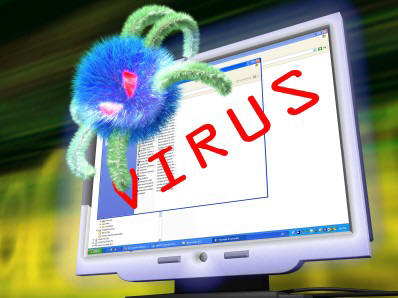
Security Risks

**Viruses**

A computer virus is a program that makes copies of itself, attaches itself to programs you have installed on your computer and then damages your system.



**Worms**

Similar to a virus, a worm is a program that makes copies of itself and then spreads through a network, damaging systems as it goes along



**Trojans**

•This is a program that looks harmless and tricks you into running it on your computer.

•It then carries out its real task for example, displaying adverts on the desktop or installing unwanted toolbars

**Hacking**

•Gaining unauthorised access to a computer or network.

•This is breaking the computer misuse act.

Security Risks

**Spyware**

Spyware is a software program that once installed on your computer, **can monitor and collect personal information** about your web surfing habits and the w eb pages that you visit.

You are usually **unaware that your machine has been infected** by spyware and it can sit in the background, collecting information about you and then transmitting it back to the author of the spyware - often advertisers who want to know what you are interested in and what adverts you click on.



**Keyloggers**

Keyloggers are another form of spyware. The purpose of a key logger is to **monitor and store a record of every keystroke** made on the computer. This data may then be sent to a remote server without your knowledge. It is specifically looking for user names and passwords used for things such as **bank accounts, credit card numbers** etc.

**Phishing**

Phishing is a form of **online fraud** where criminals aim to **steal valuable information** such as credit cards, social security numbers, user IDs and passwords for bank accounts.

They set up a **fake website which looks identical to a legitimate company** such as a bank or insurance company. They then try to trick people into logging into the site and giving their account details and security codes.

**Identity Theft**

Identity theft is where **criminals obtain personal information** such as your date of birth, bank account numbers, your mother's maiden name, your pet's name and so on.

These personal details are often used as questions by companies for you to prove who you are over the telephone. So, if the thief can answer these questions there is a good chance they will succeed in impersonating you and could possibly purchase things in your name, take out loans, even take money from your accounts!

**DOS (Denial of Service) Attacks**

A DoS attach is an illegal act, with the **intent of disabling a server**.

A server responds to external requests from its network. For example a web server responds to a browser calling for a web page to be delivered from its hard drive. Each request takes a small amount of time and some CPU resources on the server.

With a 'Denial of Service' attack, the **server is overwhelmed by millions of rogue requests** being sent it, effectively **using up all its resources** and denying normal service for legitimate users.

Security Precautions

**Encryption**

Encryption means to **scramble a message** in such a way that **only the people who are meant to read it can** do so.

A message sent 'in the clear' looks like:

"This is a message anyone can read"

and the encrypted message looks like gibberish:

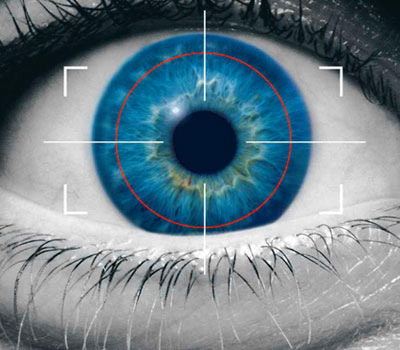
fu11^&\*\*$$HHPPHDYhg\*\*&&£--20dkmama@()@88787399(&\*&))\*\*OJKK@\_D

Encryption works by both people **making use of a secret 'key'** that only they know (or at least their computers know). The original message is mixed in with the key to create a secret message. This is done by some very crafty mathematics so that it is very very hard for someone to crack the code - very powerful computers working for a long time would be needed to crack a good code.

**Password**

Your password should be **kept secure** at all times, never written down or given out to other people.

Passwords should be carefully chosen. They should not be something, which is easily associated with you and could be guessed e.g. your favourite football team or your dog's name. They **should contain a mixture of letters, numbers and symbols**. This makes it difficult for special password cracking software to identify your password.

**Biometrics**

This describes various technologies used to measure some **feature of a person** in order to identify them.

For example

* **Fingerprint recognition**
* **Iris recognition**
* **Voice recognition**
* **Facial recognition**

These biometric systems are very secure as the **biometric information is unique to that one person**.

Biometrics is a controversial topic because many people are concerned with privacy issues when they are applied to things like passports and identity cards.

Anti-Virus Software

http://ns.bdnews24.com/blog/en/wp-content/uploads//2012/03/anti-virus.gifAnti-virus software is software used to prevent, detect and remove malware (of all descriptions), such as: computer viruses, malicious BHOs, hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraudtools, adware and spyware. Computer security, including protection from social engineering techniques, is commonly offered in products and services of antivirus software companies

Firewalls

A firewall is designed to help **protect a computer network from intruders**. It does this by controlling **what data can and cannot pass through it.**

A firewall can either be

* A piece of software e.g. Windows has a built in Firewall, Zone Alarm is a free firewall or you can purchase commercial software firewalls.
* A piece of hardware. These boxes are much faster than the software version but they are also much more expensive and tricky to set up.

You would expect home networks to be protected by a software firewall but a large corporation would have several layers of hardware firewalls protecting their networks as well as intruder detection software applications looking for odd behaviour on their networks. Basically, the more valuable or sensitive the information, the higher the level of protection expected.

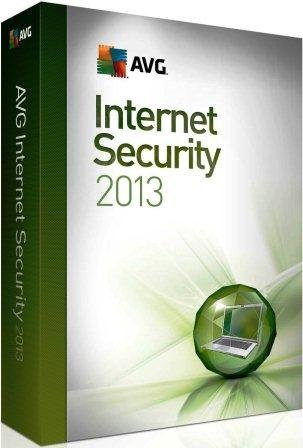
Security Protocol (SSL)

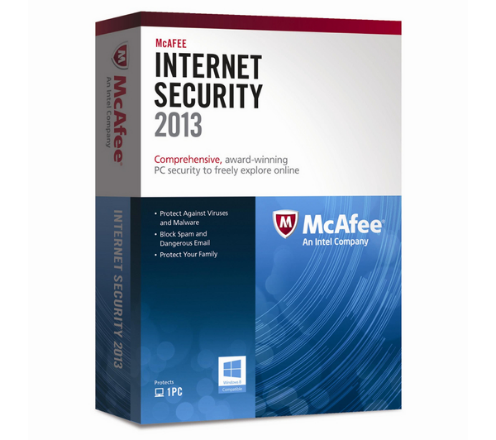
SSL stands for 'Secure Socket Layer'. It is a web browser security technology.

SSL is **built into a web browser**. SSL allows **confidential data to safely pass from your web browser to a distant server** via the Internet. The confidential data is 'encrypted' or scrambled so that only the server can read it.

For example, e-commerce shops use SSL to **keep your credit card details secret.**

You can tell when SSL is being used as a **small padlock appears** somewhere on the browser window or your URL will have an S, for secure, after HTTP. If you click on the padlock, a 'certificate' window appears that confirms you are connected to the real server and not a fake one.

Security Suites

Security suite software is not a single program, but is usually composed of **more than one application** that aims to provide **total protection** to its user. Still at its core is an antivirus program. But aside from an antivirus program, the other applications in the suite provide more security from the threats that arose along with the Internet age.

Security suites commonly **includes a firewall, anti malware, anti spyware, and email protection programs.**