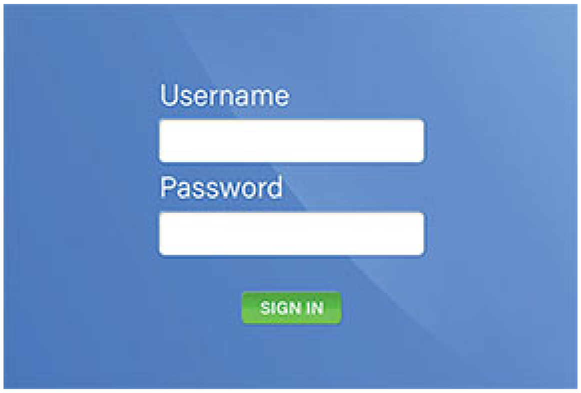
(Total 2 marks)

5. Describe the aim of a white-box penetration test.

(Total 2 marks)

6. The table below shows screenshots of three different security measures.

Tick the box next to the CAPTCHA screenshot.

Security measure	Tick one box
	
	
	

(Total 1 mark)

7. Give **three** examples of when it would be suitable to use a CAPTCHA system.

(Total 3 marks)

8. Shade the **two** lozenges that are examples of social engineering.

A	Blagging	○
B	Blogging	○
C	Faking	○
D	Phishing	○
E	Porting	○
F	Smashing	○

(Total 2 marks)

9. Define the term 'cyber security'.

(Total 2 marks)

10. Define the term 'malware'.

(Total 2 marks)

11. Explain how **each** of the following cyber security threats could be used by a student to gain unauthorised access to a school network:

- weak and default passwords
- misconfigured access rights
- removable media
- unpatched and/or outdated software.

In your answer you should also describe some possible consequences of these threats.

(Total 8 marks)

12. Shade **one** lozenge to show which statement best describes the definition of the term 'social engineering'.

A	The art of hacking a network to access confidential information.	○
B	The art of hacking a network to access public information.	○
C	The art of manipulating people so they give up confidential information.	○
D	The art of manipulating people so they give up public information.	○

(Total 1 mark)

13. Phishing is a form of social engineering.

Describe **two** methods a school could use to protect its staff and students from phishing.

(Total 4 marks)

14. A company has decided to move its business online but it is concerned about making sure that only authorised users can gain access to the system. The company has set up a CAPTCHA system to check that the user is not a robot.

Explain **three** different electronic methods that could then be used to confirm user identity.

(Total 6 marks)

15. Penetration testing can be conducted as either black-box or white-box testing.

Explain the difference between these two types of penetration testing.

(Total 4 marks)

16. A virus is a specific category of malware.

Describe **three** other different categories of malware.

(Total 6 marks)

17. Most schools have a computer network.

Some schools allow teachers to access the school network from their home computers.

Give **one** reason why some schools allow this and **one** reason why some schools do not allow this.

(Total 2 marks)

18. Social engineering is where someone is tricked or manipulated into providing secure information or access to a secure system. Describe each of the following social engineering techniques.

(Total 3 marks)

19. A games café is evaluating the security for their network.

(a) State **two** reasons why using a biometric authentication measure is better than password authentication for staff accounts.

(2)

(b) Explain why it would not be appropriate for the café to use MAC address filtering on their wireless network.

(2)

(Total 4 marks)

20. Social engineering is where someone is tricked or manipulated into providing secure information or access to a secure system. Describe each of the following social engineering techniques.

Blagging

Phishing

Shouldering (or shoulder surfing)

(Total 3 marks)

21. AQATravel is a tour operator that sells holidays to places all around the world. They hold all of their customer and business data electronically. Following recent news articles about the effects of malware attacks on businesses, the management of AQATravel have been investigating how they could protect themselves against malware attacks.

Discuss four methods that AQATravel could use to prevent infections from malware and/or to minimise the damage that could be caused by malware.

(Total 12 marks)

22. The algorithm below, expressed in pseudo-code, allows three users to log in to a computer program with individual usernames and passwords.

- For this algorithm, array indexing starts at 0.
- Line numbers are included, but are not part of the algorithm.

```
01   userlist ← [ 'Rachel', 'Sam', 'Tracey' ]
02   passlist ← [ '49Class', 'Smile', 'b1K3' ]
03    REPEAT
04      OUTPUT 'Enter Username'
05      username ← USERINPUT
06      OUTPUT 'Enter Password'
07      password ← USERINPUT
08      validlogin ← False
09      FOR usernum ← 0 TO 2
10         IF username = userlist[usernum]
11         AND password = passlist[usernum] THEN
12            validlogin ← True
13         ENDIF
14      ENDFOR
15   UNTIL validlogin = True
16   OUTPUT 'Login Successful'
```

The valid usernames and passwords are listed below.

Username	Password
Rachel	49Class
Sam	Smile
Tracey	b1K3

(a) Shade in **one** lozenge in each row of the table below to indicate the most appropriate data type to use for each listed **Variable** from the algorithm, when the algorithm is implemented in a programming language.

