Pearson
BTEC Level 2 Technical Certificate in IT Support

First teaching September 2017

Sample Assessment Materials: Unit 3: Security Protection and Risk Management

Version 1.0

Edexcel, BTEC and LCCI qualifications

Edexcel, BTEC and LCCI qualifications are awarded by Pearson, the UK's largest awarding body offering academic and vocational qualifications that are globally recognised and benchmarked. For further information, please visit our qualification websites at www.edexcel.com, www.btec.co.uk or www.lcci.org.uk. Alternatively, you can get in touch with us using the details on our contact us page at qualifications.pearson.com/contactus

About Pearson

Pearson is the world's leading learning company, with 40,000 employees in more than 70 countries working to help people of all ages to make measurable progress in their lives through learning. We put the learner at the centre of everything we do, because wherever learning flourishes, so do people. Find out more about how we can help you and your learners at qualifications.pearson.com

References to third-party material made in this specification are made in good faith. We do not endorse, approve or accept responsibility for the content of materials, which may be subject to change, or any opinions expressed therein. (Material may include textbooks, journals, magazines and other publications and websites.)

BTEC L2 Technical Certificate in IT Support
Unit 3: Security Protection and Risk Management

Information for candidates

Instructions

- Answer all questions.
- An onscreen notepad is provided for you to make notes during the test. These notes will not be marked.
- An accessibility panel is provided on every screen. This allows you to magnify your screen and apply a range of colour filters

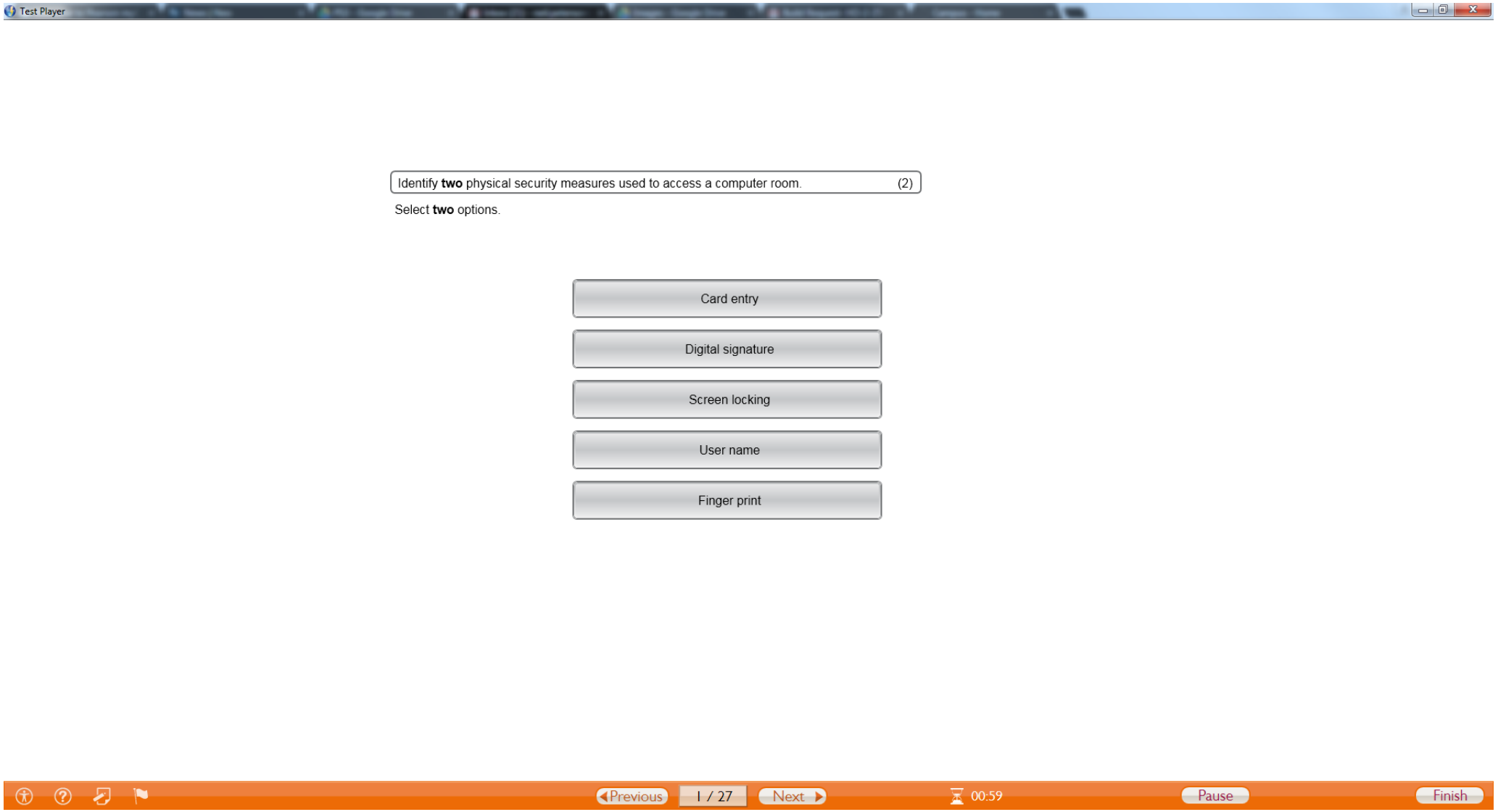
Information

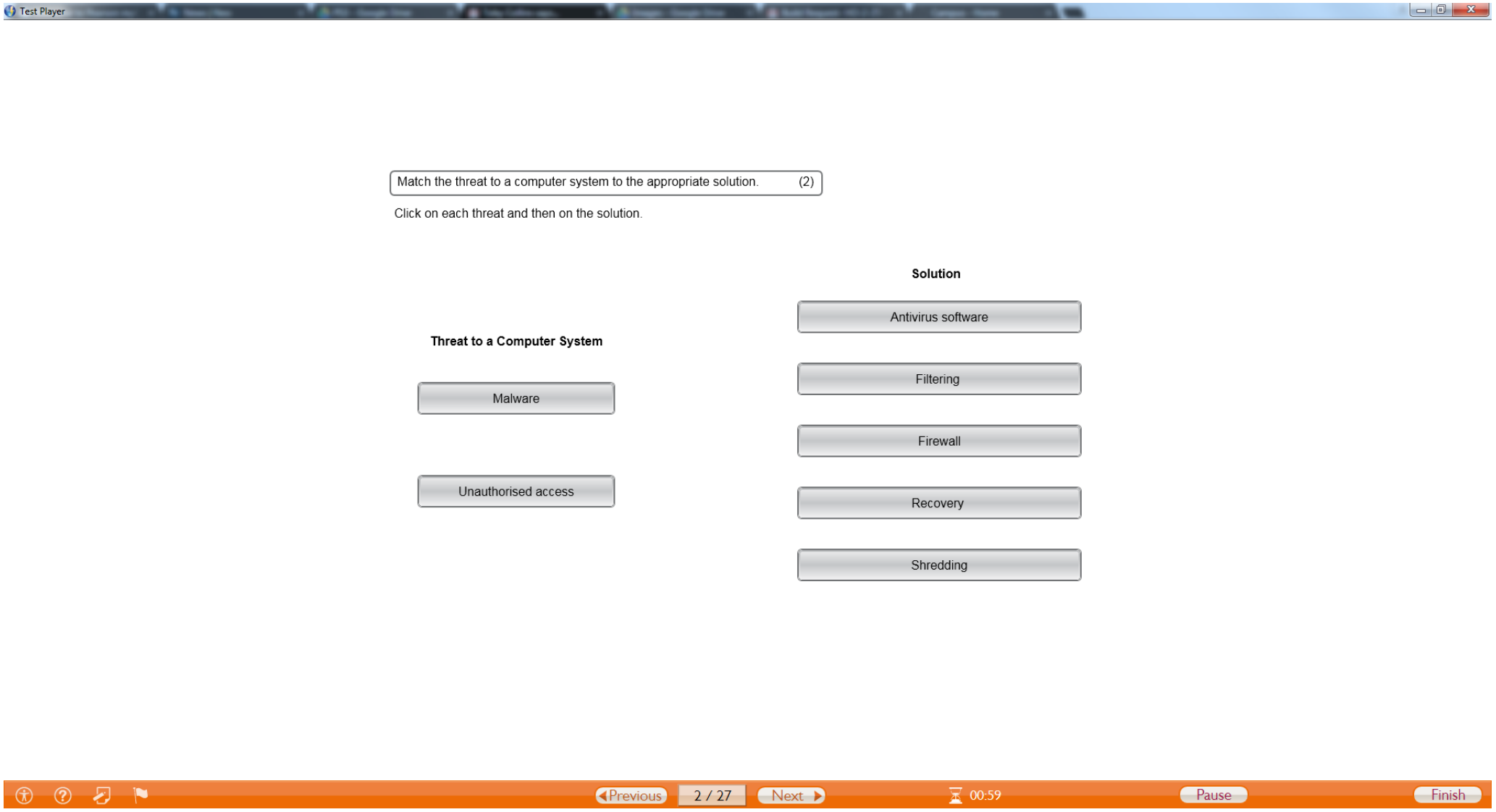
- The assessment is **1 hour 15 minutes** in duration.
- The **total mark** for this test is **60.**
- The number of marks for each question is shown in brackets e.g. (2). Use this as a guide as to how much time to spend on each question.

