Curriculum for Excellence

National 4/5

Information Systems Design & Development

Security risks and Security Precautions

Hacking

When you access a website, you sometimes require privileges. This means you need a login name and password to gain access. Having access and the legal right to access is known as having “privileges”.

Hacking is gaining unauthorised access to a computer system (in this case via a webpage). Since this isn’t your legal right to do so, it is not privileged access. A **hacker** is somebody who gains access to a person’s computer **without their permission**. The **Computer Misuse Act** makes this against the law. Once they have gained access to a computer they can view, edit and delete the files on it. This could be personal, private or sensitive information.

Security Risks – Malware

Malware is malicious software and can be split into three categories: **Viruses, Worms** and **Trojan Horses**.

Your teacher will show you a video clip “What is Malware?”. Complete the following exercises. All your answers should be entered into the presentation template – check with your teacher if you don’t know what this is.

Viruses

A computer virus is a self-replicating program. A virus must be have 2 criteria:

1 – It must be executable

2 – It must replicate

Human activity is required to open and spread a virus. This could be opening an infected file, such as an e-mail attachment.

A virus can sit on your computer for a long time without causing harm, so longs as the infected file is never opened.

Viruses will often be attached onto other files, such as a Spreadsheet file. Every time the Spreadsheet file is opened, so is the virus, where it can then replicate and cause harm.

Worms

A computer worm is very similar to a virus. The main difference is that a worm can **replicate itself.**

Unlike a virus, a worm **does not** need to attach itself onto another program.

Some worms will only replicate themselves and consume bandwidth on the network. Others can cause harm to computers, such as deleting files.

The ILOVEYOU worm infected over 50 million Windows computers in 2000. It was estimated to have caused $5.5 billion in damages!

Trojan Horse

A Trojan will usually **disguise** itself as a useful program or file. The same way as the mythical Greek Trojan Horse.

They can be used to steal information, but most are designed to create a **back door** on your computer. This allows an attacker to gain **remote access** to your computer, to do what they want!

Those on the receiving end of a Trojan Horse are usually tricked into opening them because they appear to be receiving legitimate software or files from a legitimate source.

Unlike viruses and worms, Trojans do not reproduce by infecting other files nor do they self-replicate.

Why are they created?

Financial Gain

- They can be used to steal card details from people and then spend their money.
- They can be used to steal personal or sensitive information and sell it to others to use. For example government or military information.
- They can be used to steal information from a company and then blackmail the company for money, or they will release the information to the public.

Revenge

- A person may attack a company or individual who they do not like. Such as a company that they have been sacked from.

Attention

- Some people will enjoy the attention they receive while others just like to watch the harm it will cause other people.

Other Security Risks – National 5

Spyware

Spyware is software that **collects user information.**

It is often installed on a computer when the user is downloading other files, especially on file sharing websites. This is why you should always scan any downloaded files.

Once installed it will monitor user activity and **send** it back to somewhere else.

Spyware is widely used for advertising purposes, but it can also be used to gather information about e-mail addresses, passwords or card details.

Most Spyware is **not** illegal.

When you download a file, you will have to accept a **licence agreement form**.

This may include information about installing Spyware on your computer. However, most users do not take the time to read this! Therefore **you** have gave it permission to be installed on your computer, and therefore makes it **legal**.

Any Spyware installed **without** the users' permission is **illegal.**

Phishing

Phishing is a way of trying to get user information such as personal information or card details. Phishing is different because it will try to get the user to type in the details themselves.

Phishing scams are often sent through E-Mail and will pretend to be something useful.

Common Phishing scams include an E-Mail telling you that you have won the lottery, usually from a foreign country, or for a user to verify an account for a bank.

The idea is that the user will fill in their card details or enter their bank pin numbers or passwords back to the sender, who is in fact just a malicious user wanting your details.

Phishing scams are clever and unsuspecting people can be victims very easy. Here are some handy tips:

- Organisations will not ask for confidential information by E-Mail (or phone), so do not send them.
- Never reply to an E-Mail unless you are certain that you know where it came from.