	Most appropriate data type (shade one lozenge per row)				
Variable	**Integer**	**Real**	**Boolean**	**Character**	**String**
`password`	○	○	○	○	○
`validlogin`	○	○	○	○	○
`usernum`	○	○	○	○	○

(3)

(b) It is suggested that line `09` of the algorithm is replaced with the following line:

```
FOR usernum ← 0 TO LEN(userlist)
```

The function `LEN` returns the number of items that are stored in the array that is passed to it as a parameter.

Explain why using the `LEN` function would make the algorithm more flexible and why the suggested replacement line would not work as it is.

(3)

(c) It is suggested that lines `08` to `14` of the algorithm are replaced with the following lines:

```
FOR usernum ← 0 TO 2
   IF username = userlist[usernum]
   AND password = passlist[usernum] THEN
      validlogin ← True
   ELSE
      validlogin ← False
   ENDIF
ENDFOR
```

Explain why making this replacement would mean that the algorithm no longer worked.

(3)

(d) State which of the three passwords listed in the table above is the least secure and explain why this is the case.

(2)

(Total 11 marks)

23. List **three** different measures that can be used to maintain the security of a computer system.

For each measure:

- Outline what the measure is.
- Explain what types of threat to cyber security it is effective against.

(Total 9 marks)

24. Explain each of the cyber security threats listed below.

(a) Social engineering.

(2)

(b) Outdated software.

(2)

(c) Misconfigured access rights.

(2)

(Total 6 marks)

25. Most schools have a computer network.

Some schools allow teachers to access the school network from their home computers.

Give **one** reason why some schools allow this and **one** reason why some schools do not allow this.

(Total 2 marks)

26. Organisations often spend a lot of money on cyber security.

Penetration testing is an attack on its own computer system by an organisation to try and identify security weaknesses.

Describe **one** difference between black-box and white-box penetration testing.

(Total 1 mark)

27. Social engineering is often used to try to gain unauthorised access to a computer system. Phishing is a commonly used social engineering technique where emails are sent that pretend to be from a reputable organisation / company to try and obtain personal details.

Describe another **two** social engineering techniques. You should also explain measures that an organisation can take to try to reduce the security risks from phishing and the two other social engineering techniques you have described.

(Total 6 marks)

28. In recent years, there has been a large growth in the use of cloud storage.

Discuss the advantages and disadvantages of using cloud storage.

In your answer you should include an explanation of the reasons for the large growth in recent years and consider any legal, ethical and environmental issues related to the use of cloud storage.

(Total 9 marks)

29.

Barnes Pest Control is a small business with four employees. Each of their employees has a standalone desktop computer. They have decided to use a network instead of standalone machines.

Two security measures that Barnes Pest Control could use are authentication and encryption. Explain each of these security measures and how Barnes Pest Control could use them.

(Total 4 marks)

30.

Computer viruses, Trojans, adware and spyware are different types of malware.

Describe the similarities and differences between these different types of malware. Your answer should also describe measures that can be taken to reduce the risks from these malware.

(Total 9 marks)

31.

The pseudocode below is written to make sure that the user enters a value within a given range.

```
inp ← USERINPUT
WHILE inp ≤ 0 OR inp ≥ 10
  OUTPUT "not in range"
  inp ← USERINPUT
ENDWHILE
```

(a) (i) Tick the set of test data that is the **most** appropriate to check that the code works as expected.

Test data	Tick **one** box
-1, 0, 9, 10	
0, 1, 10, 11	
-1, 0, 10, 11	
0, 1, 9, 10	

(1)

(ii) Why is the set of test data that you have chosen in part (i) likely to be enough to show that the code above works as expected?

(1)

(b) Develop an algorithm using pseudocode or a flowchart that asks the user to create a new password.

The algorithm should:

- get the user to enter a password
- get the user to re-enter the password
- repeat the two bullet points above until both entered passwords are identical
- output "`password created`" when they are identical.

(5)

(c) State **two** possible weaknesses of the passwords that this algorithm would accept.

(2)

(Total 9 marks)

Mark schemes

1.

2 marks for AO1 (understanding)

Maximum of **two** marks from:

- (weak) passwords are easily cracked // a program could be used to try out lots of passwords // users might choose passwords which are not strong enough // (weak) passwords can be easily guessed;
- usernames/passwords may have appeared in data leak;
- (if users write down/store their passwords) these can be stolen;
- susceptible to shouldering;
- it is difficult to verify the actual identity of the person logging in (eg compared to fingerprint/Touch/facial recognition/Face ID, multi-factor authentication);

[2]

2.

2 marks for AO1 (understanding)

1 mark for the method and **1 mark** for a valid expansion.

