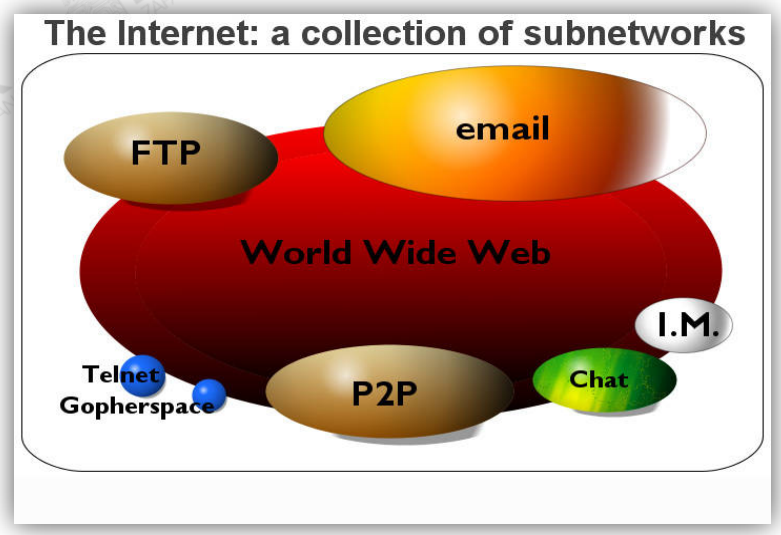
Topic: 1.2.2 Security aspects

THE INTERNET

The word "Internet" is basically derived from "interconnection of computer networks". Alternatively referred to as the **net** or the **web**, the **Internet** was initially developed by the IPTO with the intention of helping to develop the progress of computing technology by linking the work being done by all the best academic computer centers. The Internet as we know it today first started being developed in the late 1960's and transmitted its first message on Friday, October 29, 1969. In 1993, the Internet experienced one of its largest growths to date and today is accessible by people everywhere in the world.
The Internet contains billions of web pages created by people and companies from around the world, making it a limitless location to locate information and entertainment. The Internet also has thousands of services that help make life more convenient. For example, many financial institutions offer online banking that enables a user to manage and view their account details online.

The Internet basics

- The Internet uses the TCP/IP protocol and is accessed using a computer modem, broadband, 3G or network that is connected through an ISP.
- The Internet is explored, which is more commonly referred to as surfing, using a computer browser.
- Finding information on the Internet is achieved by using a search engine.
- Users browse web pages by following hyperlinks.
- Files, pictures, songs, and video can be shared by uploading and downloading.
- The Internet is also used for communicating with others through networks, forums, chat, e-mails, and IM.

