BTEC DIT

Component 3 Effective Digital practices

Learning Aim B: Prevention and management of threats to data

Knowledge and Assessment Organiser

Student name: .....

How can we prevent threats to data?

Contents

Key terms

Exam question command words

Command verbs	Definition
Describe	To give an account of something, such as steps in a process or characteristics of something. The response should be developed as they are often linked, but do not need to include a justification or reason.
Discuss	Identify the issue/situation/problem/argument that is being assessed in the question. Explore all aspects of an issue/situation/problem/argument etc. by reasoning or argument.
Draw	Produce an annotated process either in the form of an information flow or data flow diagram
Evaluate	Review information then bring it together to form a conclusion, drawing on evidence, including strengths, weaknesses, alternative actions, relevant data or information. Come to a supported judgement of a subject's qualities and relation to its context.
Explain	An explanation that requires a justification/exemplification of a point. The answer must contain some element of reasoning/justification.
Give/State/Name	Require recall of one or more pieces of information.
Identify	Usually requires some key information to be selected from a given stimulus/resource.
Annotate the diagram to explain how ...	Label the diagram and provide an explanation for each identification.
Assess	Give careful consideration to all the factors or events that apply and identify which are the most important or relevant. Make a judgement on the importance of something, and come to a conclusion where needed.

How can we prevent threats to data?

Small Question

How can we restrict user access to data?

Small Question

What is back-up and encryption?

Small Question

How do we find weaknesses in a system?

Essential knowledge & tasks

Key terms

Swipe card – is a plastic credit card sized device, often with a metallic strip that contains information that is scanned by a sensor to verify their user's identity and access to a secured location.

Protecting data on a computer system

Key terms

Local Area Network(LAN) – is a network based on geographical location, such as an office or school. This is usually in one building or a cluster of building close together.

Access Control List (ACL)- is a list that tells the network which data can be sent and received.

Shoulder surfing – is obtaining sensitive personal information from a user by literally looking over their shoulder while they use digital devices such as computers, cash –dispensing machines etc.

Session cookies – are data stored by the web browser until it is closed.

Worms – are small computer programs that can spread to other programs.

Trojans – are types of malware disguised as legitimate programs.

Rootkit – is a collection of tools or programs that allow an unauthorised user to obtain undetected control of a computer system.

Spyware – is software that is installed on a device without the user's knowledge. It can gather information about their computer activities by transmitting data secretly from their hard drive.

Vulnerable – describes a weakness in the design implementation or configuration of a system. Known vulnerabilities can be exploited by 'black hats' to attack a digital system.

How can we restrict user access to data?

Physical security measures

This is securing a system's data from threats through preventing physical access to the IT systems. Commonly this can be performed through:

- **Locks** – Either electric or key-operated and requiring a unique combination (e.g. passcode) or item (e.g. key or swipe card) to bypass. These can be on doors to access rooms, locks on cabinets containing devices, or locks on devices themselves.
- **Surveillance** – A method of observing a physical space through digital, live recording, often fed back to a secure location for review. For example, CCTV cameras.

Pros	Cons
Can deter attackers by visually seeing the prevention methods.	Can be very expensive to initially install. It can require quite a bit of specialist equipment.
Prevents access to actual physical locations containing data & the theft of these devices.	Internal threats will be able to bypass physical security measures very easily in many cases.

Security technique	Benefits	Drawbacks
Electronic swipe lock	• Prevents access to digital system. • Traditional key or electronic lock requiring PIN or swipe card.	Both keys and card can be lost or stolen or copied.
Secured Device	• Uses steel cable and lock to secure mobile devices to heavy furniture. • Makes theft of devices very difficult.	You have to use your device in a stationary position once you've secured it to an object.
CCTV camera	• Acts a as deterrent but also records potential threats. • Can be controlled through an organisation network.	Having CCTV will not actually stop data being stolen, but it may help investigators identify those who stole it.

Levels of access

This involves separating logged in individuals into user-groups, with each group being assigned specific permissions for accessing files and software, as well as what functions they can perform.

For example, in most organisations only IT admin staff can install software, regular users cannot. This helps prevent the spread of malware.

It's important that users are assigned the correct settings. Businesses should work to the "principle of least privilege". This means that users can only access and do exactly what they need to perform their job role.