- A code can be sent to your phone as a (text) message/in an email/as a pop-up to one of your devices;
  the user then types in the code (as well as the password);
  any hacker would need to access the phone as well as the password;
- An authenticator app on a mobile phone;
  this generates a code which the user uses to complete the log-in;
- Use two-factor authentication/2FA // strong customer/multi-factor authentication;
  this asks for a second form of identification such as something you know/ possess/are;
- Biometrics;
  (to be authenticated) reference data is compared to the individual's (unique) biometric data;
- Smart cards/fobs;
  the user inserts a Smart Card to a reader and enters the PIN, the authentication request is then verified (using digital certificates);
- Ask security / memorable question;
  the user is asked a question that only they know the answer to;

[2]

3.

2 marks for AO1 (understanding)

Maximum of **two** marks from:

- A user may forget to do updates manually;
- Automatic updates mean that a computer is protected more quickly;
- Automatic updates from a trusted / known (secure) source will be safe // manual updates may be from an infected source;

[2]

4.

2 marks for AO1 (recall)

Maximum **one** marks from:

- the process of attempting to gain access to resources/a computer system;
- the practice of testing a computer system/network/web application // to test the effectiveness of security measures;

Maximum of **one** from:

- without knowledge of usernames/passwords/other normal means of access;
- to find vulnerabilities/weaknesses (that an attacker could exploit);

[2]

5.

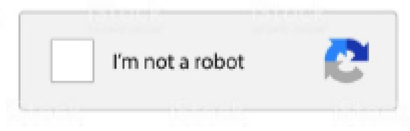
2 marks for AO1 (recall)

to simulate (an attack from) a (malicious) insider; who has knowledge of / basic credentials for the target system;

[2]

6.

Mark is for AO1 (understanding)



;

R. If more than one box ticked.

[1]

7.

3 marks for AO1 (understanding)

1 mark for each of the following points (maximum of **three** marks):

- account registration;
- account access;
- online voting systems;
- ticket purchasing / transaction completion;
- on pages where comments / reviews can be posted;
- on parts of the website where fraudulent click-throughs may be possible;

[3]

8.

2 marks for AO1 (recall)

A Blagging;
D Phishing;

R. If more than two lozenges are shaded.

[2]

9. **2 marks for AO1 (recall)**

- (the processes/practices/technologies/methods designed to) protect networks/computers/programs/data;
- from attack/damage/threats/unauthorised access;

[2]

10. **2 marks for AO1 (recall)**

- (Malware is a blanket/umbrella term for) computer software/program/code;
- with malicious/hostile/intrusive intent;

[2]

11. **8 marks for AO2 (apply)**

Level	Description	Marks
4	Responses at this level will contain a **thorough explanation** of how **all** of the threats could be exploited by a student. The response makes clear reference to a school network. The response is well structured and coherent. **More than one** consequence has been described.	7-8
3	Responses at this level will contain a **detailed explanation** of how **most** of the threats could be exploited by a student. The response makes clear reference to a school network. The response is well structured and coherent. **At least one** consequence has been described.	5-6
2	Responses at the upper end of the level will contain some **explanations** of how **most** of the threats could be exploited by a student. The response makes some reference to a school network. The response makes sense when read as a whole. Responses at the lower end of the level will mostly contain **descriptions** of how **some** of the threats could be exploited by a student. The response might make some reference to a school network. The response makes some sense when read as a whole. In this level students may not have referred to the consequences.	3-4
1	Responses at the upper end of the level will contain **descriptions** of **at least one** of the threats and/or consequences. Responses at the lower end of the level will include a few **statements** related to one or more of the required threats/consequences.	1-2
No creditworthy material		0

Indicative Content

The indicative content below is written in a generic manner for the benefit of examiners. Responses should be worded in the context of a school to gain the highest marks. For example reference to pupils using default passwords or them gaining access to staff-only areas through misconfigured access rights.

- Weak and default passwords:
  - ○ students could use brute force methods to crack passwords
  - ○ weak admin passwords would allow students to gain admin level access
  - ○ default passwords allow students to gain access without any effort
  - ○ default passwords are published online so everyone knows them.
- Misconfigured access rights:
  - ○ allows students to access areas they are not supposed to
  - ○ network admins might not know that secure areas had been breached as no-one has ‘broken in’
  - ○ students could reconfigure network
  - ○ students could create new user accounts to give themselves admin access.
- Removable media:
  - ○ could contain malware that allows students to gain access to network
  - ○ could be used to steal data
  - ○ could be used to allow students to take control of certain network processes (eg remote access systems).
- Unpatched and/or outdated software:
  - ○ could allow students to exploit known weakness/flaw
  - ○ known weaknesses/flaws are published online
  - ○ once in a student could install malware.

[8]

12.

1 mark for AO1 (recall)

C The art of manipulating people so they give up confidential information.

R. if more than one lozenge shaded.

[1]

13. **4 marks for AO2 (apply)**

A **maximum of 4 marks** can be awarded.

One mark for each point and **one mark** for an expansion.

Answers that are too similar to each other must only be credited once.