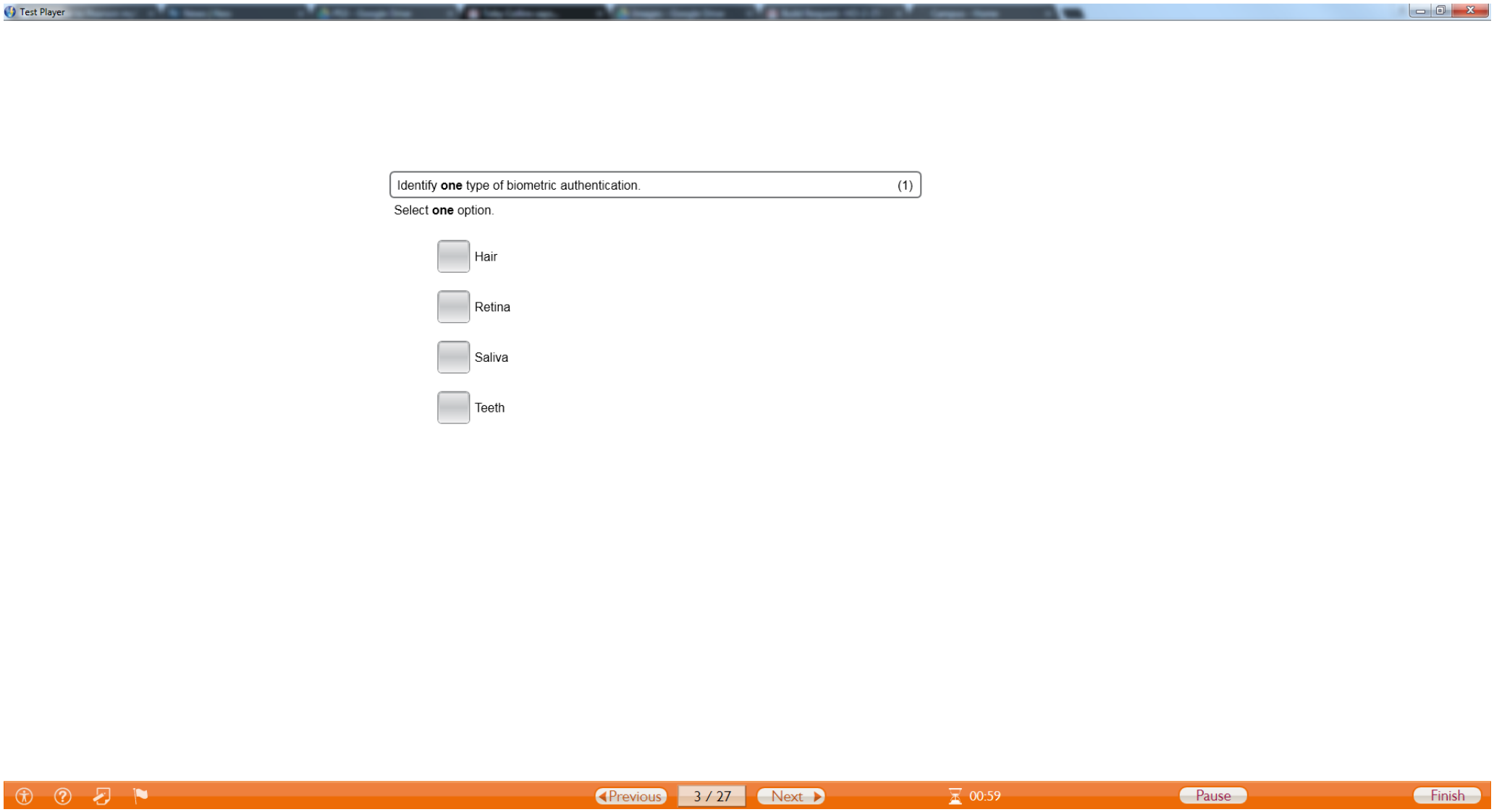
Advice

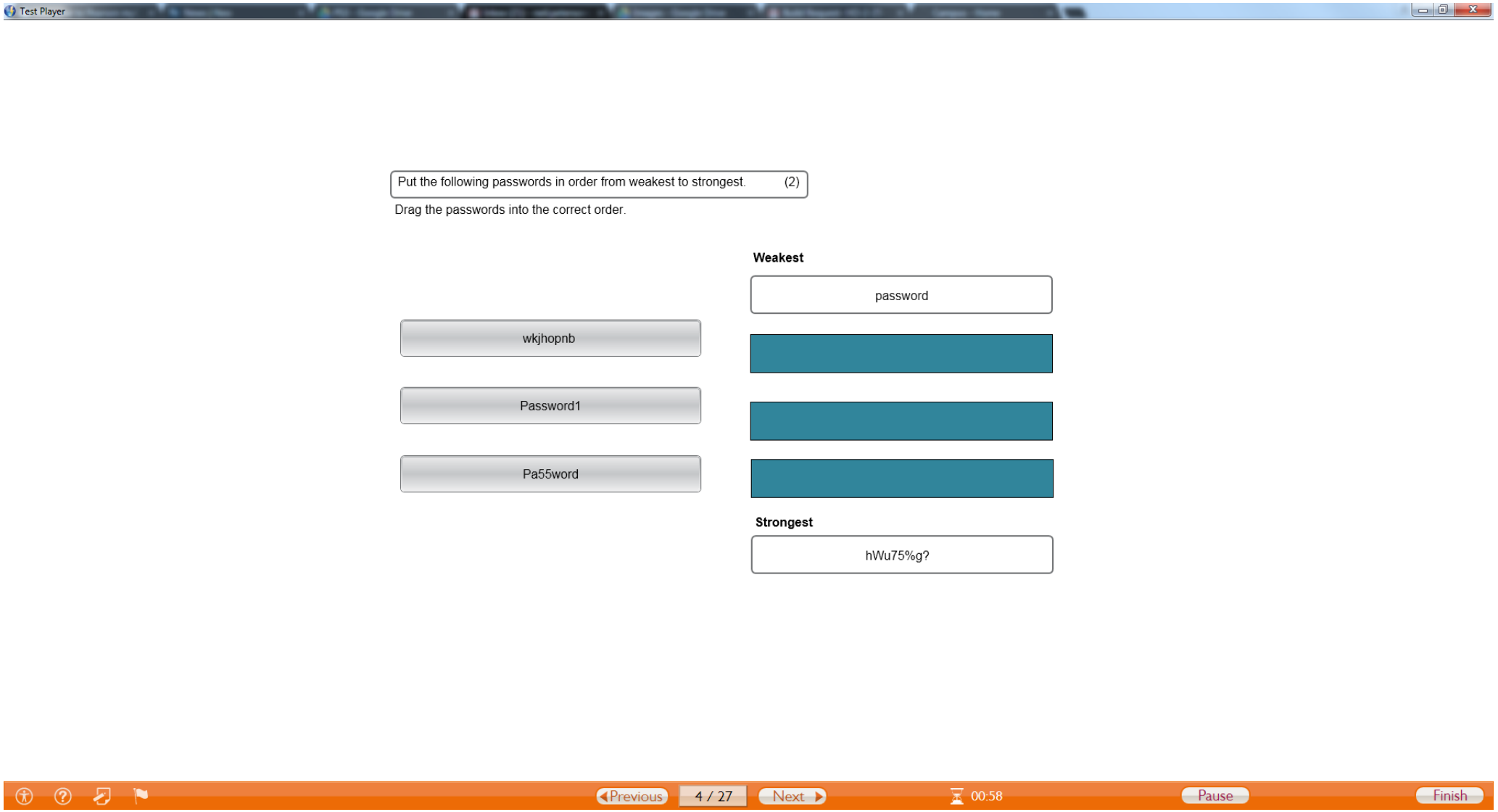
- Read each question carefully before you start to answer it.
- Keep an eye on the time.
- Try to answer every question.
- Check your answers if you have time at the end.

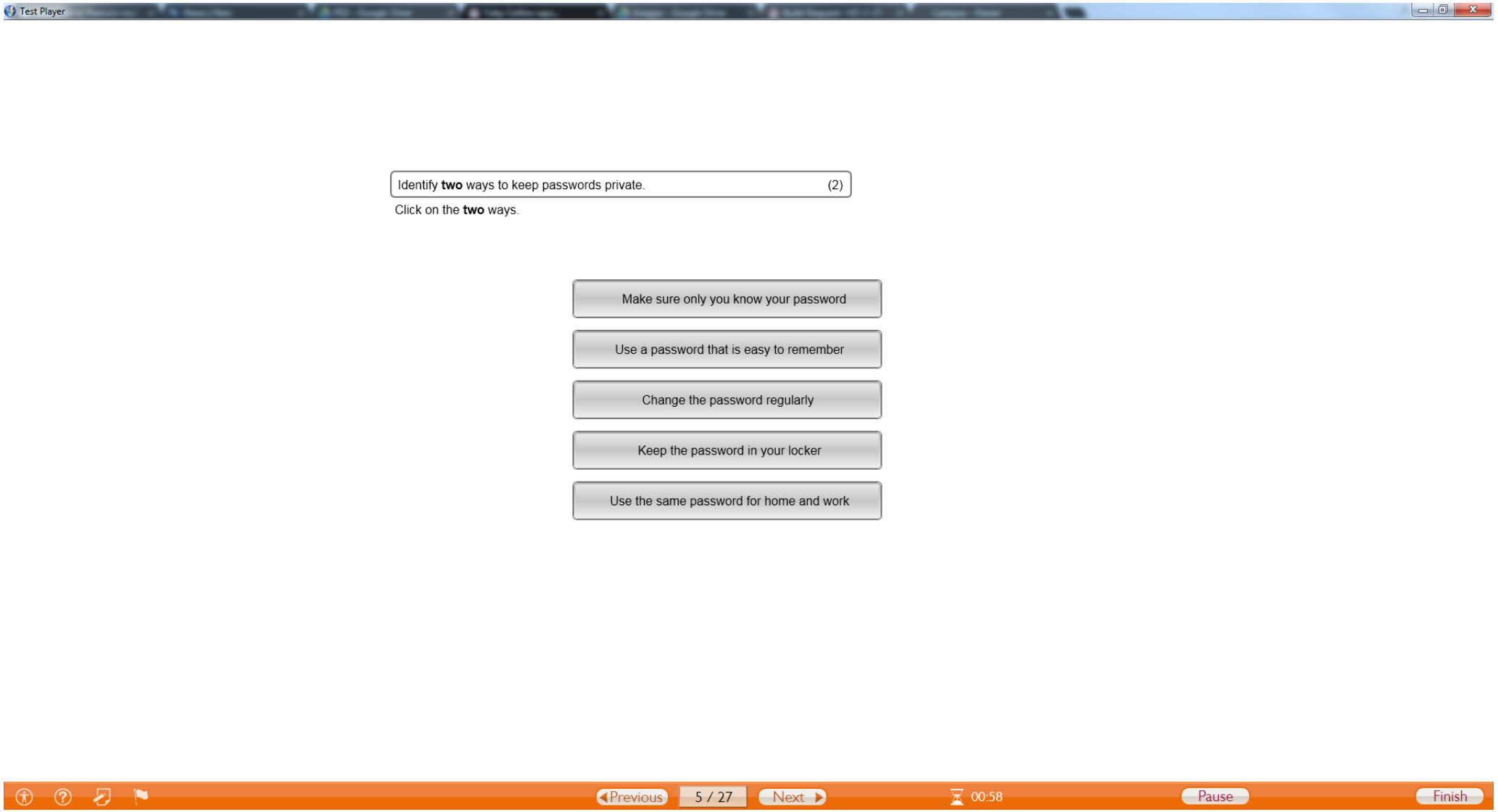
Start Test


Test Player
Identify **two** physical security measures used to access a computer room. (2)
Select **two** options.
Card entry
Digital signature
Screen locking
User name
Finger print
Previous
1 / 27
Next
00:59
Pause
Finish


Test Player
Match the threat to a computer system to the appropriate solution. (2)
Click on each threat and then on the solution.
Threat to a Computer System
Malware
Unauthorised access
Solution
Antivirus software
Filtering
Firewall
Recovery
Shredding
Previous
2 / 27
Next
00:59
Pause
Finish


Test Player
Identify **one** type of biometric authentication. (1)
Select **one** option.
Hair
Retina
Saliva
Teeth
Previous
3 / 27
Next
00:59
Pause
Finish