Pros	Cons
Reduces the impact of a security breach, as the access will be restricted to certain files & features.	Doesn't actually prevent access to data, only limits the damage that can be caused during an incident.
Reduces the likelihood of occurring and damage caused by human error.	May restrict the user's ability to do their job by limiting their access to files & features.

Authentication

When someone wants to gain access to a user's account on an IT system, it is important that we have some method of authenticating that they are in fact the person they claim to be.

There are a number of methods of doing this.

Passwords

A secret string of characters used to secure and control access to a company's system. This is the most common method of ensuring only authorised users can view system content.

Password complexity is important in ensuring this is an effective security method. Good passwords should:

- Be a minimum of 8 characters.
- Contain uppercase & lowercase letters, numbers & symbols.
- Not be reused on multiple different systems.
- Not contain dictionary words or names (preferably it should be a random mix of characters).

Pros	Cons
Actually prevents access to user accounts on computer systems, rather than just limiting impact.	Relies on the end user setting their password with a good level of complexity & not revealing it to others.
Simple and easy to set up for both the system admin and the user. Also cheap to setup.	It can be hard to remember a variety of different complex passwords.

Password cracking

Dictionary attacks

A program attempts passwords using words in a dictionary. This will likely include common words or passphrases

Brute-force

A program attempts to try changing each letter in turn until it finds the password. Longer passwords make this take more time

Guesswork

By knowing personal information about someone, it is possible for a human to guess the password. This uses social engineering, such as finding out where someone is going on holiday, to help crack a password

Biometrics

A method of verifying the identity of a user through the use of unique physical characteristics. Retina (eye) scans, fingerprint identification, voice analysis and facial recognition are a few examples of common biometrics.

This can be used as a method of authenticating access to a computer system. For example, you'll commonly see fingerprint id on smartphones. However, it can also be used as part of physical access security in place of keys & swipe cards.

Pros	Cons
Can save time, as users do not have to remember and enter a security string.	Can be expensive to initially purchase and install due to its speciality.
Users have accountability for their actions, as a physical trait cannot be stolen.	Physical traits are not changeable, so if compromised in a breach, they cannot be reset.

Two- factor authentication

A form of authentication used to reduce the vulnerabilities of standard passwords by adding a second authentication challenge.

After entering a password, a user may be expected to use a biometric scanner, a unique one-time code or perhaps a security token or swipe card.

Pros	Cons
Much more secure, as two different methods of authentication would need to be compromised to gain access to a system.	Logging into a system may take a lot longer which will be frustrating and affecting productivity of employees.
Still very cheap to implement as the 2nd-factor authentication can rely on existing systems, like email or employee smartphones.	If you don't have access to the second authentication method (e.g. your smartphone) then you can't log in.

Task 1

The following table contains six scenarios. Tick which factor(s) of authentication are being used. The first one has been completed for you.

Scenario	Something you are	Something you know	Something you have
A school needs to make changes to student accounts in the canteen. They authenticate the student for payment by use of a fingerprint scanner.	✓		
When setting up a bank account at a modern bank, they take a photo of you and ask you to enter a four-digit Personal Identification Number (PIN). In order to withdraw cash at the counter, they can check the photo of the customer and then ask for their PIN and card.			
In order to carry out online banking a password and user ID is first needed. If a user wants to send money to another person, they will be sent a verification number to their mobile phone which they must then enter into the website.			
A social network site requires users to log in with a username and password. If a user has lost their password then it asks a security question in order to reset the password.			
Inland Revenue are responsible for collecting tax from people and businesses. When a user tries to log in using their ID number and password, the website will phone the user's registered telephone number with a security code. This must then be entered into the system to log in.			
A mobile phone makes use of a fingerprint scanner to allow people to log into the phone. The same fingerprint scanner can then be used to authenticate payments from the phone.			