Example responses include:

- Train staff/students to be cautious of emails;
  - ○ that come from unrecognised senders;
  - ○ that ask you to confirm personal/financial information (over the Internet);
  - ○ that make urgent requests for personal/financial information;
  - ○ that are not personalised;
  - ○ that try to upset you into acting quickly by threatening you with frightening information;
- Train staff/students not to click on links/download files/open attachments (in emails); from unknown senders/sources;
- Prevent students from being able to download; anything from the internet/email links;
- Train staff/students to never enter personal information; in a pop-up screen;
- Train staff/students not to copy web addresses (into a browser); from pop-ups;
- Protect the school computers with a firewall/spam filters/anti-virus/anti-spyware software; and keep the software updated;

[4]

14. **3 marks for AO1 (understanding) and 3 marks for AO2 (apply)**

2 marks per method, 1 mark for stating the method, 1 mark for an explanation.

- Passwords; a set of characters that is only known by the person who is being authenticated//a set of characters that is entered and compared against a database / recorded version;
- Biometric; measures such as fingerprint, facial, iris, voice-print that use the user's physical features to prove who they are;
- Email confirmation; sends an email which requires a valid email address and for the recipient to respond to prove the email and hence user is valid;

A. Other methods that are not in the specification that are appropriate should also be awarded marks. Examples such as 2 Factor Authentication (2FA), Authenticator Apps, security questions.

[6]

15. **4 marks for AO1 (understanding)**

Maximum of 3 marks if only 1 type of testing.

Black box testing:

- the tester does not know how the system operates;
- the tester is acting as an external hacker;
- requires a lot of investigation and guessing / brute-force to find issues;
- may not test all of the system especially if you do not know it's full functionality;
- you are trying to discover and exploit the weak spots in the system;

White box testing:

- the operation of the system is known;
- the tester is simulating a malicious insider;
- can be targeted to test specific vulnerabilities;
- you know exactly what you are trying to test;
- because you know what you are testing you should be able to test all possible scenarios;

R. Any direct opposites. Statements such as “Black box has no knowledge of how the system operates. White box has knowledge of how the system operates.” would be awarded only one mark.

[4]

16.

3 marks for AO1 (recall), 3 marks for AO1 (understanding)

1 mark each for stating, 1 mark each for describing.

- Trojan (horse); a program which misleads the user into thinking it is another piece of software which, when run, executes another program;
- Spyware; a program which records data such as usernames and passwords on a host system and forwards the information to a third party;
- Adware; code embedded or attached to program files which will persistently show adverts (that attempt to generate revenue);
- Worm; code which will run autonomously and replicates itself on a host system;
- Ransomware; a program that encrypts user’s data to make it unreadable until they pay for the key;
- Remote Access Tool (RAT); allows access to control and monitor a computer from a remote network location;
- Rootkit; malware that has managed to gain ‘root’ admin privileges;
- Bots / Zombies; a program installed on a computer that performs a job for the remote owner of the bot / zombie such as sending spam or sending web requests to perform a DOS or attacking a computer system;
- Scareware; malware that tells you something is wrong with your system in an attempt to get you to make a purchase;
- Keylogger; a program that monitors / records a user’s keystrokes in order to steal passwords / confidential details;

R. Specific named examples on their own, e.g. “Wannacry” would receive no marks, “Ransomware such as Wannacry” would receive 1 mark.

R. References to ‘virus’ as this is the example in the question.

[6]

17.

All marks AO1 (understanding)

Reasons for allowing:
Teachers can access resources on the school network to allow them to plan lessons at home;
Teachers can teach lessons from home (using videoconferencing) if they are not able to get into work (eg travel difficulties);
Teachers can access electronic copies of student work so that they do not have to carry marking home;

Reasons for not allowing:
Data protection issues – schools may not want potentially sensitive student information to be accessed outside of school;
To try to help teachers have a work-life balance;
Increased security risks as teachers may not have fully-protected computers at home (eg if a teacher does not have anti-virus software on their home computer this may cause problems when they connect their computer to the school network);

Max 1 mark: if only described reasons for allowing access

Max 1 mark: if only described reasons for not allowing access

[2]

18. **3 marks for AO1 (understanding)**

1 mark each for describing the social engineering technique.

Blagging
This is where a victim is tricked/persuaded by a fraudster to give their details or payment information for a false reason/purpose;

Phishing
Is where the victim receives and responds to a communication that appears to be from a valid or known source but is in fact fraudulent. (It allows the fraudster to capture private information before the victim realises);

Shouldering
This is where someone watches and records\remembers a victim entering their pin or security information such as passwords. (They can then use this information to gain access to a system);

[3]

19. (a) **All marks AO2 (apply)**

Staff could forget their password // staff can't forget biometric measure;
Shouldering risk when staff entering their password // no risk of shouldering when using biometric data;
Lower risk of hacking;

Max 2

2

(b) **All marks AO2 (apply)**

Network is made available to members of the public;
Won't know the MAC addresses for (most) of the devices connecting to the network;

2

[4]

20.