Test Player
Put the following passwords in order from weakest to strongest. (2)
Drag the passwords into the correct order.
wkjhopnb
Password1
Pa55word
Weakest
password
Strongest
hWu75%g?
Previous
4 / 27
Next
00:58
Pause
Finish

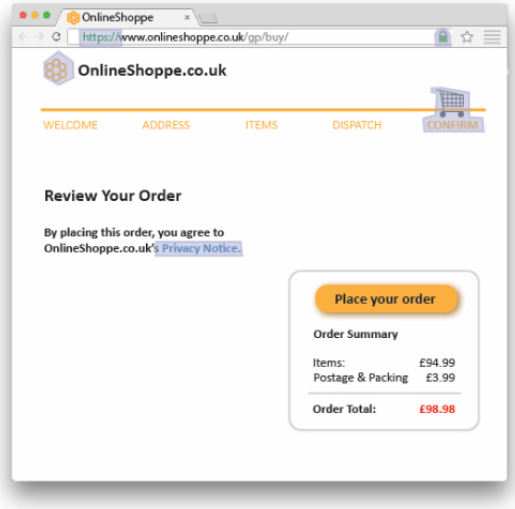

Test Player
Identify **two** ways to keep passwords private. (2)
Click on the **two** ways.
Make sure only you know your password
Use a password that is easy to remember
Change the password regularly
Keep the password in your locker
Use the same password for home and work
Previous
5 / 27
Next
00:58
Pause
Finish

Test Player

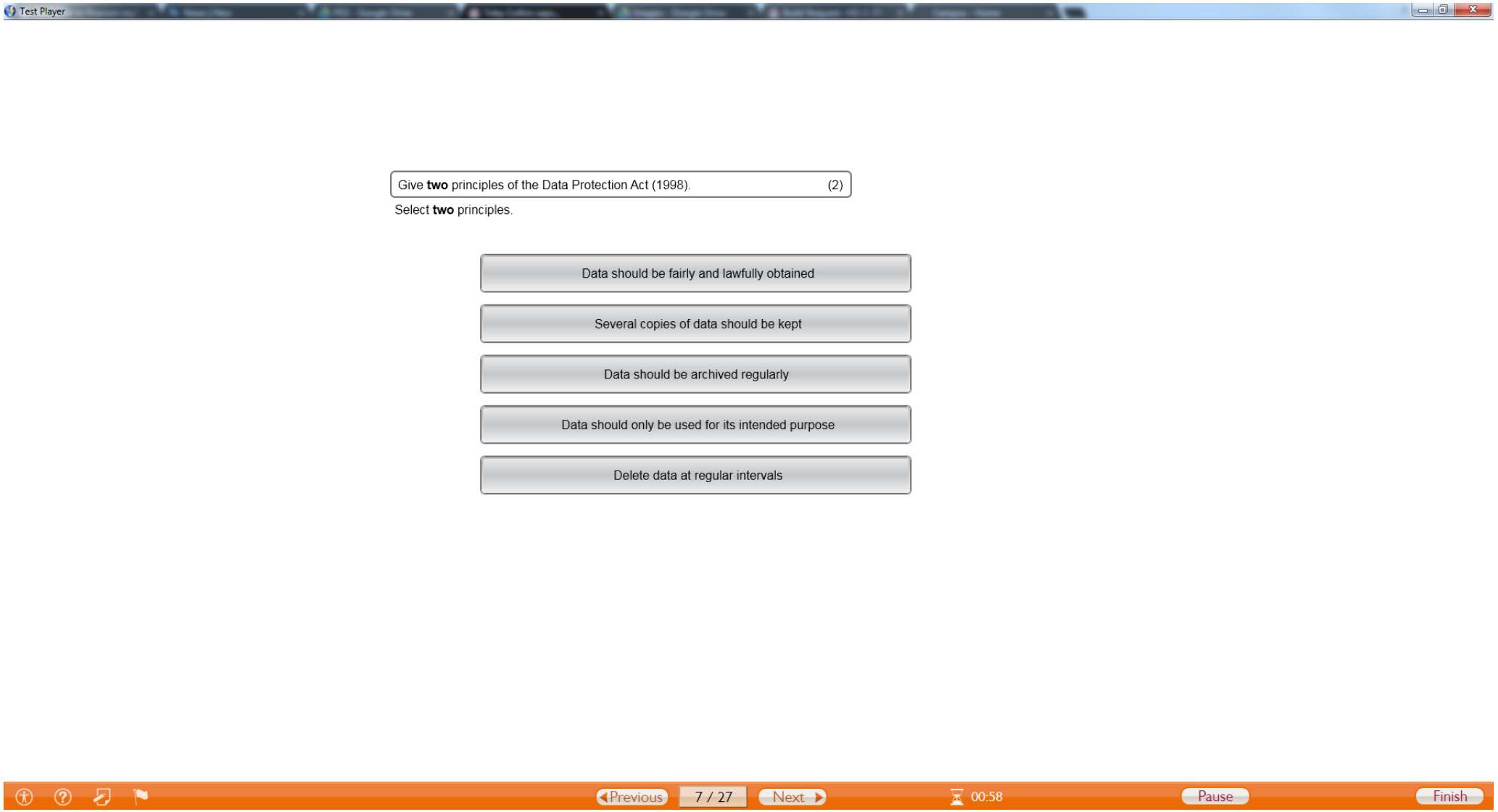
The image shows a page from a secure website

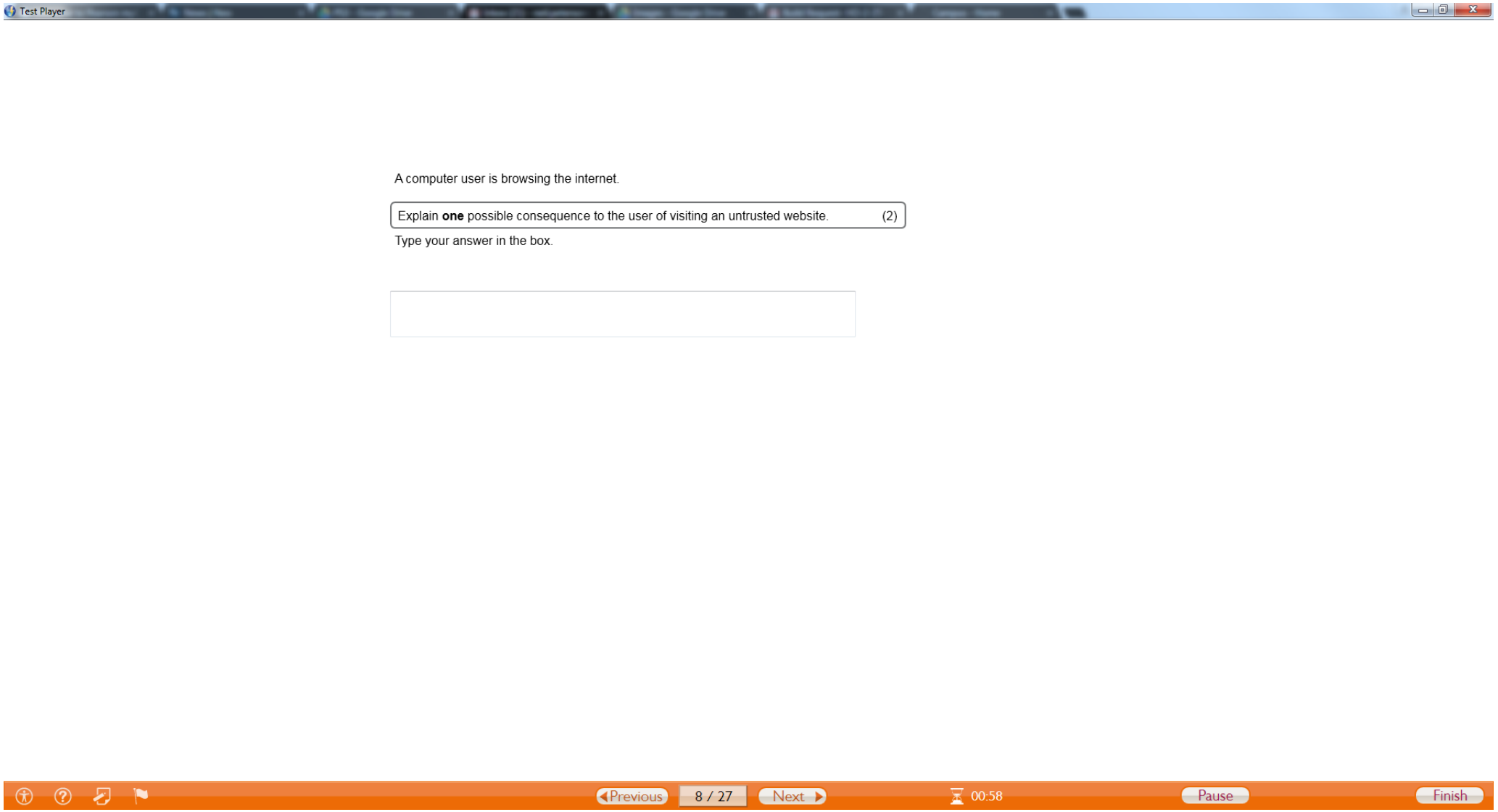
Which **two** parts of the image show that the website is secure? (2)

Click on the **two** correct parts of the image.



Previous 6 / 27 Next 00:58 Pause Finish


Test Player
Give two principles of the Data Protection Act (1998). (2)
Select two principles.
Data should be fairly and lawfully obtained
Several copies of data should be kept
Data should be archived regularly
Data should only be used for its intended purpose
Delete data at regular intervals
Previous
7 / 27
Next
00:58
Pause
Finish


Test Player
A computer user is browsing the internet.
Explain **one** possible consequence to the user of visiting an untrusted website. (2)
Type your answer in the box.
Previous
8 / 27
Next
00:58
Pause
Finish

Test Player

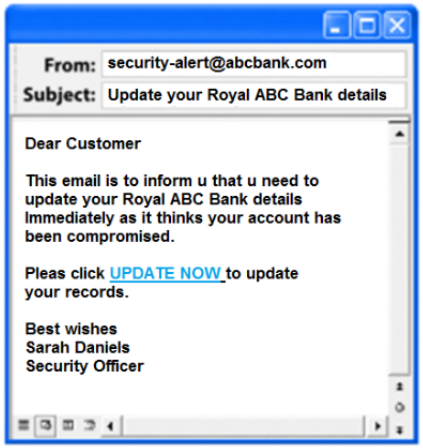
The image shows a phishing email.