Anti-virus software

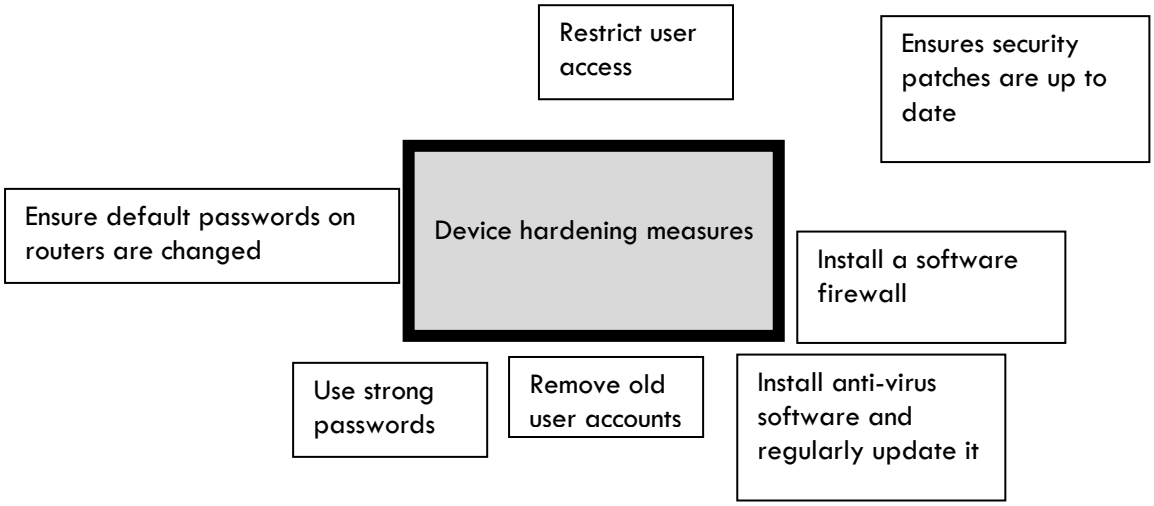
Anti-Virus software is a piece of software used to scan for and remove malware (viruses, worms, trojans, spyware, rootkits, etc.) from a computer, server, or mobile device.

Anti-virus also often has a real-time protection feature which scans all data coming into a system and all files and folders as they are executed. This helps prevent malware from ever infecting your system.

Anti-viruses usually use virus signatures (a unique data pattern to each virus) to detect malicious programs, which are subsequently removed. This is known as "signature detection". It can also use "heuristic detection" which monitors the behaviour of your computer and spots anything that is behaving like a virus.

Pros	Cons
Prevents all forms of malware from ever infecting your computer system.	It must be regularly maintained and updated. Otherwise it won't detect some malware.
Usually reasonably affordable and relatively simple to set up.	Running a scan can be resource intensive and lead to your computer running slowly.

Device hardening



Benefits and drawbacks

- ✓ Protects a system from a range of attacks.
- ☒ Requires technical staff to stay up to date with the latest security threats to ensure device hardening remains effective.
- ☒ Technical skills are required to apply device hardening.

Interface design

Software interface design is usually based around assisting user accessibility and ease-of-use. However, it is sometimes given additional features to enhance security. Some of these features include:

- **Obscuring data entry** – Reduces shoulder surfing or accidental password sharing by replacing sensitive data entry with a special character (often a * or •).
- **Autocomplete** – Completes user data entry automatically (such as choosing from a list) rather than typing it in. This can prevent spyware keylogging your password, but generally is a security threat as attackers won't need to know your details as the system will enter for you.
- **"Stay logged in"** – Allows users to remain logged in, even after leaving the site. This can also prevent spyware keylogging your password, but could allow anyone who has access to your computer to access your systems as they'll be already logged in.

Pros	Cons
Good design can reduce the need for overly stringent security measures.	Focusing on security may sometimes worsen ease-of-use & accessibility.

Firewalls

Firewalls monitor incoming and outgoing network traffic and blocks suspicious packets based on a set of security rules.

A firewall can be a hardware device installed between external and internal networks to protect against external cyber threats or viruses. Most commonly this would be between the Internet and the businesses' LAN.

It can also be a software program installed on a computer. This performs the same packet filtering as a hardware firewall but protecting individual devices rather than the whole network. However, it also has additional features such as filtering network traffic to and from software applications.

Most businesses will use both a hardware firewall and software firewalls installed on each individual device.

Pros	Cons
Prevents external attackers from gaining access to your computer system by blocking their attempts.	Firewalls can be restrictive, preventing employees from performing legitimate activities, like visiting certain websites.
Usually very cheap to install and set up software firewalls. Most operating systems come with them built-in.	Software firewalls take up resources and slow computer & network performance. Hardware firewalls could slow internet speed.