3 marks for AO1 (understanding)

1 mark each for describing the social engineering technique.

Blagging (pretexting)
This is where a victim is tricked / persuaded (by a fraudster) to give their details or payment information (for a fraudulent reason / purpose);

Phishing
Is where the victim receives and responds to a communication that appears to be from a valid or known source (but is in fact fraudulent. It allows the fraudster to capture private information before the victim realises);

Shouldering (or shoulder surfing)
This is where someone watches and records / remembers a victim entering their pin or security information such as passwords. (They can then use this information to gain access to a system);

[3]

21.

4 marks for AO1 (understanding) and 8 marks for AO2 (apply)

Level	Description	Mark Range
4	**Level 4 High mark range** **Subject Criterion Context** A **clear understanding** shown through the use of at least **four** relevant examples that **discuss** the methods a company or individual could use to protect their devices from malware and/or minimise the damage caused by infection. Examples are well supported by reasoned arguments and the detail given should explain how and why the methods\techniques would be in/effective.	10-12
3	**Level 3 Higher mid mark range** **Subject Criterion Context** A **more developed understanding** shown through the use of suitable examples that **discuss / explain** at **least three** methods a company or individual could use to protect their devices from malware and / or minimise the damage caused by infection. Examples are supported by explanations of how the methods \ techniques would be in/effective.	7-9
2	**Level 2 Lower mid mark range** **Subject Criterion Context** **Some understanding** shown through the use of suitable examples that **describe** at **least two** methods a company or individual could use to protect their devices from malware and/or minimise the damage caused by infection. Examples are supported by limited descriptions and at least one explanation of how the method \ technique would be in/effective.	4-6
1	**Level 1 Lower mark range** **Subject Criterion Context** At the higher end of the mark range there is a simple **description** about at **least one** method \ technique that could be used by a company or individual to protect their devices from malware and / or minimise the damage caused by infection. The answer may not include an explanation of how the method(s) would work. Simple **statements / example(s)** of methods / techniques (for example a bulleted list) supported by no comments is limited to the middle of this range.	1-3
No creditworthy material		0

Method **AO1 (Understanding)**	**Explanation** **AO2 (apply)**
Regularly back up data and test backups.	Back up data so that you can restore data that has been accidentally deleted or destroyed. It is important to test that back-ups work on a regular basis.
Secure the backups.	Make sure that backups are off site so they are not lost under the same circumstances as the main data. Also if the backups are air-gapped then this will prevent a severe malware infection getting access to the backups as there is no physical connection.
Block or remove email attachments or links.	Check links contained in e-mails and do not open attachments included in unexpected e-mails.
Disable pop-ups.	Ensure the pop-up blocker is turned on and any website screening options are also on.
Control software downloads.	Only download software, especially free software, from sites you know and trust. Or prevent software downloads completely.
Ensure software is up to date.	Make sure all software is up to date and patched to prevent any exploitation of known vulnerabilities.
Anti-virus is up to date.	Ensure anti-virus automatically updates so that the latest vulnerabilities are detected and dealt with.
Disable macro scripts.	Prevent macros from running which could cause or run malicious code.
Only allow specified programs to run.	Preventing any unknown programs running should prevent any malicious code before it gets a chance to run.
Manage the use of privileged accounts and access levels to files.	Controlling the access to files should act as an internal firewall \ barrier to prevent unauthorised access or execution of programs.
Use virtualized environments \ sandboxes.	Operations are carried out in a controlled and temporary working space\environment which can be easily reset without effecting anything outside of the space\environment.
Use network filtering or a firewall.	Prevent \ block access into and out of the network using filtering and firewall to stop any malicious communications or transfer of viruses.
Remove the ability to use removable media.	Prevent unknown or unauthorised files to enter or leave the network.
MAC address filtering.	Can prevent access by unauthorised devices.
User training.	To educate staff in dangers of social engineering techniques and other unsafe practices.
Pen testing.	To allow organisation to understand where weaknesses may be, in order to strengthen their system security.

R. Encryption, unless it is discussed in terms of minimising damage

[12]

22. (a) **3 marks for AO1 (knowledge and understanding)**

1 mark per correctly identified data type:

- `password` : String
- `validlogin` : Boolean
- `usernum` : Integer

On any row, do not award a mark if more than one lozenge is shaded.