Identify **two** features that indicate that this is a phishing email. (2)

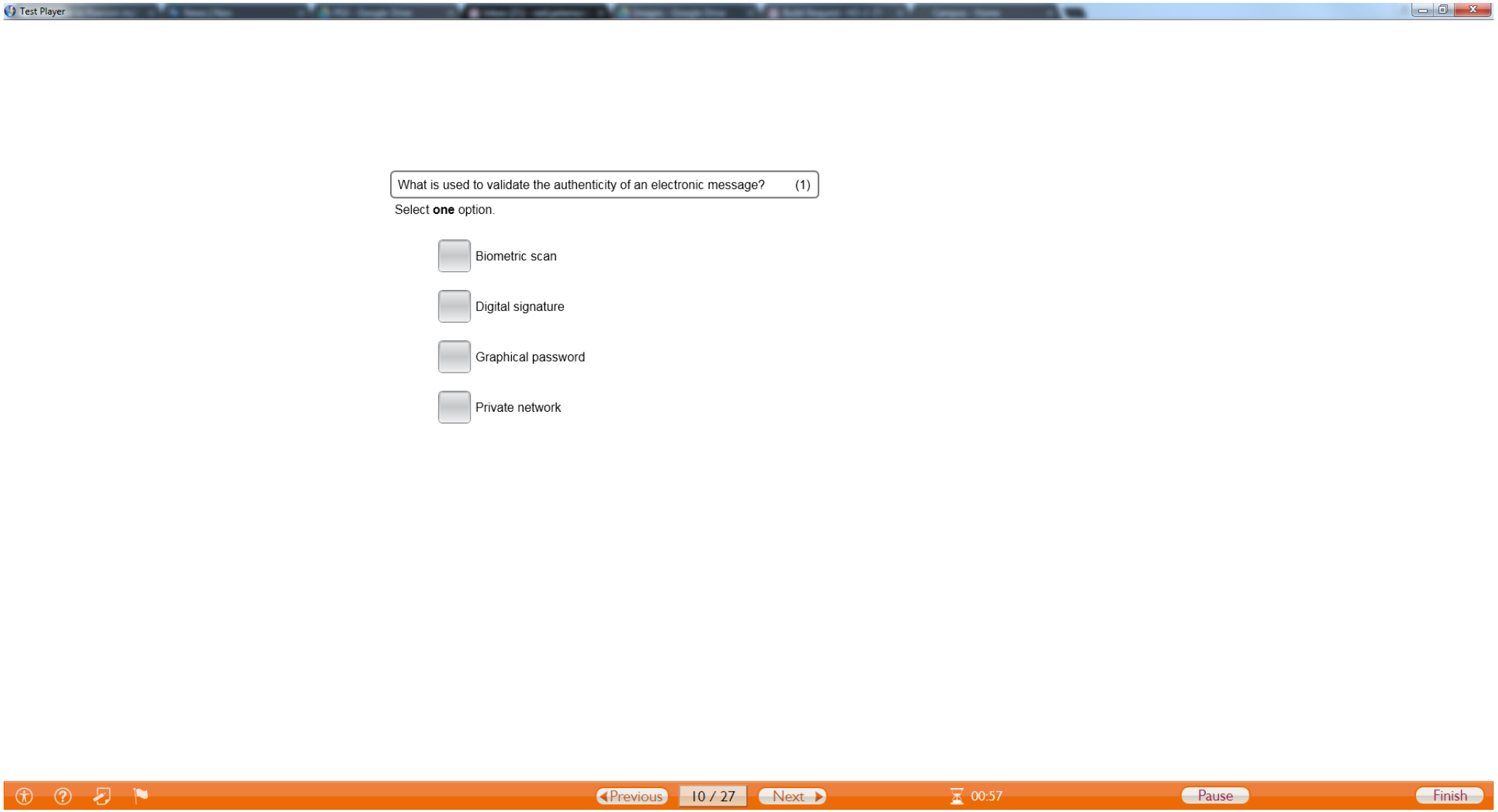
Type your answers in the boxes.

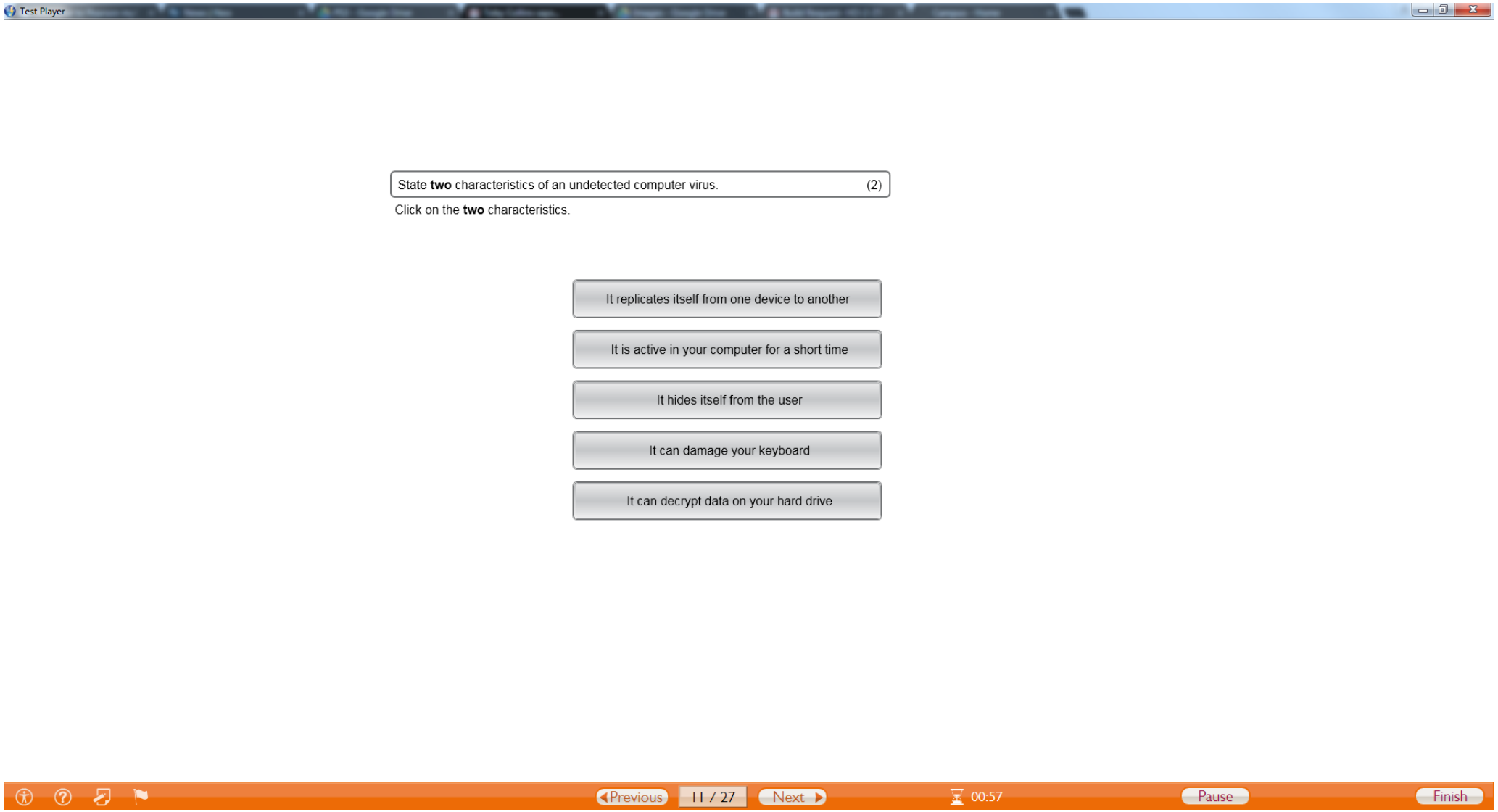
Feature 1

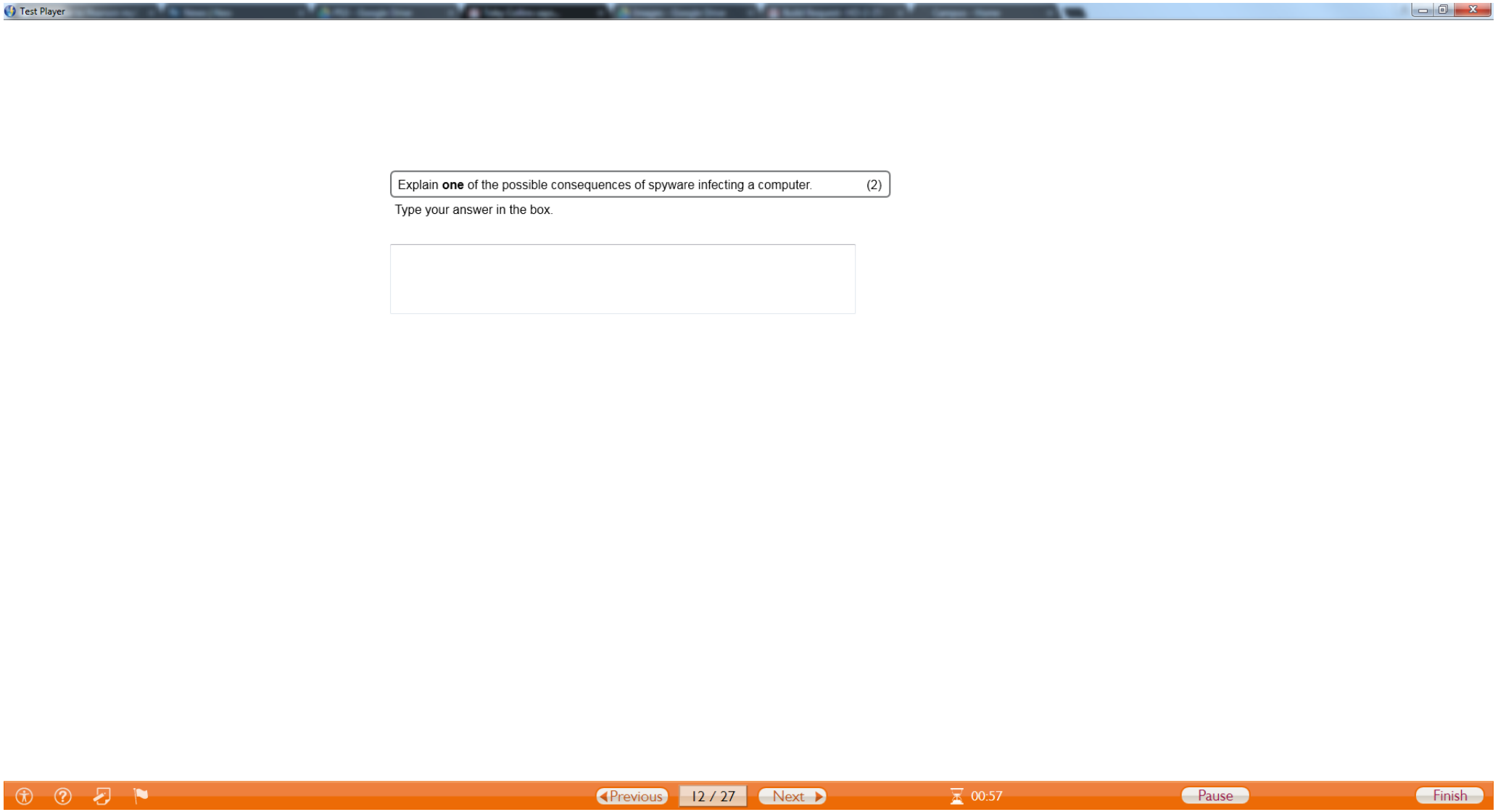
Feature 2



Previous 9 / 27 Next 00:57 Pause Finish


Test Player
What is used to validate the authenticity of an electronic message? (1)
Select one option.
Biometric scan
Digital signature
Graphical password
Private network
Previous
10 / 27
Next
00:57
Pause
Finish