Thinking point

Firewalls can be used by some businesses to block you visiting certain websites. Why do you think they do this?

Security patches

Are additional settings or program codes that fix vulnerabilities in applications, operating systems and device firmware, and are usually downloaded from the manufacturer.

Task 2

Gisela has just changed her Internet provider. The new provider has sent her a new Wi-Fi router. She is currently going through the setup of the router and has been asked if she would like to enable the inbuilt firewall.

(a) The table below gives a list of potential benefits, drawbacks and functions. Tick those which a firewall will give her.

Benefit or function	The firewall may be able to provide this (✓)
Block certain programs from accessing certain ports on the network	
Reduce the chance of an attacker gaining access to the home network	
Fire packets of information to malicious computers	
Report suspicious packets of data to the police	
Speed up the network / access to the internet	
Inspect packets so that those that look suspicious are dropped / rejected	
Create a wall around the network so that only information that comes from computers with the network password will be introduced to the network	
Prevent computers with certain IP addresses from accessing the network	

Exam question

A food and grocery retailer has stores located around the country. It also has a website where customers can view details of products and purchase them online.

The retailer is considering the following measures to minimise threats to data.

Option 1: locking all doors into rooms containing computer devices.

Option 2: facial recognition software to unlock all computer devices.

Option 3: two -factor authentication using individual user's smartphone.

Evaluate the impact of each method on digital security. Which method would have the greatest impact?

(9 marks)

Hint!

To evaluate you need to consider the benefits and drawbacks of each method, then make a judgement as to which method will improve security most.

Hint!

Make sure you give reasons for all your points. For example, why does option 1 have drawbacks? Why have you chosen one method as being more secure than others?

Always give a conclusion!

Hint!

Remember to give your answer in the context of the question. For example, discuss how locking doors could make it harder for a visitor to head office gain access to a computer even if they knew a workers username and password.

What is Back up & Encryption?

During the last lesson, we saw several methods of data level protection. This can be referred to as "Device Hardening". Making the system secure by reducing the vulnerabilities of the system that could be exploited.

Backup and recovery, along with encryption are two more important methods of device hardening.

Backup & Recovery

In any kind of computer system, it is critical to back up data. This way if data is lost, such as from cyber-attack, physical threats, and human error, then we can recover this lost data and protect ourselves from harm.

Backups aren't something you make once and forget though. You should take regular backups. How regular depends on your business, as for some a weekly backup is fine, as they don't do much business on a daily basis. Some might need hourly backups though. Generally, daily backups are common.

Backups should also be stored in a remote location. This means they're stored somewhere other than where the original data is. This way, if your building burned down or flooded, your backup won't be affected. It is quite common to use cloud storage for remote backups.

Pros	Cons
Prevents losing critical data from a range of possible risks.	Can be extremely costly to implement backups with lots of data.
Well managed backups reduces the potential maximum downtime of a system following an incident.	Large backups will take considerable resources to make and your computer performance may be very slow during it.

Encryption

This is the process of converting plain-text data into an encoded form known as ciphertext. This ciphertext is unreadable until it is decrypted.

We encrypt data using an encryption **algorithm** and an encryption **key**. The algorithm is the process performed to convert the data into the ciphertext. The key is a unique string that is applied to the algorithm to ensure the encryption output is unique (so someone using the same algorithm but a different key will get different ciphertext output).

We most commonly think of encryption when we are transmitting data, such as when we send our bank details to an online shopping website over the internet. However, we sometimes encrypt stored data too.

- **Stored data** – We can encrypt individual files or an entire drive. This way we would only be able to view the data if we have the decryption key. This way, even if a device is stolen you will still be sure the data is safe. Websites that store passwords of their users will encrypt the passwords, so even if their database is hacked into, user's passwords will still be safe.
- **Transmitted data** – When transmitting files over the internet they can be intercepted by malicious users and read. This is why we encrypt transmitted data, as if it is stolen during transmission, they'll only

receive the ciphertext, which they can't understand. Websites that have HTTPS in the title are using SSL encryption, so you know the data going between your computer & the server is secure.

Pros	Cons
Ensures data is safe even when being transmitted over a public network like the internet.	If you lose the decryption key then you'll never be able to decrypt your data and view it.