3

(b) **3 marks for AO2 (apply)**

Max 2 marks for why using `LEN` makes the algorithm more flexible:

- If the number of items in the array // number of users/passwords changes;
- then line `09` // the `FOR` loop will not need to be changed;

Max 2 marks for why the stated line will not work:

- The loop would count up to 3 // the loop will go past the end of the array;
- because array indexing starts at 0 it should only count up to 2;

Award 2 marks for why the line will not work if the response includes the corrected line of pseudo-code:

```
FOR usernum ← 0 TO LEN(userlist)-1
```

3

(c) **3 marks for AO2 (apply)**

`validlogin` get set after each comparison;

if the user details/username/password match the first or second user then `validlogin` will be reset to `False` later on;

`validlogin` will only reflect whether or not the user details/username/password matches the last value(s) in the arrays;

3

(d) **1 mark for AO1 (knowledge and understanding)**
1 mark for AO2 (apply)

Least Secure Password: Smile;
Reason: It is a word (in the dictionary) // it only contains alphabetic characters // it does not contain any numbers/symbols;

2

[11]

23.

9 marks for AO1 (knowledge and understanding)

Award up to **three marks for each measure**. Of these:

- Award up to two marks for an outline (one per point)
- Award one mark for an example of a threat that it would be effective against.

The table below lists common examples but is not exhaustive; alternative valid responses should also be credited.

Virus Checker	**Outline:** Scans files to look for malicious code Needs to be updated regularly with latest virus definitions Can quarantine / delete malware/suspicious files **Effective against:** Malware (accept examples)
Firewall	**Outline:** Analyses/scans network traffic Can block traffic from suspicious hosts/ computers/addresses/ports **Effective against:** Hackers Transmission of malware
Login system / Authentication / Password / Biometric	**Outline:** User has to enter username and password Can be authenticated by other methods such as biometric (accept examples) Login details matched to a database of users **Effective against:** Hackers Unauthorised access
MAC address filtering	**Outline:** Each hardware device has unique hardware address A database of allowed hardware/MAC addresses is kept/whitelist To connect to a network a device must have an address on the database/whitelist **Effective against:** Unauthorised devices
Encryption	**Outline:** Data is stored/transmitted as ciphertext (**A.** in coded form) Only people who know the encryption method/key can decrypt/read the data **Effective against:** Data theft
Prevention of use external storage devices / USB ports	**Outline:** Ports on a computer are disabled Storage devices connected to them cannot be accessed // flash drives cannot be used **Effective against:** Putting malware onto a computer Theft of data
Access rights	**Outline:** Users are associated with certain privileges These might control files that can be accessed/run // level of internet access // ability to create/delete files // ability to change settings **Effective against:**

	Hackers Theft of data Authorised users doing unauthorised things
CAPTCHA	**Outline:** Users have to type in some distorted text // recognise images for a set of images Humans can do this but it is a difficult task for computer programs / bots **Effective against:** Automated hacking programs Bots
Automatic software updates	**Outline:** Operating system / software configured to download updates from the internet Hackers look for security vulnerabilities in software Updates can patch security vulnerabilities **Effective against:** Hackers Malware

[9]

24. (a) **2 marks for AO1 (knowledge and understanding)**

1 mark for defining social engineering: Manipulating / fooling people into revealing confidential information / login details / bank details (etc)

1 mark for naming or describing an example: blagging, phishing, pharming, shouldering

2

(b) **2 marks for AO1 (knowledge and understanding)**

1 mark for explaining what outdated software is: Software that has not has patches applied to it // been upgraded

1 mark for explaining why it is important that software is updated: Hackers discover weaknesses/flaws in software and try to exploit these

2

(c) **2 marks for AO1 (knowledge and understanding)**

1 mark for explaining what access rights are: Privileges/rules/ restrictions on what actions a particular user/person/program can take

1 mark for explaining potential impact of a misconfigured access right: user/person /program could delete/view/copy/run files that they shouldn't be able to // user/person /program could change settings that they shouldn't be able to // user/person/program could access resources they should not be able to

2

[6]

25.

All marks AO1 (understanding)

Reasons for allowing:
Teachers can access resources on the school network to allow them to plan lessons at home;
Teachers can teach lessons from home (using videoconferencing) if they are not able to get into work (eg travel difficulties);
Teachers can access electronic copies of student work so that they do not have to carry marking home;

Reasons for not allowing:
Data protection issues – schools may not want potentially sensitive student information to be accessed outside of school;
To try to help teachers have a work-life balance;
Increased security risks as teachers may not have fully-protected computers at home (eg if a teacher does not have anti-virus software on their home computer this may cause problems when they connect their computer to the school network);

Max 1 mark: if only described reasons for allowing access
Max 1 mark: if only described reasons for not allowing access

[2]

26.

Mark is for AO1 (understanding)

With black-box penetration testing the tester does not know how the security systems work, with white-box testing the tester does know how the security systems work;

Note: answer must cover both black-box and white-box to be awarded a mark

[1]

27.

2 marks for AO1 (understanding) and 4 marks for AO2 (apply)

Level 3 (5–6 marks):
Clear descriptions of two social engineering techniques have been included along with a detailed description of appropriate measures that can be taken by an organisation to reduce the risks from phishing and the social engineering techniques that have been described.

Level 2 (3–4 marks):
A description of one or two social engineering techniques has been included along with an appropriate description of one or more measures that can be taken by an organisation to reduce the risks from social engineering.