Test Player
State **two** characteristics of an undetected computer virus. (2)
Click on the **two** characteristics.
It replicates itself from one device to another
It is active in your computer for a short time
It hides itself from the user
It can damage your keyboard
It can decrypt data on your hard drive
Previous
11 / 27
Next
00:57
Pause
Finish


Test Player
Explain **one** of the possible consequences of spyware infecting a computer. (2)
Type your answer in the box.
Previous
12 / 27
Next
00:57
Pause
Finish

Test Player

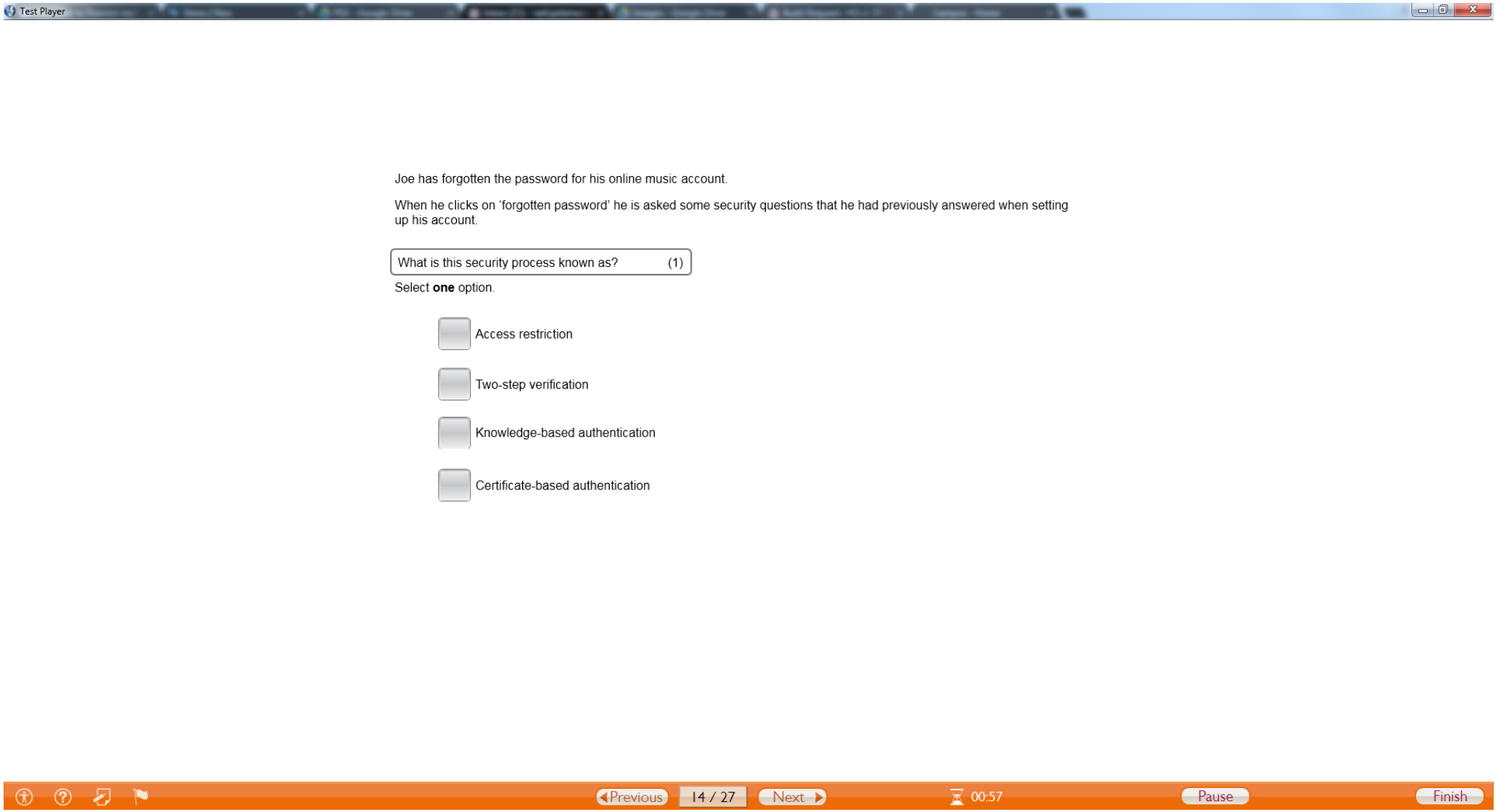
When registering for an account on a retailer's website a user sees this screen test.

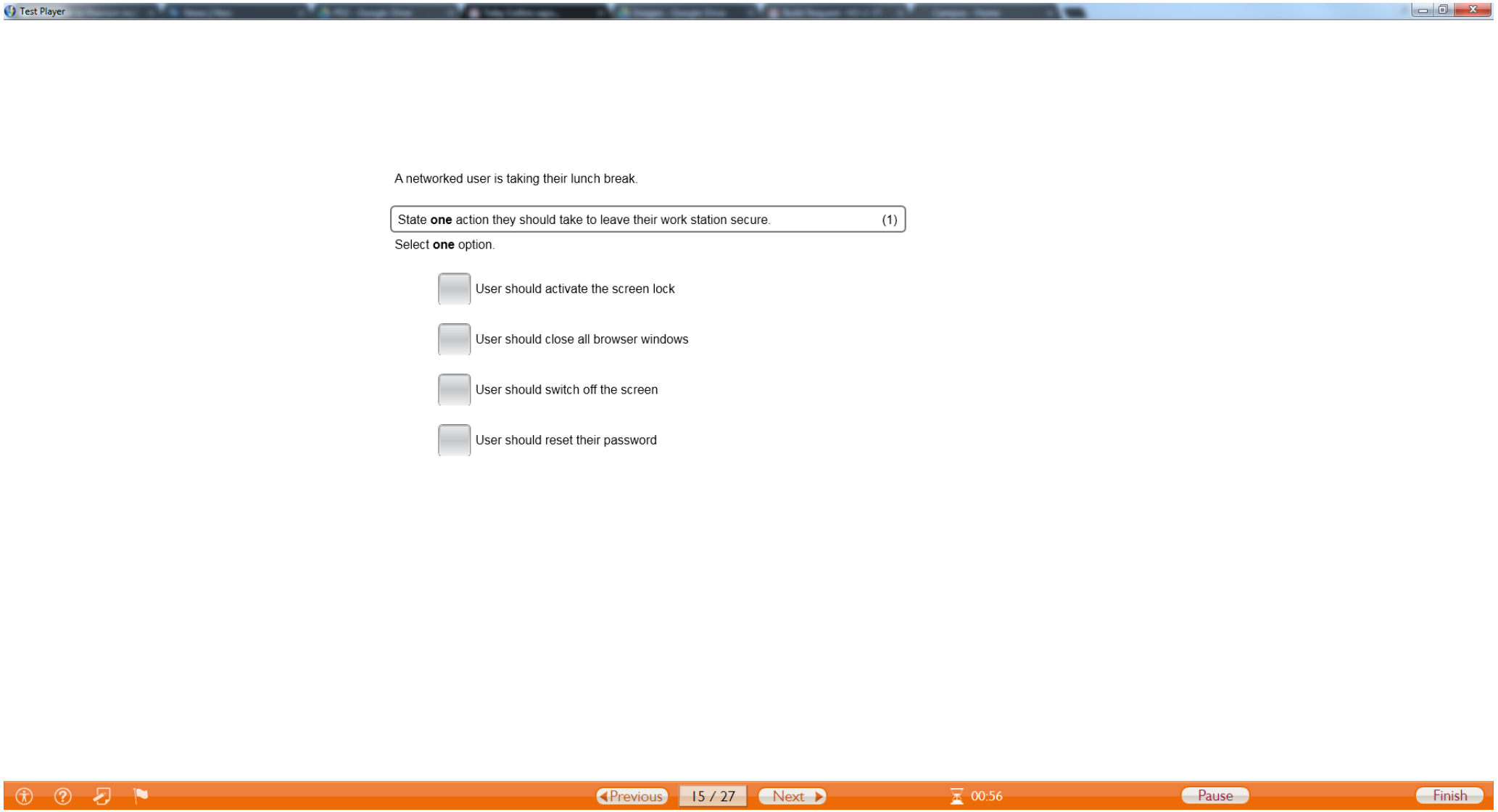
Why is this type of test used? (1)

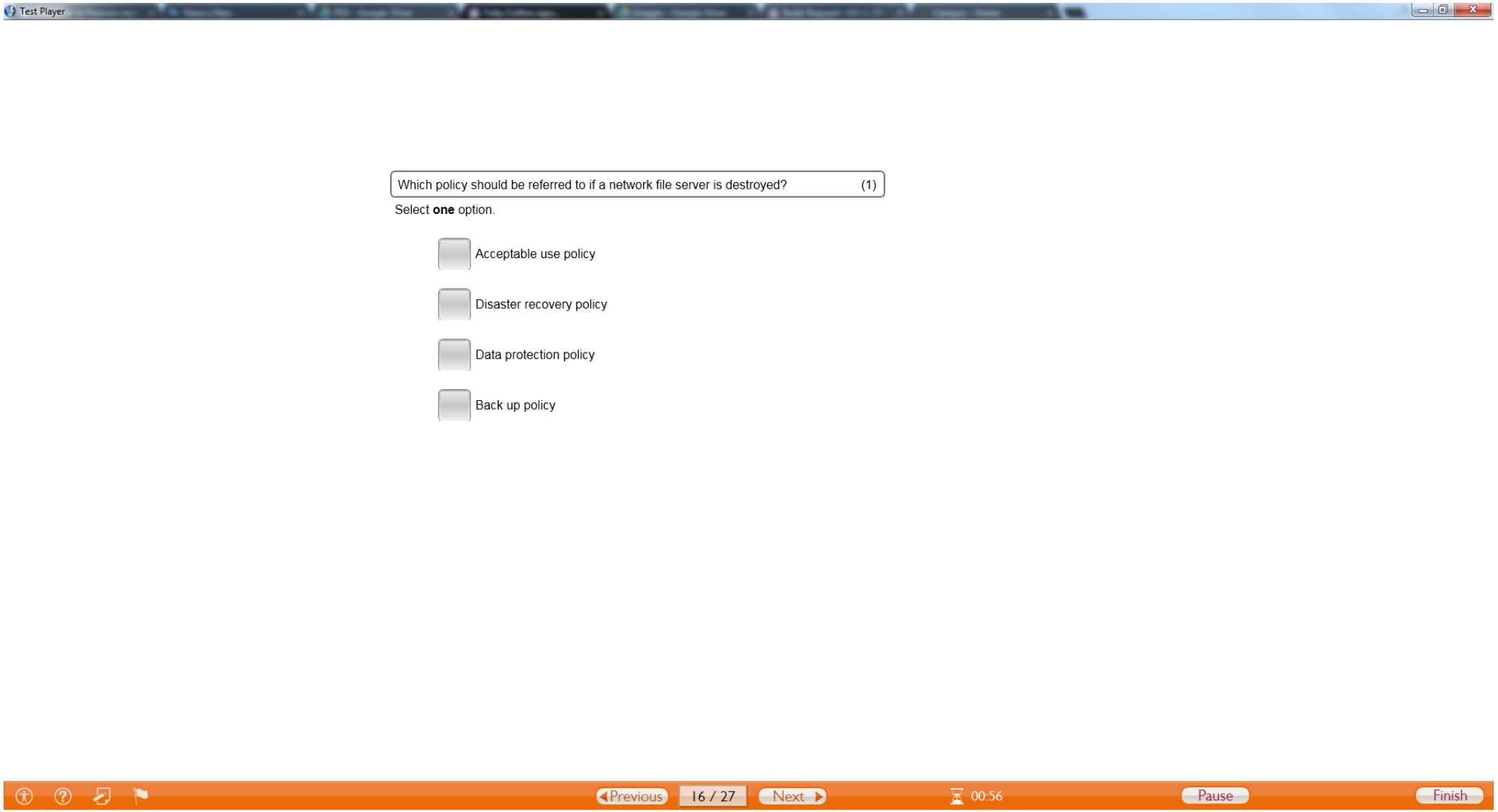
Select **one** option.