Task 1

A file contains the following text which has been encrypted using a very simple algorithm.

uif wbmvf pg bdijfwfnfou mjft jo uif bdijfwjoh. – bmcfsu fjotufjo

(a) Work with a partner to decrypt the algorithm.

The algorithm used is a Caesar cipher. Each letter is one letter further in the alphabet. E.g. a becomes b, b become c,… z becomes a. To decrypt just move each letter to the previous letter in the alphabet.

u	i	f		w	b	m	v	f	
p	g		b	d	i	j	f	w	f
n	f	o	u		m	j	f	t	
j	o		u	i	f		b	d	i
j	f	w	j	o	h	.		-	
b	m	c	f	s	u		f	j	o
t	u	f	j	o					

What does encryption mean?

(c) A user wishes to encrypt an external hard disk so that if it is stolen the data still cannot be accessed. How could the user achieve this?

Exam question

A company designs and makes greetings cards which it sells through its high street shops.

The company stores its data in files on its digital systems at head office. The data in each files in encrypted.

Explain one way that data encryption increases the security of data stored in files.

[2 marks]

How do we find weaknesses in a system?

White hat/grey hat hacking

White hat hackers are requested by companies to try to find weaknesses in systems to improve security
They find weaknesses and improve system security by:

- Ethical hacking
- Penetration testing

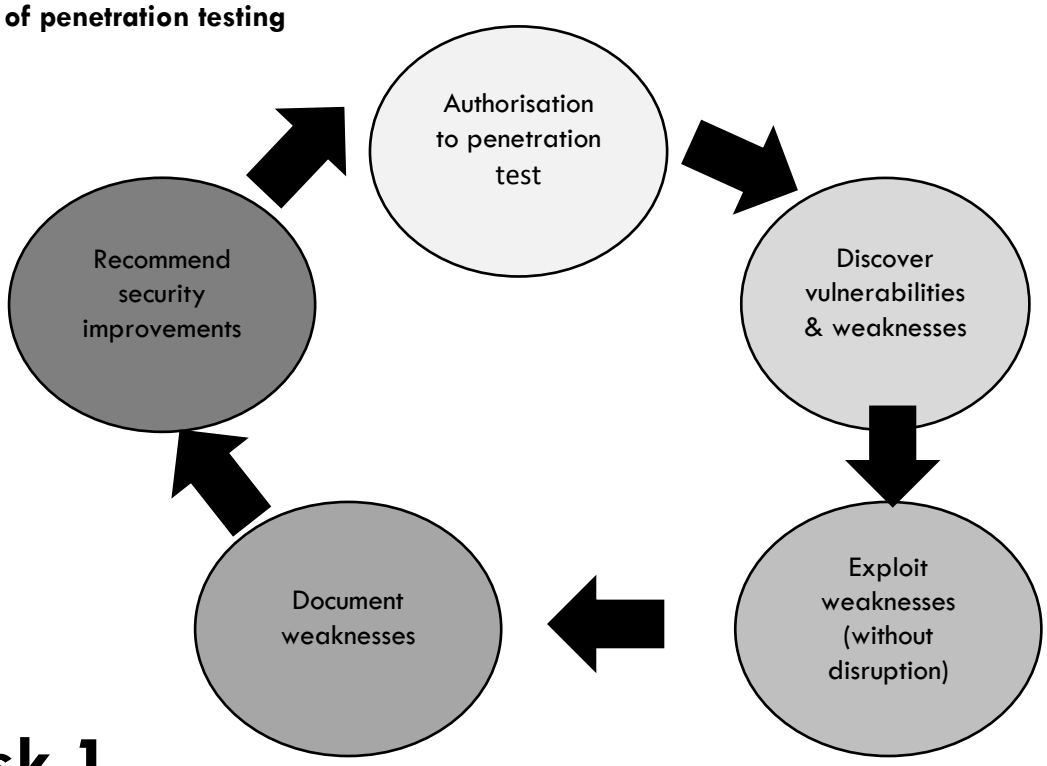
Grey-hat hacking – An individual who finds and reports an exploit/vulnerability they have found in a system or application but has not been explicitly asked to do so by its owner.