Level 1 (1–2 marks):
Answer includes one of the following: an identification of one or two social engineering techniques, a description of a method that an organisation can use to reduce the risks from phishing, identification of a social engineering technique and a description of a method that an organisation can use to reduce the risks from that social engineering technique.

0 marks:
No creditworthy answer

Guidance – Indicative Response for AO1
Pharming – setting up a fake website that looks like an official website for a reputable organisation / company (to try and harvest personal details);
Shouldering / shoulder surfing – observing a legitimate user entering (security) data into a computer system;
Baiting – leaving a malware infected portable storage device around hoping that a legitimate user will insert it into the computer system;
Pretexting / blagging – persuading (often by use of a faked scenario) legitimate users to divulge personal data;
Maximum two marks for AO1

Guidance – Indicative Response for AO2 (note must be appropriate for the social engineering techniques described for marks to be awarded)
To reduce risks from phishing: allow emails only from known sources;
To reduce risks from pharming: web filters;
To reduce risks from shouldering: careful placement of terminals;
To reduce risks from baiting: lock down systems so portable storage devices are not usable;
To reduce risks from blagging: use of security details which cannot be accidentally divulged eg biometric measures;
General strategies for reducing the risks from social engineering: train / educate users; making use of appropriate security protocols for handling sensitive / security data; performing frequent (unannounced) tests of security measures;

Maximum four marks for AO2
Maximum three marks for AO2 if no strategy to reduce the risks from phishing has been given

[6]

28. **All marks AO2 (apply)**

Level 3 (7–9 marks):
Answer demonstrates a **sustained line of reasoning** with a **substantiated** explanation for the recent large growth in the use of cloud storage that includes **both** technological and social reasons.

There is a **logically structured** consideration of the advantages and the disadvantages associated with the use of cloud storage – including **relevant** points covering **at least two** of legal, ethical and environmental issues.

Level 2 (4–6 marks):
Answer includes an explanation for the recent large growth in the use of cloud storage that includes **both** technological and social reasons.

There is a **logically structured** consideration of the advantages and the disadvantages associated with the use of cloud storage – including **one or two relevant** points related to legal, ethical and environmental issues.

Level 1 (1–3 marks):
The answer includes either a description of some of the reasons for the recent large growth in the use of cloud computing and / or brief consideration of the advantages and / or disadvantages associated with using cloud storage.

0 marks:
No creditworthy answer

Guidance – Indicative Response (reasons for growth)
Higher bandwidth mobile networks (eg 4G);
Increased availability of mobile devices;
Reduction in cost of large capacity storage devices;
Improvements in network security;
People have a higher level of trust in cloud storage;
Improvements in web browser software;
Increased availability of supercomputers (for cloud processing);
Companies have managed to develop business models based on cloud computing that allow them to make a profit;

Guidance – Indicative Response (advantages of cloud storage)
Enables user to access their data from more places / devices;
Enables user to more easily share data with others (can make parts of their cloud storage publically available);
Increases the amount of storage available;
Reduced cost of computing devices for users as no need for as much built-in secondary storage;

Guidance – Indicative Response (disadvantages of cloud storage)
Increased security risks;
Relies on access to high-bandwidth network connection;
Could potentially cost more due to ongoing costs;
Reliance on company providing the cloud service;
Increased chance of others accessing personal data (data privacy issues);

[9]

29.

2 marks for AO1 (understanding) and 2 marks for AO2 (apply)

1 mark for AO1: Authentication is ensuring that a user is who they are claiming to be;

1 mark for AO2: The business could give each employee their own username and password // the business could use a biometric system, e.g. fingerprints, to check which employee is logging in / to ensure that only employees can log in;

1 mark for AO1: Encryption is changing data so that it cannot be read (except by authorised users / those with the decryption key);

1 mark for AO2: The business could use encryption to prevent unauthorised people from reading sensitive data; **A.** example of sensitive data eg personnel records

[4]

30.

Nine marks for AO1 (understanding)

Level 3 (7–9 marks):
Clear descriptions of the similarities and the differences between all or almost all of the four stated types of malware.

At least three appropriate measures that can be taken to minimise the risks posed by malware have been described.

Level 2 (4–6 marks):
Answer includes one of the following:

- Clear descriptions of the similarities and the differences between all or almost all of the four stated types of malware.
- Descriptions of the similarities and the differences between some of the types of malware and descriptions of more than one appropriate measure that can be taken to minimise the risks posed by malware.

Level 1 (1–3 marks):
Answer includes one of the following:

- Descriptions of some of the differences between the different types of malware.
- Descriptions of some of the similarities between the different types of malware.
- Description of appropriate measures that can be taken to minimise the risks posed by malware.