- If you are unsure, contact the company direct before disclosing any information or go to a local branch.
- No companies, including banks, will ever ask for your pin number. If you forget it, a new one can be sent out to you by your bank.

Check the URL if you click them: www.bamkofscotland.co.uk

This Phishing scam looks genuine, can you spot anything suspicious?

Dear valued PayPal member,
It has come to our attention that your PayPal Billing Information records are out of date.That requires you to update the Billing Information If you could please take 5-10 minutes out of your online experience and update your billing records, you will not run into any future problems with PayPal online service. However, failure to update your records will result in account termination. Please update your records in maximum 24 hours. Once you have updated your account records, your PayPal session will not be interrupted and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.

Please click here to update your billing records.

Thank you for your time!
Marry Kimmel,

What was wrong?

- **No username**
- **Account will terminated – an attempt to get you to do it asap**
- **Wording – "5-10 minutes of your online experience" sounds unusual**
- **Click here – cannot see hyperlink address**

If you do need to update your details, go to the official website by typing it into the address bar or doing a search for it. Avoid clicking on links through E-Mail.

Remember that you can get a company logo very easily and attach it to a message!

Keylogger

A Keylogger **records** all of the **keys** that a user presses on a keyboard, **without** the user knowing about it.

All of the recorded keys can be saved to a text file and then send out periodically by E-Mail or uploaded somewhere else.

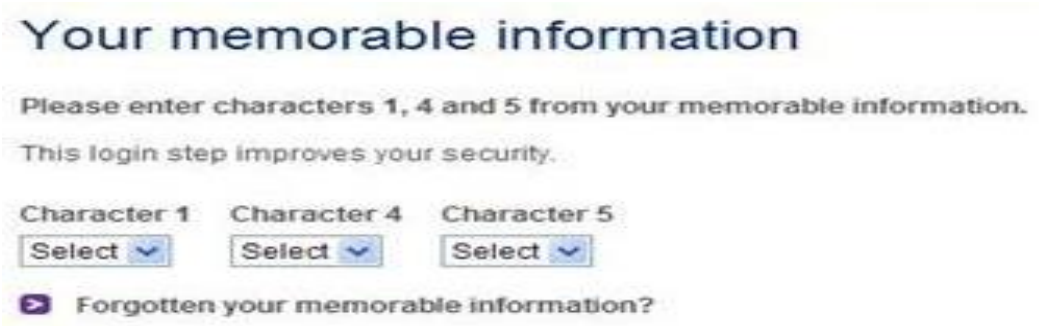
Keyloggers can be hardware based or software based.

They can be installed and run without being detected in the running programs list, so that the victim has no idea they are being targeted.

Keylogging is **illegal** if you are using it on **someone else's** computer or for **malicious purposes**, such as gathering card details and passwords. It is legal to install one on your **own** computer however. For example parents might want to record what their children are doing.

Many websites will now ask you for a **password** and a **memorable phrase**, in which you have to select a combination of random letters from it from a **drop down list**.

This avoids the user typing it in, and therefore will not be recorded by the keylogger.



A typical key log report might look something like this:

File Edit Format View Help

```
[2009-21-01 03:45:16 PM]chat.yahoo.com [Ent]
mike98a [Tab] mike [Ent]
hi david [Ent]
let's skip school tomorrow, he? [Ent]
Nobody should find out! [Ent]
What do u mean? [Ent]
Of course! [Ent]
[2009-21-01 03:46:09 PM]check out this link: [Ent]
www.forbiddenstuff.com/thread12961.html [Ent]
send it to you by email [Ent]
[Ctl]N [Alt] [Tab] [Ent]
mail.yahoo.com [Ent]
mike98a@yahoo.com [Tab] mike [Ent]
david_ros@gmail.com [Tab] fun stuff [Ent]
[2009-21-01 03:49:54 PM]here's the link, make sure nobody
sees it [Ent][Ctl]v [Ent] [Alt] [Tab]
```

It can be difficult to know if a keylogger is installed on your computer. Many are not picked up by anti-virus software, as they are not seen as threats.