- To check that the new user name is available
- To allow automated password generation
- To tell humans and computers apart
- To ensure that the user's keyboard is working properly

Previous 13 / 27 Next 00:57 Pause Finish


Test Player
Joe has forgotten the password for his online music account.
When he clicks on 'forgotten password' he is asked some security questions that he had previously answered when setting up his account.
What is this security process known as? (1)
Select one option.
Access restriction
Two-step verification
Knowledge-based authentication
Certificate-based authentication
Previous
14 / 27
Next
00:57
Pause
Finish


Test Player
A networked user is taking their lunch break.
State one action they should take to leave their work station secure. (1)
Select one option.
User should activate the screen lock
User should close all browser windows
User should switch off the screen
User should reset their password
Previous
15 / 27
Next
00:56
Pause
Finish


Test Player
Which policy should be referred to if a network file server is destroyed? (1)
Select one option.
Acceptable use policy
Disaster recovery policy
Data protection policy
Back up policy
Previous
16 / 27
Next
00:56
Pause
Finish

Test Player

Every company should have a policy for how frequently data is backed up.

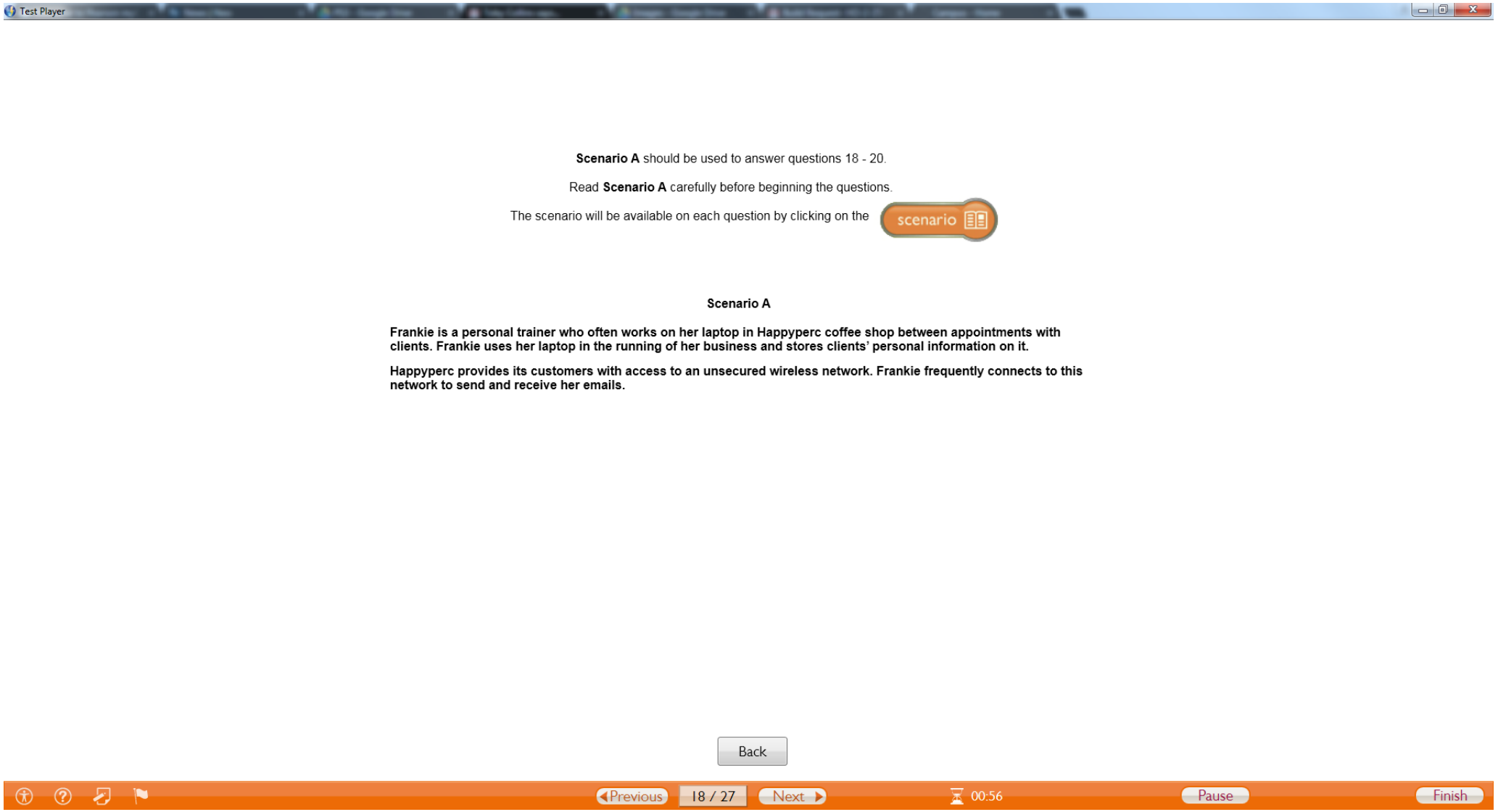
Explain **two** factors which affect how frequently data needs to be backed up. (4)

Type your answers in the boxes.

Factor 1:

Factor 2:

Previous 17 / 27 Next 00:56 Pause Finish


Test Player
Scenario A should be used to answer questions 18 - 20.
Read **Scenario A** carefully before beginning the questions.
The scenario will be available on each question by clicking on the scenario
Scenario A
Frankie is a personal trainer who often works on her laptop in Happyperc coffee shop between appointments with clients. Frankie uses her laptop in the running of her business and stores clients' personal information on it.
Happyperc provides its customers with access to an unsecured wireless network. Frankie frequently connects to this network to send and receive her emails.
Back
Previous
18 / 27
Next
00:56
Pause
Finish

Test Player

The question relates to **Scenario A**. Click on the scenario button to see the scenario. scenario

Identify **three** risks associated with Frankie using her laptop in Happyperc coffee shop. (3)

Type your answers in the boxes.

Risk 1

Risk 2

Risk 3

Previous 18 / 27 Next 00:56 Pause Finish

Test Player

The question relates to **Scenario A**. Click on the scenario button to see the scenario. scenario

Explain **one** precaution that Frankie could take to improve security when accessing the internet in Happyperc. (2)

Type your answer in the box.

Previous 19 / 27 Next 00:56 Pause Finish

Test Player

The question relates to **Scenario** A. Click on the scenario button to see the scenario scenario

Happyperc are considering using encryption to secure their wireless network.

Explain **two** ways encryption would provide security for the Happyperc wireless network. (4)

Type your answers in the boxes.

Way 1

Way 2

Previous 20 / 27 Next 00:56 Pause Finish

Test Player

Scenario B should be used to answer questions 21 - 24.

Read **Scenario B** carefully before beginning the questions.

The scenario will be available on each question by clicking on the 

Scenario B

Kernow Technologies is a small company with a Local Area Network (LAN) of computers. A file server stores data centrally in individual user areas and in shared areas.

Staff are given user controlled access rights to the LAN.

The company uses a legacy operating system.

Managers, sales and customer service staff have different levels of access to centrally stored data.

Levels of access to files and to the system are controlled by access rights.

Back

Previous 21 / 27 Next 00:55 Pause Finish

Test Player

The question relates to **Scenario B**. Click on the scenario button to see the scenario. scenario

Give **two** types of file access rights that could be set up for staff. (2)

Type your answers in the boxes.

Type 1

Type 2

Previous 21 / 27 Next 00:55 Pause Finish

Test Player

The question relates to **Scenario B**. Click on the scenario button to see the scenario. scenario

System access controls can restrict access to user files on the system.