Penetration testing

- Process used by cybersecurity professionals in order to identify security vulnerabilities in a computer system. This can involve techniques like port scanning, vulnerability scanners & packet sniffers to identify weak points such as open network ports, coding flaws, out of date software & missing encryption.
- **Analysis of system data/behaviours –** The process of observing a system's data and its users' actions in order to assess whether the data is being held securely and whether it can be accessed in some way. This might identify a weakness, such as users taking confidential data out of the business to work at home.

Pros	Cons
Gives you confidence that the security measures you have in place are effective in protecting your data.	It can be a very expensive and time consuming process to perform. Especially in large businesses.

Stages of penetration testing



Task 1

Highlight the benefits of PENTRATION TESTING using your GREEN highlighter.

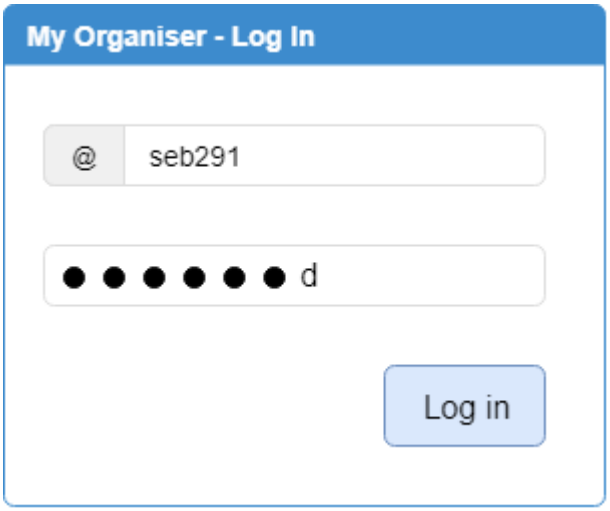
- Testing uses the actual methods that an attacker might use so it gives a realistic idea of how well the system is protected.
- Vulnerabilities spotted can be fixed to improve data security.
- Just because one hacker could not gain access to the system does not mean other hackers would not be able to gain access.
- It is expensive to carryout penetration testing.
- New security vulnerabilities and cyberattacks are being discovered penetration testing needs to be carried out regularly.

Explain the difference between a **white hat hacker** and a **grey hat hacker.**

Task 2

Link Builder Marketing specialise in building software which can help boost company rankings in search engines. The employees use an app for organising their to do lists and schedules.

When they enter their password, the letter is first shown briefly so the user can see they have entered the correct letter. The letter then changes to a dot.



(a) Explain **one** reason this helps keep the system secure.

(b) Explain **one** way that entering passwords could be made more secure.

(c) What additional security feature could help to protect this system?

Task 3

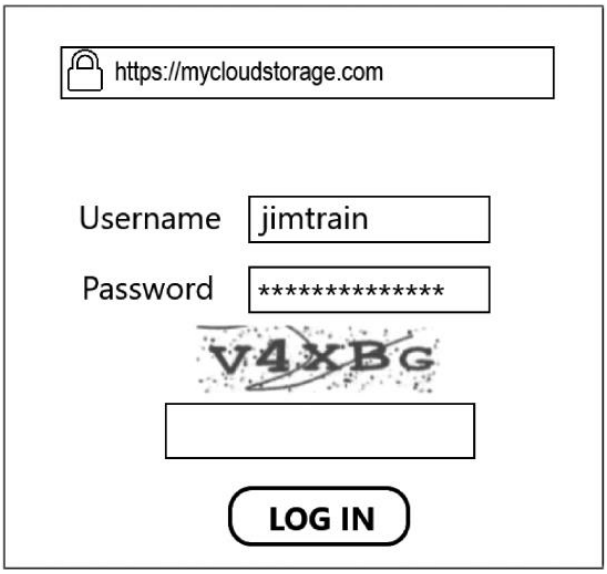
A central – heating engineer receives details of his daily appointments on the company's laptop. He also accesses the company's systems via an internet browser to update his progress, diagnose problems and order spare parts. The browser has an autocomplete facility so that engineer does not have to log in to the system each time.

Describe ONE advantage and ONE disadvantage of autocomplete.

Exam question

Jim has his own personal training business. To access his cloud storage area Jim logs in using his unique username and password. Annotate the image to explain **two** ways the login page keeps his details secure when logging in.

