



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.

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.

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.

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.

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



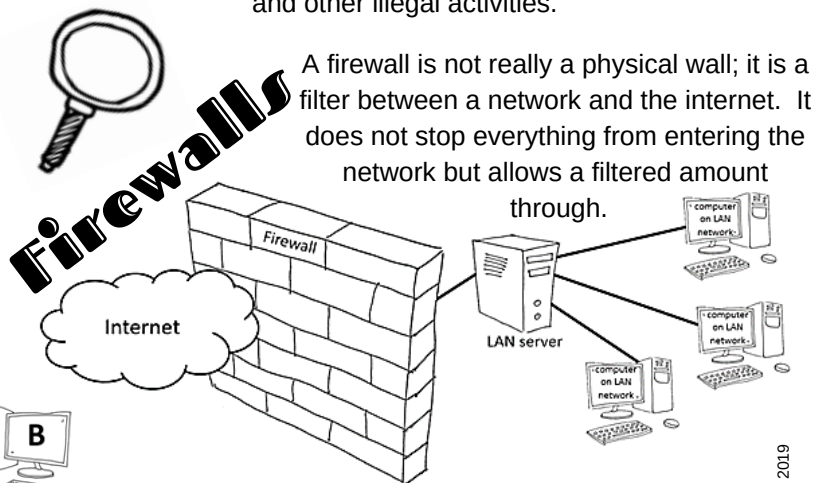
Software Patches

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.



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.

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

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.

