ICT Level 2 – Networking and Staying Safe

1 of 20 – Welcome

Welcome to this session on networking and staying safe.

By the end of this session, you will:

* Understand what is meant by computer networking
* Know a number of the security risks associated with networking
* Understand the different methods that can be used to keep users safe

2 of 20 – Introduction to networking and staying safe

**What is networking?**

A network is the space that computers send information through, in order for users to communicate with each other. Networks can be found in a number of different places.

Computers that are connected through a network can share resources with each other. This might be something simple – like a laptop, a tablet, and a personal computer all sharing the same internet connection at home.

Alternatively, it could be something slightly more complicated – like hundreds of computers being connected to the same business network, housed inside a large company.

3 of 20 – Different types of networks

You might remember from an earlier session that there are a number of different network types available for computer users now. The main types are:

* Local area network (LAN)
* Wide area network (WAN)
* Personal area network (PAN)
* Mobile broadband

These networks can be used in a number of different places on a number of different scales – meaning some of them will be used by hundreds of users while some will only be used by a few. However, even when there are only a handful of users connected to a network, there are still some security risks that computer users need to keep in mind.

4 of 20 – Introduction to security risks

Security risks broadly refer to anything that can damage a computer system or network. This damage might take the form of limiting the network somehow, meaning that it cannot perform the tasks it normally does, or it cannot perform normal tasks properly.

However, this damage might also mean that the network’s stored data – meaning, data that is stored on any computer system that is connected to the network – becomes compromised or vulnerable, so people who should not be able to access the data will now be able to.

There are a number of different threats that have to be considered in network security, such as:

* Trojan horses
* Password attacks
* Unauthorised access

We will look at these, alongside one or two others, in more detail.

5 of 20 – Malware, viruses, worms

Malware, viruses, and worms are terms that are often used in place of each other, as they typically refer to different types of the same security threat.

Broadly speaking, malware – or viruses, or worms – are pieces of code that are added to a computer, usually without the knowledge of the user. This code might be delivered with a software download, or even something simple, like clicking a link to a certain website.

When malware has been introduced to an individual computer, this virus can then move through the network that this computer is a part of, eventually infecting other computers in the process.

These pieces of code can cause huge amounts of damage to a computer system, damaging and compromising massive amounts of stored data in the process. Fortunately, there are one or two programs available now that hunt these viruses down before they can do any real damage.

6 of 20 – Trojan horses

Trojan Horses are introduced to a computer system through some kind of download. This malware – which is not categorised as a virus – is usually disguised as a program designed to perform a seemingly harmless task on a computer system.

However, once downloaded and installed, a Trojan Horse can run riot on a computer system! It can cause changes to the system itself, including how it is set up to run, and it can trigger unusual activity from other programs, even when the computer system is not active – meaning there is no one using the computer at the time.

The reason that Trojan Horses are malware and not viruses is because Trojan Horses cannot duplicate their code – meaning, they cannot copy themselves onto other computer systems throughout a network. While this limits the security risk to other networked computers, a Trojan Horse can still cause a lot of damage to an individual computer.

7 of 20 – Phishing

Phishing is the term used to describe an individual who is disguising themselves online, usually as some kind of an authority figure. Phishing is often done for one of two reasons:

* Distributing dangerous links – an individual might send emails containing malware, or links to malware, which can compromise the computer and maybe even an entire network
* Gaining information – an individual might send emails asking for certain login details, such as a user’s password for example, and this is usually done under the guise of ‘fixing a problem’ or ‘checking for suspicious activity’

Although phishing will not always lead to viruses or malware being introduced to a computer, it is still a risk to watch out for as some of a user’s most personal and valuable information can become available through this type of hack.

8 of 20 – Password attacks

A password attack is a broad term that refers to the process of hackers trying to decode users’ passwords. This is usually done so that the hacker can then gain access to certain information, that would otherwise be password protected. There are many ways that hackers can gain access to people’s passwords, such as:

* Cracking programs
* Dictionary attacks
* Password sniffers

This is a security risk that all network users are vulnerable to, as there is not currently one single program that can protect individuals against this kind of attack. However, companies are trying to limit attacks by asking for more complicated passwords, demanding that users include a minimum number of characters, plus a number and/or punctuation mark.

9 of 20 – Unauthorised access

The types of malware that have been discussed are different methods for someone to gain unauthorised access – typically to messages, files, and resources, but broadly to programs, websites, and servers.

Here is some more information about unauthorised access:

* Unauthorised access is the term used when someone who is not allowed to access certain data, somehow gains access to it
* Gaining access will be the end result of most security attacks, as these usually occur when an individual or a group of individuals working together are trying to gain access to information that is normally kept private – this might be bank details, passwords, or any kind of personal account that stores sensitive or valuable data
* Companies that rely on large networks to connect all of their computer systems will often limit access to certain employees – meaning if someone does not need to know something, then they will simply not be able to access it on the system. Hackers have found many ways around this, though

10 of 20 – How can users protect themselves?

Even though there is no way to get rid of every possible security risk, there are certain steps that computer and network users can take, in order to make their systems more secure. Things such as:

* Anti-virus software
* Malware detection software
* Access levels

These can all be introduced to systems in order to protect them from threatening software or even threatening users, i.e. users trying to gain access to areas that they have been restricted from.