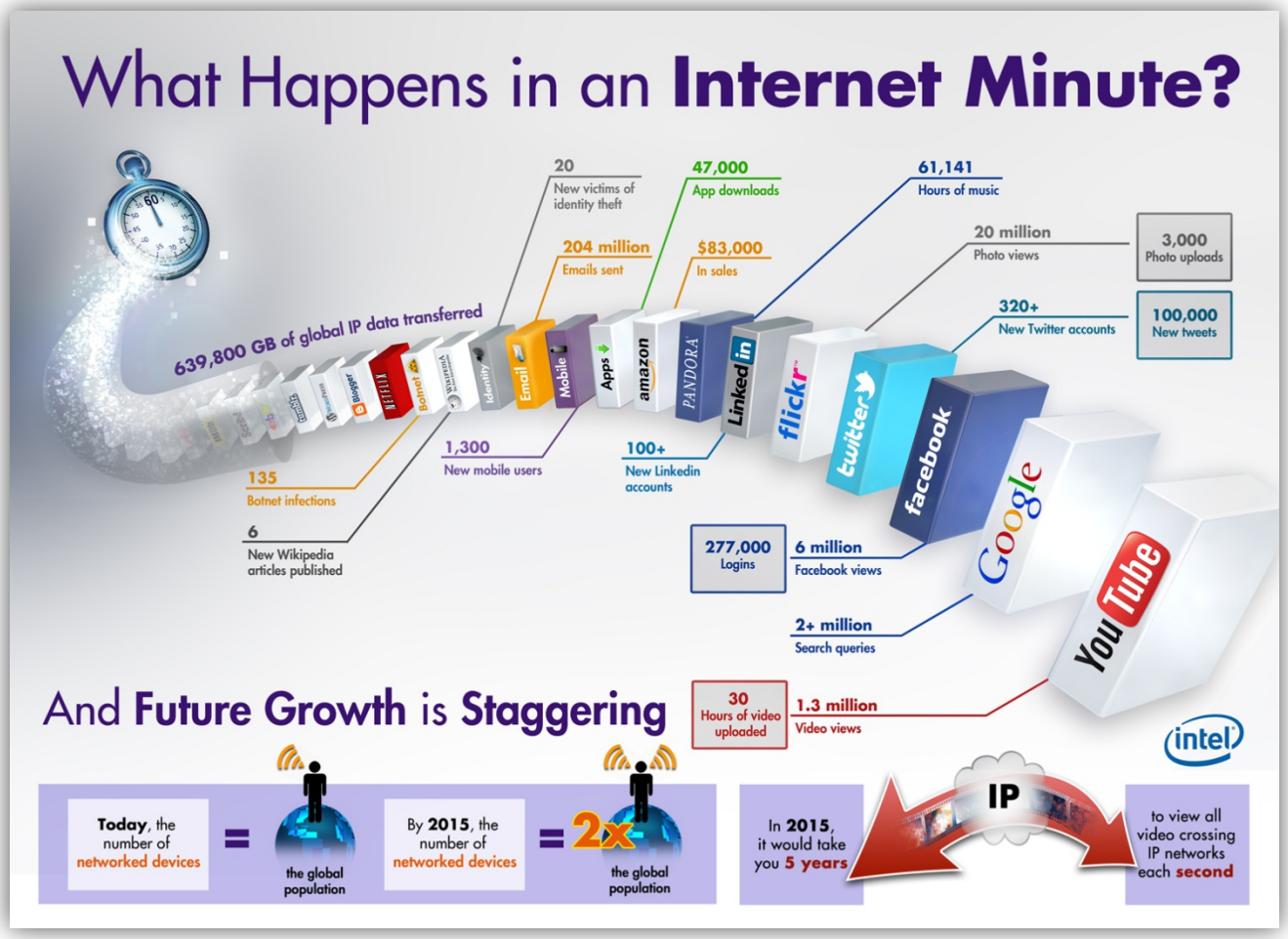


Topic: 1.2.2 Security aspects

Connecting to the Internet

You may require the following to connect to the internet:

- a computer
- telephone line (cable being the exception)
- modem and/or router
- an ISP (Internet Service Provider)
- Web browser, e.g. Internet Explorer, Firefox, Chrome, Safari, Opera etc.



Topic: 1.2.2 Security aspects

SECURITY CONCERNS FOR INTERNET USAGE

Internet is used widely and has become a common platform to share the files between the computers in the world. Internet has made new ways to interact among the people and the organizations.

And with increase in the usage of the Internet there are many threats in the computer market like Trojans, spy wares, virus attacks. These threats attack the computer; corrupt data files, and may even crash the system. So it is also very important to protect your computer from these malicious attacks. So to avoid these threats and the hackers in order to be safe on the Internet, we must follow some safety measures to prevent these threats to our computer. Hence Computer security is essential to prevent loss of your precious data.

Here are certain security aspects you need to be aware of to protect your valuable data and resources:

Internet Confidentiality & Privacy

The *Internet* provides little assurance of privacy or confidentiality. The use of firewalls, anonymizers, and encryption can help mitigate the risks. Major considerations to keep in mind are discussed below.

- **Silent communications:** There are thousands of rogue actors and infected computers probing machines across the Internet at any given second. These bad apples are almost certainly trying to get control of your machine through any security fault or unpatched module they can find. Fortunately, their communications are fairly straightforward to trap, since by definition they are unsolicited -- it is easy to tell the difference between packets from a website you just accessed from a probe and from some site you never heard of before.

  The technological solution to this threat is called a "firewall", a program that monitors all communications and traps all illicit packets. Most operating systems now come with a firewall preinstalled. However, some, such as the Windows firewall, only block suspect incoming communications, leaving completely open access to the Internet *from* your machine. This is a barn-door sized hole that is eagerly used by almost every program you have on your computer to contact the home company for all sorts of reasons ranging from automatic checking for updates to transmission of usage metric data for their own proprietary purposes. The solution to this is a third party firewall that protects both incoming and outgoing communications. The free version of Zone Alarm is widely used.

- **Surfing leaves tracks:** There is little privacy or confidentiality on the Internet. Websites can track your surfing on their site by IP address and related system information, including system names and Internet network addresses that often uniquely identify your computer. Search engines generally record your queries together with your computer identification, building up a profile of your interests over time.