(4)



B2: Exam Questions (Independent study materials)

A retailer is considering the following measures to minimise threats to data.

- Option 1 – locking all doors into rooms containing computer devices.
- Option 2 – facial recognition software to unlock all computer devices.
- Option 3 – Two- factor authentication using individual user's smartphone.

Evaluate the impact of each method on digital security. Which method would have the greatest impact?

The following example has some good bits but is far from being great. Why?

***Answer*:**

Identified possible benefits of option 1.

Only people with keys or swipe cards can unlock doors to gain access.

Identified possible drawbacks of option 1.

Relies on all users unlocking and locking doors

Identified possible benefits of option 2.

Only authorised people with recognised faces are allowed access into the system.

Identified possible benefits of option 3.

Uses two factors which is more secure than just a password.

Hint

Evaluate – question requires you to review information, by considering the evidence – including strengths, weaknesses and alternative approaches and then to reach a supported judgement of a particular aspect in a given context.

Hint

Evaluate – to evaluate you need to consider the benefits and drawbacks of each method, then make a judgement as to which method will improve security the most.

Make sure you give reasons for your points. For example: Why does option 1 have drawbacks? Why have you chosen one method as being more secure than the others?

Level	Mark	
	0	No rewardable material
1	1-3	• Demonstrates isolated elements of knowledge and understanding, with major gaps or omissions • Few of the points made will be relevant to the context in the question • Limited evaluation which contains generic assertions leading to a conclusion that is superficial or unsupported
2	4-6	• Demonstrates some accurate knowledge and understanding, with few minor omissions • Some of the points made will be relevant to the context in the question, but the link will not always be clear • Displays a partially developed evaluation that considers some different competing points, although not always in detail, leading to a conclusion which is partially supported
3	7-9	• Demonstrates mostly accurate and thorough/detailed knowledge and understanding • Most of the points made will be relevant to the context in the question, and there will be clear links • Displays a well-developed and logical evaluation that clearly considers different aspects and competing points in detail, leading to a conclusion that is fully supported

Q1.

Clare is a designer for a games development company.

She works from home and in public places such as cafés, train stations and airports.

Clare uses her laptop to prepare designs.

Clare has recently been a victim of phishing.

Describe **one** way that this could have happened.

(2)

.....

.....

.....

.....

Q2.

TechnoWhizz is a technology development company based in London that makes a range of digital systems, devices and apps.

They are considering using ethical hackers to help protect their systems, devices and apps.

Hackers are categorised using a range of hat colours.

Explain **one** benefit of using a white hat hacker.

(2)

.....

.....

.....

Q3

Chocawoca is a confectionary manufacturer that makes high quality sweets and chocolates that they sell in their shops and online.

At present, staff who work at Chocawoca use a card entry system to gain access to their secret recipe rooms, cards are swiped at the entrance. They are considering changing this to use a biometric system as they think this will improve security.

Explain **two** benefits of biometric systems to Chocawoca.

(4)

1 .....

.....

.....

.....

2 .....

.....

.....

.....

