System Security

Forms of Attack

ACTIVE
Using software (i.e. virus) or other technical methods to gain access.

PASSIVE
Spying on a system to identify vulnerabilities.

SOCIAL ENGINEERING
A person is tricked into giving away information that gives others access.

INSIDER
An employee, former employee, contractor or business associate that has access to the system may steal sensitive information or give away access details to others.

PASSWORDS

One of the most common ways that a cyber-criminal can gain entry to a computer system if the user does not have an adequate password or does not keep the password secret.

Removable Media

There are two threats with removable media:

- The removable media getting into the wrong hands
- The removable media getting infected with malware

Software Patches

Software patches fix known security problems in software but also notify cyber-criminals that there was a problem so anybody NOT uploading the latest patch is vulnerable

Penetration Testing

White-box penetration	Black-box penetration
This simulates a potential attack from INSIDE the organisation and includes some basic knowledge of the target system such as the software used. This simulates a threat from an employee or somebody who was sacked by the company and holds a grudge.	This simulates an EXTERNAL attack such as illegally gaining access to a computer system or cyber warfare and is a more realistic test as most crackers will not have the inside knowledge that a white-box penetration test assumes.

Network forensics is a specialist area that involves monitoring and examining data to discover the source of security attacks and other illegal activities.

When a cyber-criminal inputs SQL code into an online form to side-step the need to enter a valid user ID or password it is known as **SQL injection**.

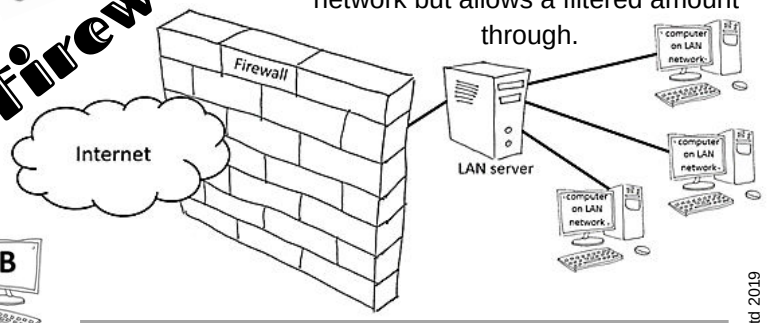
Malware is a term used to describe a variety of hostile or intrusive software.

A **brute force attack** is a method used to obtain information such as a user password or personal identification number (PIN) through trial-and-error.

Phishing is when a criminal sends an email or text message pretending to be from a bank or official account to ask for personal information.

Firewalls

A firewall is not really a physical wall; it is a filter between a network and the internet. It does not stop everything from entering the network but allows a filtered amount through.



Denial of Service (DoS) attacks are when the cyber-criminal sends loads of messages flooding the targeted server with messages to overload the system and stop legitimate customers and users from accessing the server.

Data inception is when the cyber-criminal spies on the network traffic and gathers the information they need or alters information as it moves around the system.

Access rights define who has permission to access data on the computer system.

A **network policy** should include rules for: generating passwords, user access levels, responsibility of training, use of removable media, firewall settings, installing and updating anti-malware software and software patches and details of penetration testing.

ENCRYPTION

A method of altering the original message using a secret code that only the authorised computers on the network know. When a website has the address **https** rather than **http** it shows that any data the user inputs on that website (i.e. payment or personal details) will be encrypted and unreadable for anyone listening in.

System Security

Revise it

Read through the handout and then select a revision technique from those described in this section, you can even do more than one if you want!

Highlight

Highlight key words (maximum of 2 per sentence) and then cover the page and try to write down all the key words you can remember. Go back and fill in all the ones you have missed.

Mind map

Using the handout, draw a mind map and include as many colours, images and diagrams as you can to illustrate it

Bullet Points

Write the main headings (leaving space between each) and then write bullet points of the main key points you need to remember under each heading. Re-read the handout and add any missed points to your list.

Post-it notes

Write a key word and the definition on a post-it note and stick them around your study area as a reminder of the terminology.

Record your notes

Re-write the handout in your own words and record yourself using your phone as you read your notes aloud.

TEST YOURSELF

Cover your notes and the answer before you attempt to answer this practice exam question.

Discuss how a network policy can benefit a company. *[8 marks]*

Mark your answer

For two or three brief points with very little explanation award 1 - 2 marks. For three to five detailed points covering at least two of the suggested bullet points below award 3 - 5 marks. For six or more detailed points that form a well-written, balanced discussion covering all of the suggested bullet points below award 6 - 8 marks.

- A firewall would prevent harmful malware from entering the network.
- Training of employees could prevent social engineering.
- Using different user levels can limit the dangers from outside attacks.
- Encrypting data could prevent data from being intercepted.
- Using strong passwords can prevent brute force attacks.
- Regular penetration tests allows weaknesses in the network to be discovered and fixed.
- Updating and patching software stops cyber-criminal gaining entry through week areas.