Network Security

You'll do more work on cyber security in unit 6.

Networks are more vulnerable to attack by hackers, viruses, malware and other attacks than a standalone machine. This is simply because all an attacker needs to do is access any machine on the network in order to gain access to every other machine.

If an attacker accessed a network they could:

- steal data
- corrupt or delete data used by the organisation
- flood the network with traffic in a denial of service attack
- install malware on other machines on the network

For example, on a school network students should not have access to data that staff might need access to and very few staff should have access to servers.

Network security is used to prevent unauthorised access to data. In other words, to keep people who shouldn't be on the network out and to allow people who should be on the network in – but only to the parts of the network they are supposed to access.

This is done in 4 ways:

1. authentication
2. encryption
3. firewalls
4. MAC address filtering

Authentication

Authentication is checking (authenticating) who a user is and which parts of a network they should be allowed access to.

This is most commonly done using usernames and passwords, although more complex methods can be used such as fingerprint or iris recognition.

Locking an account after a set number of attempts to access it is a way to restrict brute-force attacks to gain access to a network.

Password security is an important part of this process and will usually involve requiring a level of complexity and length of passwords and often for passwords to be changed on a regular basis.

Encryption

When you encrypt data you make it unreadable to someone who shouldn't have access to it.

Encryption is used so that if a hacker gains access to data they won't be able to read it. There are various encryption methods used on networks, some of which are very complex and are virtually impossible to hack.

Obvious places to use encrypted data are online banking systems or NHS health records. These would use the HTTPS protocol when accessing them.

Firewall

A firewall is a network security device (usually operated using a piece of software) which sits between a network and the outside world, typically the internet. It aims to restrict access to the network by unwanted traffic.

The firewall monitors both incoming and outgoing network traffic and decides whether to allow or to block specific traffic based on a set of security rules.

Unauthorised users can be blocked from accessing the network by the firewall. It can also be used to block attempts to gain access to certain network ports used for FTP processes. These can be vulnerable to exploitation by hackers. It is important to monitor outgoing traffic as well. This prevents malware such as viruses, trojans or spyware sending data from the network to someone else.

Firewalls will also help restrict attempts to slow down the speed of a network using a **denial of service attack**.

FTP is File Transfer Protocol. It is used for transferring data across a network.

Types of malware are dealt with in Unit 6.

MAC address filtering

A MAC address is a unique address for every computer that never changes. The MAC address is encoded in the network interface card (NIC) within a machine and is used by Ethernet, Wi-Fi and Bluetooth. It is a 48-bit number.

MAC address filtering can be used on a network by only allowing known devices to access it. This will stop attempts from other machines to gain access to the network at all.

Although MAC address filtering can be very useful, the problem with it is that you don't necessarily know who is using the specific device. At that point, authentication comes into play.

MAC addresses never change, whereas the IP address assigned to an individual machine does change and can be hidden or manipulated using methods such as VPNs.

Activity 1:

a) Write down a definition of network security
b) Explain the purposes of network security (what it is trying to stop happening)
c) Make notes on the 4 methods of network security. You might want to use a table to do this
d) Find out what a denial of service attack is and explain how a firewall can help prevent them from happening (this is quite a complex topic and you may enjoy reading some more about DoS and DDoS attacks and their history)

Activity 2:

Obidos Travel have a simple wired network involving 7 machines as well as peripheries such as a printer and scanner.

a) Explain how Obidos Travel could use all four of the network security methods to make their system secure.
b) What password security rules should Obidos Travel put in place?