We will look at some of these options in a little more detail in the sections that follow.

11 of 20 – Anti-virus software

Anti-virus software broadly covers a number of software programs that are used to combat different types of viruses – including Trojan Horses.

This anti-virus software can be downloaded onto a computer system – or indeed onto a whole network of computers – in order to monitor and block anything that looks like a virus or threat. The software will often block the incoming threat and then send a quick alert to the computer user, to let them know what has happened.

For a large network of computers, such as those in a big business or company, there is usually a network manager – one individual who is responsible for maintaining the running and day-to-day safety of the network, and the computers housed within it. This individual will often monitor anti-virus software too, to ensure that each individual computer is up-to-date and properly protected.

12 of 20 – Firewalls

A firewall is a similar type of software to anti-virus software, in that both software types can protect whole networks of computers from incoming threats.

However, firewalls are specifically designed to stop outside users from gaining access to a protected network. A network manager might employ a firewall to keep a company’s data safe from online intruders, as the firewall will stop unknown connections being made.

Firewalls will also alert users to the threat, once it has been stopped, and this technology is now so heavily relied on by technology users that it has been introduced as a standard feature in many operating systems – meaning a new computer is likely to come with some kind of firewall program built into it.

13 of 20 – Secure passwords

This is a security tip with password attacks in mind. The only way to avoid password attacks – or rather, successful password attacks – is to make a password too hard for a hacker to decode, or decrypt.

This is why users are now told to make their passwords more secure, by using a mixture of different symbols, such as: YoU11F1ndTH1sHArd2GUeSs!1

A mixture of upper- and lower-case letters alongside numbers and symbols will make it hard for someone to guess or translate a password, even when they are using a program designed for this very task.

Using different passwords for different accounts is a useful security tip, too!

14 of 20 – Access levels

Access levels are commonly used in large companies where there is a lot of data stored inside the network. Access levels work by distributing and limiting access to certain areas of the network, meaning that only certain members of staff can gain access to certain parts of the system.

By using access levels a company can also restrict people from downloading certain programs, which may help to prevent the spread of viruses and malware.

Also, by portioning off access to different parts of the system to different users, should the network be attacked by hackers, it decreases the chances of them gaining access to the entire network.

Another day-to-day example of access levels can be found in home computers too, as parents may sometimes limit what their child has access to – such as accessing certain pages on the internet or being able to download software (restricting these things will make a home network much safer in the long-run).

15 of 20 – Question 1

Match the security risks; **Phishing**, **Password Attacks** and **Trojan Horse**, to the descriptions below:

1. A hacker using software designed to decrypt or decode an individual’s password
2. Someone disguising themselves as an authority figure via email, to gain access to private data such as passwords
3. A program performing a seemingly harmless task which is actually designed to rearrange parts of the computer system

The correct answers are:

A hacker using software designed to decrypt or decode an individual’s password is a description of **Password Attacks**.

Someone disguising themselves as an authority figure via email, to gain access to private data such as passwords is a description of **Phishing**.

A program performing a seemingly harmless task which is actually designed to rearrange parts of the computer system is a description of a **Trojan Horse**.

16 of 20 – Question 2

Why are viruses so dangerous to computer networks?

1. Because they can cause serious damage to one important computer
2. Because they can spread throughout an entire network system
3. Because a virus cannot duplicate its own code
4. Because they can gain access to everyone’s emails

The correct answer is B, because they can spread throughout an entire network system.

17 of 20 – Question 3

Read the statements below and decide which ones are true and which ones are false.

Trojan Horses are not technically viruses because their code cannot duplicate itself.

True

False

The correct answer is: True

Anti-virus software can fight off viruses, but there is no software to fight off a Trojan Horse.

True

False

The correct answer is: False

There is not currently software available to protect users from password attacks.

True

False

The correct answer is: True

Using the same password for multiple accounts will keep users well-protected.

True

False

The correct answer is: False

18 of 20 – Question 4

Using the following choice of words; **alert**, **anti-virus**, **stronger**, **block**, **decrypt**, **network**, **outside threats**, **access levels** and **unauthorised access**, fill in the blanks for the paragraph below:

**Blank** software and firewalls are both reliable methods for protecting a computer network against **blank**. Both types of software will **blank** a user, so people will know when a threat has been made, and they will also **blank** whatever the threat is too. Other security techniques are making **blank** passwords, meaning they are harder for hackers to **blank** and also using access levels. **Blank** will limit what each computer user has access to, which means that individuals within a company cannot gain **blank** to protected parts of the **blank**.

The correct paragraph should read:

**Anti-virus** software and firewalls are both reliable methods for protecting a computer network against **outside threats**. Both types of software will **alert** a user, so people will know when a threat has been made, and they will also **block** whatever the threat is too. Other security techniques are making **stronger** passwords, meaning they are harder for hackers to **decrypt** and also using access levels. **Access levels** will limit what each computer user has access to, which means that individuals within a company cannot gain **unauthorised access** to protected parts of the **network**.

19 of 20 – End

Well done! You have now completed this session on networking and staying safe.

In this session we have covered:

* What is meant by computer networking
* A number of the security risks associated with networking
* The different methods that can be used to keep users safe

If you have any questions about any of these topics, make a note and speak to your tutor for more help.