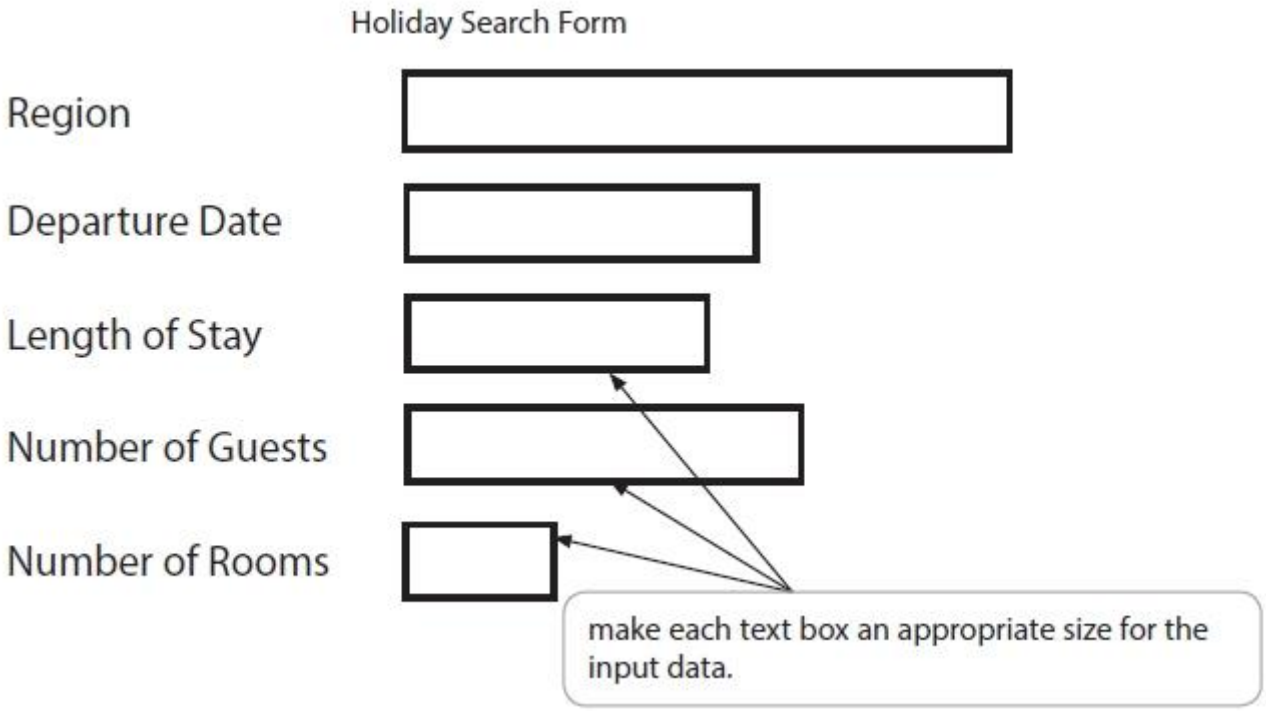
Q4

A local travel agency sells holidays through high street shops and online.

The travel agency has produced a form to allow customers to search for holidays.

Annotate the form to show **four** improvements that could be made to make it more user friendly and effective. An example has been provided.

(4)



Mark scheme

Q1

Question Number	Answer	Additional Guidance	Mark
	A description to contain **two** from: • Clare received an email which asked for personal details • Clare clicked on a link in an email she received • Then she provided her personal information. Accept any other appropriate response	Accept any other form of phishing e.g. social media posts, telephone and text message.	2

Q2

Question Number	Answer	Additional Guidance	Mark
	Any **one** benefit such as: • The white hat hacker will stay within the law whilst hacking systems (1) which will ensure the company is acting lawfully (1) • The white hat hacker will not violate ethical or moral boundaries (1) which will not result in the reputation of the company being damaged (1) • TechnoWhizz will be able to oversee the white hat hackers activities (1) giving them greater control over which systems are being tested (1) Accept any other appropriate response	• Award one mark for a benefit and one mark for a linked explanation of that benefit justification and benefit may be reversed.	2

Q3

Question Number	Answer	Additional Guidance	Mark
	Award **one** mark for each identified biometric method (to a maximum of two marks) and for correctly identifying an advantage (1) • Retinal scanning (1), there is no known way to replicate a retina(1) • Iris recognition (1), verification time is quick (1) • Hand geometry (1), the amount of data required to uniquely identify a user in a system is the smallest (1) Accept any other appropriate response	• Award one mark for an identification and one mark for a linked justification identification and benefit may be reversed.	4

Q4

Question Number	Answer	Additional Guidance	Mark
	Any **four** from: • Larger font for the title • Calendar for the date • Length of stay/Number of guests/Number of rooms to include a dropdown/spinner • Help/Instructions • Search option • Navigation • Accessibility Options/Features Accept any other appropriate response	Accept alternative / appropriate wording	4

Articles for Wider Reading and Flipped Learning

Subscribe and watch the YouTube clip on Cyber security.

https://www.youtube.com/watch?v=jGBdmHvNXfs&list=PLmyUnKEeJk-6gijRiVKEfcvZhwcj6LWpo&index=5

(ADD QR CODE FOR ANY LINKS)

Prevention and management of threats - Know it all Ninja

Read through the topics on **prevention and management of threats.** Remember to complete the on-line quiz to gain house points!

https://www.knowitallninja.com/modules/prevention-management-of-threats/