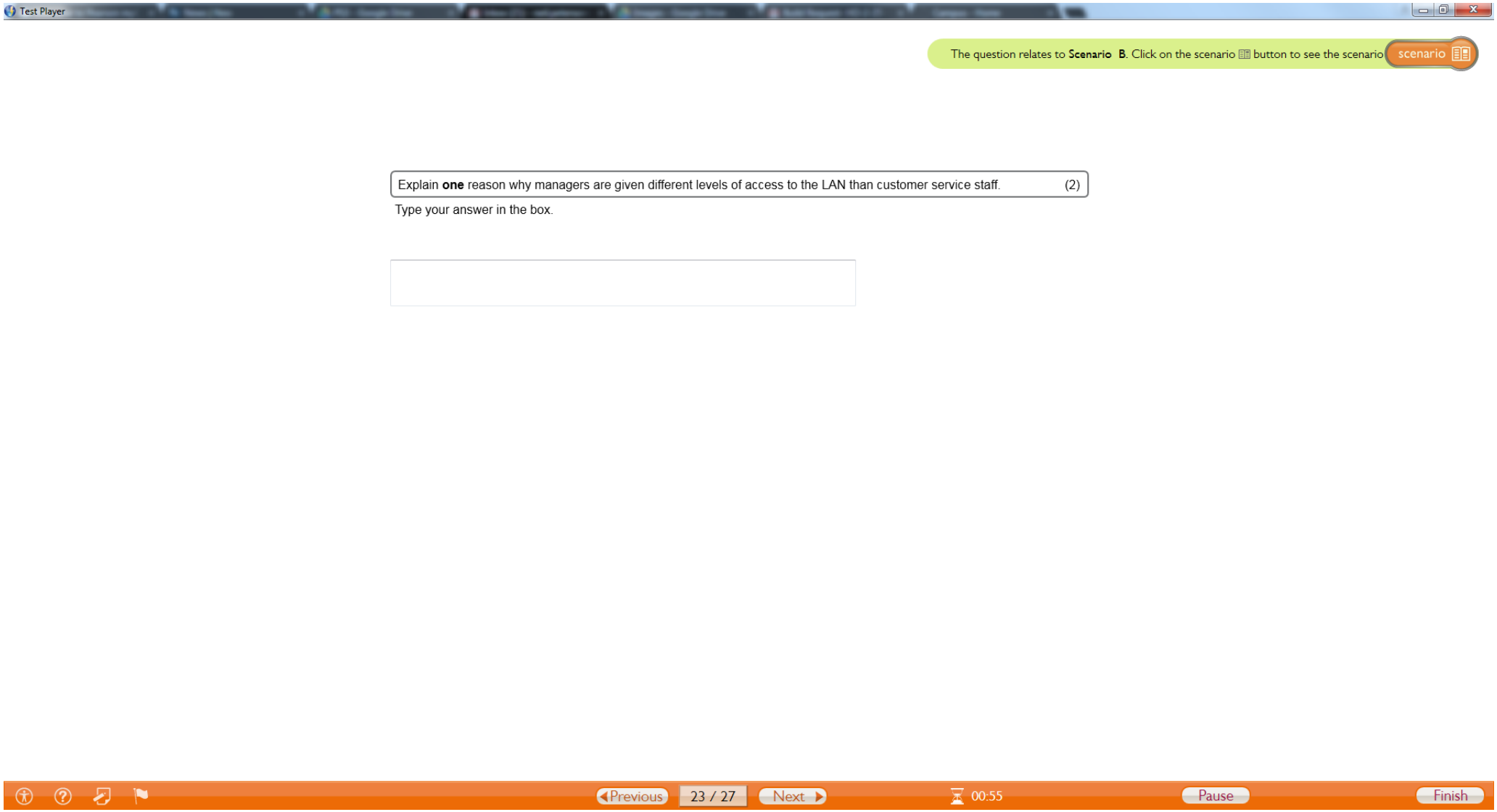
Give **two** other restrictions imposed by system access controls. (2)

Type your answers in the boxes.

Restrictions 1

Restrictions 2

Previous 22 / 27 Next 00:55 Pause Finish


Test Player
The question relates to Scenario B. Click on the scenario button to see the scenario
scenario
Explain one reason why managers are given different levels of access to the LAN than customer service staff. (2)
Type your answer in the box.
Previous
23 / 27
Next
00:55
Pause
Finish

Test Player

The question relates to **Scenario B**. Click on the scenario button to see the scenario scenario

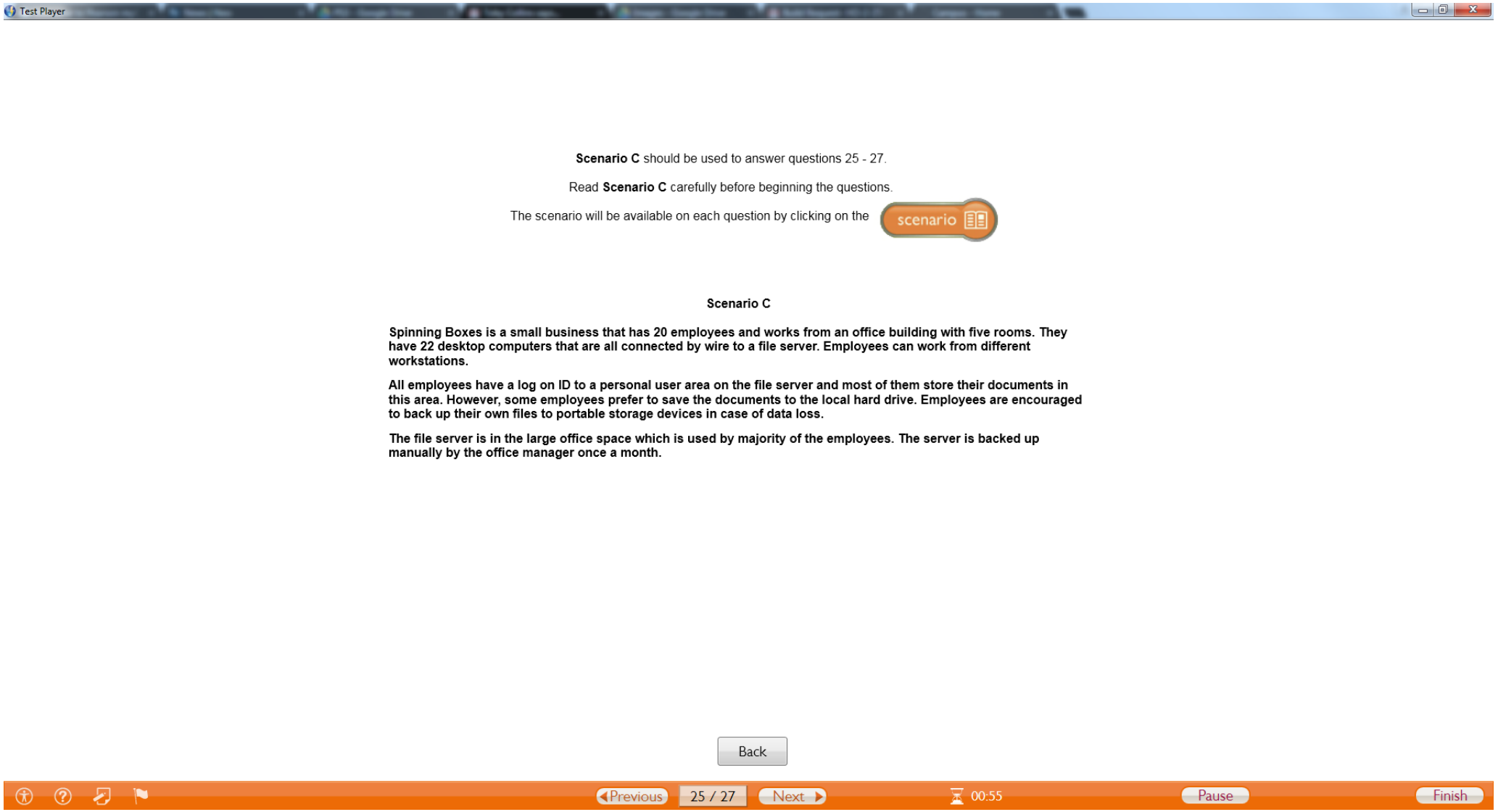
Explain **two** risks to Kernow Technologies of using a legacy operating system. (4)

Type your answers in the boxes.

Risk 1

Risk 2

Previous 24 / 27 Next 00:55 Pause Finish


Test Player
Scenario C should be used to answer questions 25 - 27.
Read Scenario C carefully before beginning the questions.
The scenario will be available on each question by clicking on the
scenario
Scenario C
Spinning Boxes is a small business that has 20 employees and works from an office building with five rooms. They have 22 desktop computers that are all connected by wire to a file server. Employees can work from different workstations.
All employees have a log on ID to a personal user area on the file server and most of them store their documents in this area. However, some employees prefer to save the documents to the local hard drive. Employees are encouraged to back up their own files to portable storage devices in case of data loss.
The file server is in the large office space which is used by majority of the employees. The server is backed up manually by the office manager once a month.
Back
Previous
25 / 27
Next
00:55
Pause
Finish

Test Player

The question relates to **Scenario C**. Click on the scenario button to see the scenario scenario

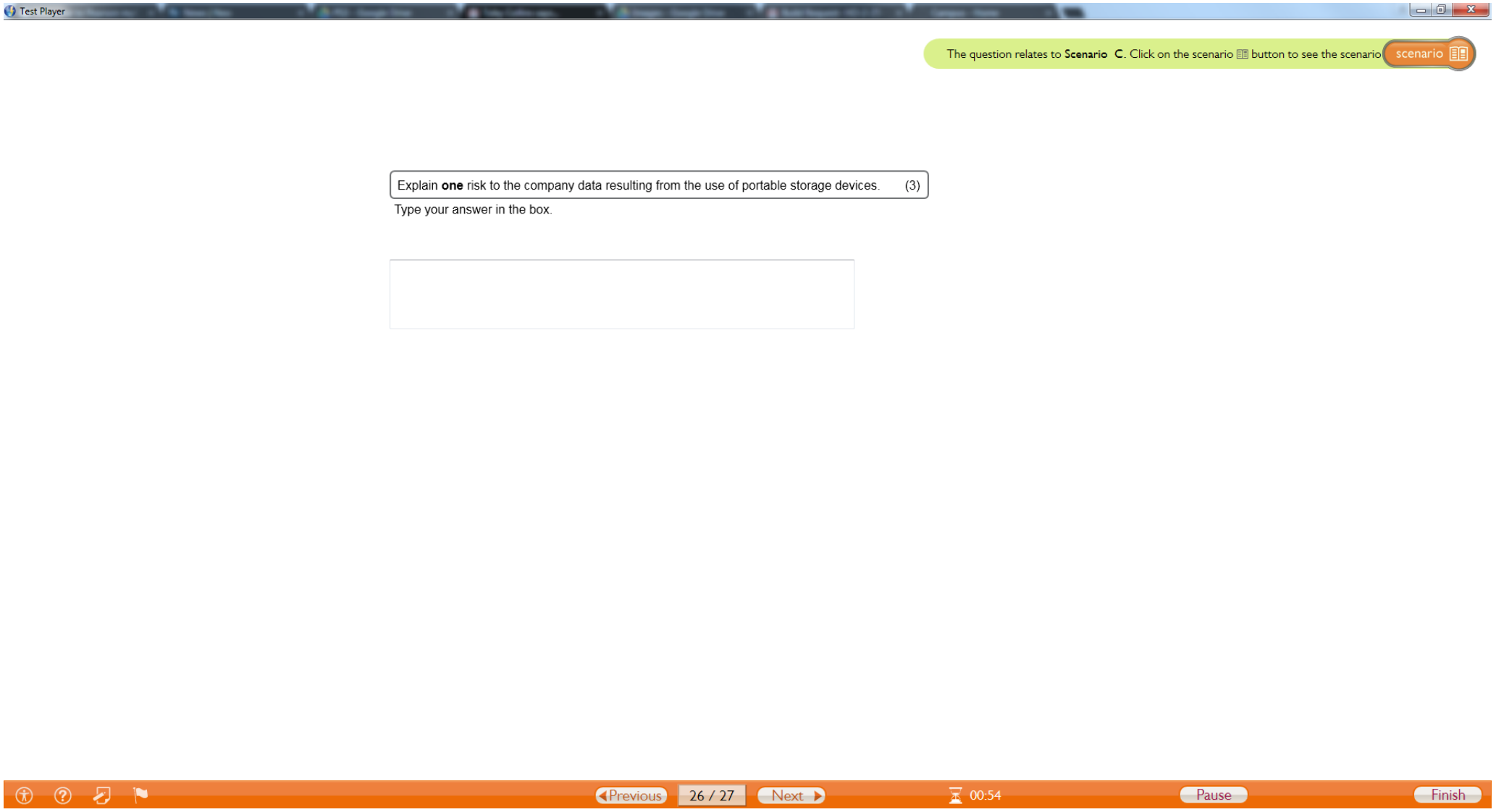
Identify **two** disadvantages of keeping the file server in the large office space. (2)

Type your answers in the boxes.