0 marks:
No creditworthy answer

Guidance – Indicative Response for differences
Users sometimes choose to allow / install adware (this is not the case with the other types of malware);
An alternative to purchasing software can be to use free software that makes use of adware;
Spyware tracks what a user is doing – adware doesn’t;
Adware does not do any harm to a computer system (unlike spyware, viruses and Trojans) though it can be irritating and be used to conceal spyware;
Spyware and Trojans are often installed unwittingly by the user;
Viruses can replicate themselves / spread without user being involved;
Trojans and viruses can be very destructive;
Spyware and adware work in the same way;
All four types of malware can be intrusive / disruptive;

Guidance – Indicative Response for minimising risks
Read software license agreements before installing software as sometimes these state that spyware will be installed;
Install anti-spyware / virus software;
Update anti-spyware / virus software regularly;
Run anti-spyware / virus software regularly;
Before downloading / installing new software complete research to check if it is safe / provided by an organisation that can be trusted;
Be careful when using peer-to-peer file sharing;
Don’t open attachments on emails from people you don’t know / trust;
Adjust browser security settings;

Maximum four marks for minimising the risks from malware.
Maximum six marks for comparison of types of malware.

[9]

31. (a) (i) Fourth box only;

Test data	**Tick one box**
-1, 0, 9, 10	
0, 1, 10, 11	
-1, 0, 10, 11	
0, 1, 9, 10	✓

1

(ii) They test the boundaries;

A. other wording that has equivalent meaning.

1

(b) Marks awarded as follows (allow any logically equivalent and correct answer). The marks are labelled **A – E** and shown in the examples where they are awarded:

A. 1 mark for assigning user input to a variable (permit any variable name);
B. 1 mark for assigning the second user input to a distinct variable from that used in **A**, or the second user input used in such a way that doesn't require a variable, e.g. USERINPUT = password1;
C. 1 mark for using a condition-controlled loop such as a `WHILE` loop with a correct Boolean expression to control this loop (this will depend on the type of loop used but will test for equality of the two passwords);
D. 1 mark for the user inputting the two passwords again within the loop and assigning these to their respective variables;
E. 1 mark for outputting "`password created`" at a point in the code where no further user input will occur
(**A.** spelling mistakes for "`password created`");

Example 1 (italicised square brackets indicate where marks are awarded):

```
password1 ← USERINPUT [A]
password2 ← USERINPUT [B]
WHILE password1 ≠ password2 [C]
  password1 ← USERINPUT
  password2 ← USERINPUT [D with line above]
ENDWHILE
OUTPUT 'password created' [E]
```

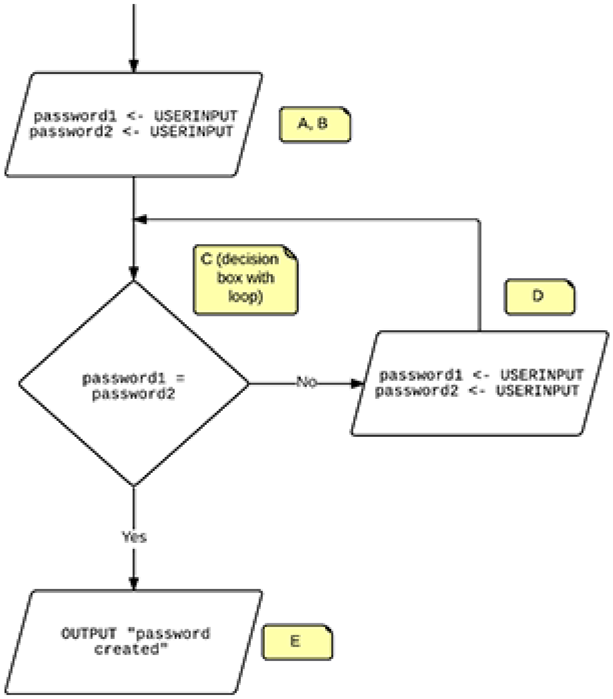
Example 2 (italicised square brackets indicate where marks are awarded):

```
password1 ← USERINPUT [A]
password2 ← USERINPUT [B]
match ← false
IF password1 = password2 THEN
  match ← true
ENDIF
WHILE match = false [C with three lines above and the IF statement within the loop]
  password1 ← USERINPUT
  password2 ← USERINPUT [D with line above]
  IF password1 = password2 THEN
    match ← true
  ENDIF
ENDWHILE
OUTPUT 'password created' [E]
```

Example 3 (italicised square brackets indicate where marks are awarded):

```
match ← false
REPEAT
  password1 ← USERINPUT [A]
  password2 ← USERINPUT [B][D with line above]
  IF password1 = password2 THEN
    match ← true
    OUTPUT 'password created' [E]
  ENDIF
UNTIL match = true [C for condition for DO-WHILE]
```

Example 4 (notes indicate where marks are awarded):



5

(c) Any creditworthy point to a **maximum of two**. Examples include:

They do not have a minimum length // they can be blank;
They do not have to have a mixture of alphabetic and numeric characters;
They may have consecutive numbers within them;
They may be easily guessable names;

2

[9]