Online Fraud

Online fraud is when the Internet is used by somebody with the intent to gain personal or financial information.

Trojans, Phishing and Keyloggers can all be used for online fraud.

Card details can be used for financial gain.

Personal information can be used for identity theft, which we are going to look at.

Identity Theft

Identity theft is **stealing** somebody's identity and pretending to be them.

Once they have collected enough information they can use it to obtain:

- Credit cards
- Bank loans
- Passports
- Driving licences etc

All in **YOUR** name

Attackers can use methods such as **Phishing** to obtain these details.

DOS Attacks

A Denial of Service attack (DoS) is an attack on a computer network or server.

It is used to make a network or server unavailable to people trying to access it. It does this by **flooding** the target with so many requests that it will either **run very slow** or **crash** the system.

They are designed to cause **disruption** to a service. They are commonly used to **crash websites**. They do not steal any information, unlike most other threats.

The effects of a DoS attack are similar to that of a ticket website, when tickets are released for a popular event. When so many people are on the website at the same time, it will crash the website or make it really slow.

The purpose of a DoS attack is to make the website or network **unavailable** to the people trying to use it.

Why would anybody want to do this?

Traditionally attackers would **blackmail** a company telling them that they were going to attack them (usually a website) unless the company paid a sum of money to them.

A company could lose a **lot** of money if their website is not properly running. For example a bookmaker website around the time of a major sporting event, such as the grand national.

Security Precautions

There are many security precautions that you can take to prevent your computer from being hacked or infected by viruses. In this section we will take a look at how you can help prevent your computer from being infected by a virus.

Anti-Virus software is used to find viruses on your computer. There are many different companies who create anti-virus software but essentially they all work the same way. They each have a database of known viruses and they will match the virus in the database against the files on the computer system and compare them to see if there are any infections.

To help prevent your computer from getting infected you can do the following:

1. Do not open attachments from people you do not know or messages that your contacts would not usually send.
2. Buy anti-virus software and keep it **up to date** as new viruses, worms & trojans are created every day!

Other Security Precautions – National 5

Networks can be kept secure in a number of ways. We have already looked at how to make a password as secure as possible.

Passwords

- Change regularly
- Don't choose family names or birthdays
- A mix of random number and letters is best

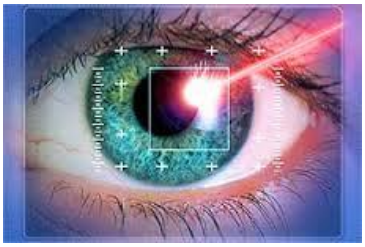
"Sorry, I can't remember my 11:00 am password. Can we discuss your plan to further improve security anyway?"

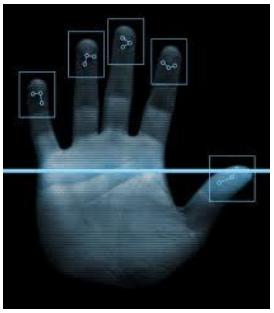
Encryption

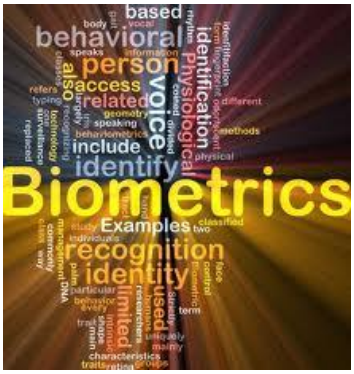
- **This means putting data into a code to prevent it being seen by unauthorised users.**

Biometrics

Using a person's physical characteristics to gain access to networks is known as Biometrics. Examples of this can be retina scan, finger prints and voice analysis.







Security Protocols

S-HTTP

This encrypts and transmits each message individually. It extends the HTTP protocol by encrypting web pages and supports authentication of message using a rage of encryption techniques.