Disadvantage 1

Disadvantage 2

Previous 25 / 27 Next 00:54 Pause Finish


Test Player
The question relates to Scenario C. Click on the scenario button to see the scenario
scenario
Explain one risk to the company data resulting from the use of portable storage devices. (3)
Type your answer in the box.
Previous
26 / 27
Next
00:54
Pause
Finish

Test Player

The question relates to **Scenario C**. Click on the scenario button to see the scenario. scenario

Assess how the effectiveness of the current backup system could be improved. (6)

Type your answer in the box.

Previous 27 / 27 Next 00:54 Pause Finish

Unit 3: Security Protection and Risk Management - Sample mark scheme

General Marking Guidance

- All learners must receive the same treatment. Examiners must mark the first learner in exactly the same way as they mark the last.
- Mark schemes should be applied positively. Learners must be rewarded for what they have shown they can do rather than penalised for omissions.
- Examiners should mark according to the mark scheme not according to their perception of where the grade boundaries may lie.
- All marks on the mark scheme should be used appropriately.
- All the marks on the mark scheme are designed to be awarded. Examiners should always award full marks if deserved, i.e. if the answer matches the mark scheme. Examiners should also be prepared to award zero marks if the learner's response is not worthy of credit according to the mark scheme.
- Where some judgment is required, mark schemes will provide the principles by which marks will be awarded and exemplification may be limited.
- When examiners are in doubt regarding the application of the mark scheme to a learner's response, the team leader must be consulted.
- Crossed out work should be marked UNLESS the learner has replaced it with an alternative response.

Specific Marking Guidance for Levels Based Mark Schemes*

Levels based mark schemes (LBMS) have been designed to assess learner work holistically. They consist of two parts: indicative content, and levels based descriptors. Indicative content reflects specific content-related points that a learner might make. Levels based descriptors articulate the skills that a learner is likely to demonstrate in relation to the Assessment Outcomes being targeted by the question. Different rows within the levels represent the progression of these skills.

When using a levels-based mark scheme, the 'best fit' approach should be used.

- Examiners should first make a holistic judgement on which band most closely matches the learner response and place it within that band. Learners will be placed in the band that best describes their answer.
- The mark awarded within the band will be decided based on the quality of the answer in response to the assessment focus/outcome and will be modified according to how securely all bullet points are displayed at that band.
- Marks will be awarded towards the top or bottom of that band depending on how they have evidenced each of the descriptor bullet points.

SECTION A

Question	Acceptable answer	Mark
1	Card entry Finger print	2
Question	**Acceptable answer**	**Mark**
2	Malware – Antivirus software Unauthorised access - Firewall	2
Question	**Acceptable answer**	**Mark**
3	Retina	1
Question	**Acceptable answer**	**Mark**
4	Award **one** mark for each of the following, up to a maximum of two marks. Responses must be in the correct order. 1 mark for 1 correct answer; 2 marks for all 3 correct answers. Password1 Pa55word wkjhopnb	2
Question	**Acceptable answer**	**Mark**
5	Make sure only you know your password Change your password regularly	2
Question	**Acceptable answer**	**Mark**
6	HTTPS Padlock	2
Question	**Acceptable answer**	**Mark**
7	Data should be fairly and lawfully obtained Data should only be used for its intended purpose	2
Question	**Acceptable answer**	**Mark**
8	Any **one** explanation that includes a consequence of visiting an untrusted website (1) and a linked justification of that consequence (1). • Their computer may get a virus (1) which would corrupt/delete/compromise data or computer system (1) • May give away personal data (1) which might lead to identity theft (1)	2
Question	**Acceptable answer**	**Mark**
9	Any **two** features from: • Generic to customer not named customer • Spelling errors/Incorrect grammar • Text speak • Immediate action Accept any other valid answers.	2
Question	**Acceptable answer**	**Mark**
10	Digital Signature	1
Question	**Acceptable answer**	**Mark**
11	It replicates itself from one device to another It hides itself from the user	2
Question	**Acceptable answer**	**Mark**
12	Any **one** explanation that includes a possible consequence of spyware	2

	infecting a computer (1) and a linked justification of that consequence (1). • Keystrokes could be recorded (1) which means that passwords are revealed/compromised(1) • Internet activity is tracked and stored (1) which means that personal information/user surfing habits can be accessed and shared (1)	
Question	**Acceptable answer**	**Mark**
13	To tell humans and computers apart	1
Question	**Acceptable answer**	**Mark**
14	Knowledge-based authentication	1
Question	**Acceptable answer**	**Mark**
15	Users should activate the screen lock	1
Question	**Acceptable answer**	**Mark**
16	Disaster recovery policy	1
Question	**Acceptable answer**	**Mark**
17	Any **two** explanations that include a factor which affects how frequently data needs to be backed up (1) and a linked justification of that factor (1). • How often the data changes/consequences of losing data (1) the frequency of backups should ensure that data is backed up often enough to recover vital data (1) • The amount of data involved (1) which affects when it can done without impacting on users(1) • Type of system being used (1) real time systems will need to be backed –up in real time (mirroring) (1)	4

SECTION B

Question	Acceptable answer	Mark
18	Award **one** mark for each of the following, up to a maximum of **three** marks • will allow other people to intercept the data being transmitted • theft of laptop • accidental damage to the laptop (coffee spill) • people physically seeing the data on the computer screen – shoulder surfing Accept any other reasonable answers	3
Question	**Acceptable answer**	**Mark**
19	Any **one** explanation that includes a precaution that Frankie could take to improve security when accessing the internet in Happyperc (1) and a linked justification of that precaution (1). • Use alternative methods of connection e.g. personal hotspots (1) which will secure the data/connection (1) • Don't access any websites that require login / other personal data/email (1) because unsecure data can be intercepted (1) Accept any other reasonable answers	2
Question	**Acceptable answer**	**Mark**
20	Any **two** explanations that includes a way encryption provides security for the Happyperc wireless network (1) and a linked justification of that way (1). • Encryption uses a key to make the data unreadable (1) those with the key can send and receive data securely (1) • Encryption restricts access to the network to those who have the key (1) preventing unauthorised access the network/wireless router (1) Accept any other reasonable answers	4

Scenario 2

Question	Acceptable answer	Mark
21	Award **one** mark for each of the following, up to a maximum of two marks • Read only (1) • Full access/read-write (1) • No access (1)	2
Question	**Acceptable answer**	**Mark**
22	Any **two** restrictions from: • Applications (1) • Folders/shared area (1) • Physical resources (1)	2
Question	**Acceptable answer**	**Mark**
23	Any **one** explanation that includes a reason why managers have different access levels to a LAN (1) and a linked justification of that reason (1). • Data stored on the LAN may be confidential e.g. financial information/payroll/personal information (1) and DPA imposes restrictions on who can see/use the data (1) • It is inappropriate for customer service staff to have unlimited access to data (1) as they could use the data for unauthorised/malicious purposes/accidentally deleted/amended (1)	2
Question	**Acceptable answer**	**Mark**
24	Any **two** explanations that includes a risk to Kernow Technologies of using a legacy operating system (1) and a linked justification of that risk to Kernow Technologies(1). • Legacy systems are no longer centrally supported by the vendor (1) therefore security updates are not available making Kernow's data more vulnerable to external attacks (1) • Vulnerabilities are no longer fixed by the provider/vendor (1) which means that the Kernow would have to pay a third party (extra cost to company) to secure their operating system/which means that patches and updates are not being provided leaving Kernow's systems open to external attacks (1) • Hackers are continually looking for vulnerabilities in older systems (1) therefore there is increased risks of external attack to Kernow's system and data/ access to data and company information(data not protected)(1)	4

Scenario 3		
Question	**Acceptable answer**	**Mark**
25	Any **two** disadvantages from: Many people have physical access (1) Could be accidentally turned off (1) Malicious damage from a disgruntled employee Increase risk of physical damage (1)	2
Question	**Acceptable answer**	**Mark**
26	Any **one** explanation that includes a risk to company data of using portable media (1) plus **two** linked justifications of that risk (1) + (1). ● Portable storage devices are small which means increased risk of theft/loss (1) which means that the data is no longer secure/gets into the wrong hands (1) which could result in breach of confidentiality between company and customer/employees (1) ● Portable storage devices could spread viruses from one computer to another (1) which means the computer systems could be compromised (1) which could result in loss/corruption of more data (1)	3
Question	**Indicative content**	
27	The indicative content is not exhaustive/prescriptive and learners should be credited for other relevant content. backup procedures: ● selection of data o Some data is saved locally/portable data which means it can't be part of central backup o All employees should be instructed to store data centrally o System should be set up to stop employees using local hard drive or external storage devices ● Timing o should take place when the system is not in use to ensure that all data is backed up and there is no impact on users ● Frequency o currently monthly which is ineffective and needs to be done more frequently e.g. every day for user flies, weekly for system files ● Media o Employees currently use portable media which increase the risk of loss o File server would need a system capable of storing sufficient data o File server would need a backup devise capable of holding sufficient data ● Planned, automated and manual o currently being done manually (could forget to backup system) and should ideally be done automatically	6

	• Type (full, differential and incremental) o the system would need to be set up for example full back up done weekly and differential backup done daily • on-site, off-site and cloud data storage o current back up is kept on site.	

Level	**Mark**	
	0	No rewardable material
Level 1	1-2 marks	• Demonstrates isolated knowledge and understanding of relevant information; there may be major gaps or omissions • Judgements on significance may be presented, but are likely to be generic assertions rather than supported by evidence • Meaning may be conveyed but in a non-specialist way; response lacks clarity and fails to provide an adequate answer to the question.
Level 2	3-4 marks	• Demonstrates accurate knowledge and understanding of relevant information with a few omissions • Assessment is presented leading to judgements on significance but some may be lacking support. • Demonstrates the use of logical reasoning, clarity, and appropriate specialist technical language
Level 3	5-6 marks	• Demonstrates accurate and thorough knowledge and understanding of relevant information; Any gaps or omissions are minor • Displays a well-developed and balanced assessment leading to rationalised judgements on significance. • Demonstrates the use of logical reasoning, clarity, and appropriate specialist technical language.