Cyber Security – the fundamentals

Cyber security consists of the:

processes, practices and technologies

designed to

protect networks, computers and data

from

attack, damage or unauthorised access

That means that cyber security is the things people do to protect computers from damage and attack. That could be a technological attack such as a virus or spyware, or a user removing personal data from a system, or a physical attack on a computer system or network.

Modern computer systems are incredibly important to our way of life. Keeping them safe and secure is a major issue

Cyber Security Threats

There are seven main cyber security threats you need to know about.

1. Social engineering – we'll come back to this later in the unit
2. Malicious code – again, we'll come back to this
3. Pharming
4. Weak and default passwords
5. Removable media
6. Misconfigured access rights
7. Unpatched and/or out-dated software

3. Pharming:

Pharming is a cyber attack intended to redirect a website's traffic to a fake website. Any username, password or other details entered there can be harvested by criminals.

Major UK banks such as Barclays, NatWest, Lloyds and HSBC have all been targets for pharming attacks

4. Weak and default passwords:

Passwords that are easy to guess are an obvious security risk. The default passwords for voice mail or for hardware such as routers are well known to hackers and must be changed – but often aren't.

A **default password** is one that a device comes set with – for example, the passcode used to access voice mail messages

5. Removable media:

Mainly USB sticks. These can be lost, leading to data breaches, or viruses and malware can be introduced to a system using them. Some organisations completely ban the use of removable media devices to counter the threat.

I once set off a virus alert at a school by plugging in a USB stick…

6. Misconfigured access rights:

This is where a network gives the wrong users access to data or systems that they shouldn't have access to. These should be restricted as part of the authentication process on the network.

Users ability to delete or alter documents should also be restricted – any user being able to delete a file on a shared drive or change an organisation's website would be a problem.

7. Unpatched or out-dated software:

Over time hackers find ways to exploit vulnerabilities in software, including whole operating systems. These can be "patched" by developers – software updates can be added to them to take care of the vulnerability. New versions of software will also be safer.

Anti-virus software also needs to be updated regularly. New virus definitions are issued every day.

Penetration Testing

Computer systems and networks need to be tested to check if they are suitably secure. This can be done using **penetration testing**.

Penetration testing is a testing process carried out by organisations. Someone attempts to gain access to a computer system or to data without using the normal means of access. The aim is to check how secure a system is.

Penetration testing can also be applied to physical premises. Can users access anywhere within a building? Should they be able to?

White-box testing:

A user with basic credentials tries to gain access to the elements of a system they shouldn't be able to access. For example, a low-level employee's credentials might be used to attempt to gain access to secure data files.

Black-box testing:

A user without any access credentials at all attempts to gain access to a system. They won't have any detailed knowledge about the system – but may be able to make some assumptions based on normal ways of setting up systems. The purpose of black-box testing is to simulate the sort of event which might occur due to a hacking attempt or cyber warfare attack.

There are two types of penetration testing. You need to know the differences between them and what they are used for.

Activity 1:

a) Write a definition of the term **cyber security** [3 marks]
b) List **four** distinct purposes of cyber security
c) Summarise **threats 3-7** from the list on the opposite page. Make sure you have **examples** of how the threat might work. You will need to **research** into this topic
d) Give **three** ways in which password security can be ensured on a local network
e) Explain the importance of changing default passwords on a computer system

Activity 2:

a) What does the term **penetration testing** mean?
b) Describe the differences between black-box and white-box penetration testing
c) Explain how black-box testing might be used to prepare for a hacking attempt

Activity 3:

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

a) Explain why Obidos Travel should conduct penetration testing [4 marks]
b) What form should this testing take and how should the company organise it? [6 marks]