Firewalls

A firewall can be either hardware or a software device/software that helps to protect a network.

You need a firewall because once you're on broadband, your computer is continuously connected to the global internet and identified by a unique number - its IP address. So it's potentially visible to anyone else on the network, and malicious users may be able to gain access to it.

Security Suites

There are many different Security Suites, all of which will carry out some or all of the elements of security listed below. To see a larger picture of this image click here.

TOP SECURITY SUITES FOR 2013

	SECURITY SUITE	Rating	Malware detection			Infection cleanup		Scan speed		Design score	Bottom line
			Signature-based detection of malware	Blocking of real-world malware: fully blocked attacks	Blocking of real-world malware: partially blocked attacks	Successful cleanup of active malware components[1, 2]	Successful cleanup of active and inactive malware components[1]	On-demand[1] in seconds[3]	On-access[1] in seconds[3]		
1	F-Secure Internet Security 2013 **$73 for 1 year/1 PC** go.pcworld.com/fsecure2013	★★★★½ SUPERIOR	99.0%	100.0%	0.0%	100.0%	90.0%	76	230	Very good	F-Secure's latest suite offers excellent protection and a friendly user interface.
2	Norton Internet Security (2013) **$50 for 1 year/3 PCs** go.pcworld.com/norton2013	★★★★½ SUPERIOR	99.8%	100.0%	0.0%	90.0%	60.0%	79	175	Superior	With its great detection rate and Windows 8–ready design, Norton's suite is definitely worth a look.
3	Trend Micro Titanium Internet Security 2013 **$50 for 1 year/3 PCs** go.pcworld.com/trendmicro2013	★★★★½ SUPERIOR	100.0%	100.0%	0.0%	100.0%	80.0%	110	341	Very good	This "titanium" suite earned high marks in almost all our detection tests, and it has a nice interface.
4	Bitdefender Internet Security 2013 **$70 for 1 year/3 PCs** go.pcworld.com/bitdefender2013	★★★★½ SUPERIOR	98.8%	100.0%	0.0%	100.0%	90.0%	121	341	Very good	Bitdefender has a user-friendly interface that will appeal to people of all experience levels.
5	Kaspersky Internet Security 2013 **$60 for 1 year/3 PCs** go.pcworld.com/kaspersky2013	★★★★☆ VERY GOOD	98.1%	94.4%	0.0%	100.0%	80.0%	70	368	Very good	Kaspersky lets both beginners and advanced users get the most out of its suite, and scored well in our tests.
6	McAfee Internet Security 2013 **$40 for 1 year/1 PC** go.pcworld.com/mcafee2013	★★★★☆ VERY GOOD	99.9%	94.4%	0.0%	100.0%	70.0%	95	300	Very good	McAfee didn't earn top marks, but it's still a proficient, user-friendly antimalware program.
7	G Data InternetSecurity 2013 **$35 for 1 year/1 PC** go.pcworld.com/gdata2013	★★★½☆ VERY GOOD	99.7%	100.0%	0.0%	100.0%	80.0%	116	362	Fair	G Data has an effective suite, but installation is a hassle, with a settings panel more suited to advanced users.
8	AVG Internet Security 2013 **$55 for 1 year/1 PC** go.pcworld.com/avg2013	★★★½☆ VERY GOOD	97.8%	94.4%	5.6%	90.0%	60.0%	108	391	Very good	AVG's security program is perfectly respectable. But that just doesn't cut it these days.
9	Avira Internet Security 2013 **$60 for 1 year/1 PC** go.pcworld.com/avira2013	★★★½☆ VERY GOOD	98.8%	94.4%	5.6%	100.0%	50.0%	101	266	Fair	This suite is competent at detecting, disabling, and cleaning up malware, but its user interface is unfriendly.

CHART NOTES: Prices as of 1/8/13. Percentages rounded to the nearest tenth. [1]Test conducted at default settings. [2]Cleanup of active malware files. Does not include removal of Registry changes or inert files. [3]Time to scan 4500MB of data; lower is better.