  To minimize these threats, you can turn your default browser settings to exclude cookies, since they can be used to build up detailed profiles of your surfing patterns over time (advertising sites

Topic: 1.2.2 Security aspects

with presence on many sites can even use cookies to track your surfing patterns across different sites). You can also use networked or single-point anonymizers to obscure your entire computer's local identifying information and obtain the maximum available Internet privacy.

- **Posting Information is always public**: When you post anything to a public Internet newsgroup, mailing list, or chat room, you generally give up the rights to the content and any expectation of privacy or confidentiality. In most countries, anything you post to a public space can be saved, archived, duplicated, distributed, and published, even years later, by anyone in the same way as a photograph taken in a public space like a city park.

  If you have ever posted anything to the newsgroups, you might find it interesting to search them now for the email address you used at the time, which is one reason you should disguise your email address when posting to the Usenet newsgroups.

- **Your Personal data can enlist all your activities**: If you give a site personal data like an email address, home address, phone number, birth date, or credit card number, be aware that the information can be easily cross referenced by a range of large service companies to assemble a detailed database of your buying habits, surfing patterns, and interests. And it usually is.

  If you do give websites personal information, it is a good idea to first read their Internet privacy policy to see how confidential they promise to keep it. Always keep a good track of security features offered by websites like "https" links, and allowing networking security options on your data.

- **Intercepting Valuable Information**: Without speculating on whom or why, Internet communications interception is technically easy to do at any of the perhaps five and twenty-five routers through which your packets are switched on the way to their destination. Software taps are easy to add. Direct physical interception through tapping into copper network cable near a house or in a switching station is straightforward with inexpensive equipment, and enables an eavesdropper to copy all of the traffic that passes over the line. Radio frequency interception of the traffic on copper lines is possible. Tapping into fiber optic line is more difficult, usually requiring a high angle bend to get a bit of light leakage, but is also technically possible.

  Encryption is the only sure solution.

- **Your Government bodies have the main control**: Many national governments are large enough with enough resources that they can and do intercept Internet communications.
  However, because of the volume of information if for no other reason, you can be reasonably assured that no-one is taking the time to look at your specific Internet packets unless you are connected to an investigation.

Topic: 1.2.2 Security aspects

The bottom line is that you have little privacy or confidentiality on the Internet, and unless your communications are encrypted and/or anonymized, you should assume that they can be read by others. At the same time you need to make a realistic threat assessment depending on what you are doing.

Internet risks associated with viruses, spy-ware and hacking

It is convenient to have access to vast content on the Internet such as important information, useful services and wonderful entertainment but unfortunately by accessing the Internet, you leave yourself vulnerable to some trouble makers who are waiting for an opportunity to harm you and your computer. Yes, we're talking about computer viruses, spyware/adware and hackers.

Computer viruses, spyware and adware- Plague to a Healthy Computer System

Computer viruses are software programs designed to access your computer without your consent, interfere with the computer's operation and records, corrupts, or deletes your personal data.

Adware are software programs designed for advertising and changing your computer's configuration. Spyware is software designed to collect personal information like what websites you visit or even discreetly transmits your personal information, such as your credit card number from your computer without your knowledge.

Another threat over the internet is of “Hackers”. The term hacker is used in popular media to describe someone who attempts to break into computer systems. Typically, this kind of hacker would be a proficient programmer or engineer with sufficient technical knowledge to understand the weak points in a security system.

What damages can they cause?

While viruses can be intentionally destructive, for example, by destroying data, many viruses are fairly benign or just plain annoying. Adware is mainly annoying but spyware can be downright dangerous if it manages to get hold of important information like your passwords or credit card information. Hackers can breaks into someone else's computer system, often on a network; by passes, passwords or licenses in computer programs or in other ways intentionally breach computer security.

Symptoms of a Virus Outbreak

The worse with viruses, adware/spyware and hackers are that they silently operate for a relatively long period of time in your computer without being detected. Therefore it's very important to follow the preventive methods described later in this guide. The common symptoms of a virus infection are that your computer works slower than normal, it stops responding and freezes often, crashes and restarts frequently or fails to run normally. Other possible symptoms are that the applications don't work properly and you can't print correctly, the discs and disc drives on your computer are inaccessible and you often see unusual error messages.

Topic: 1.2.2 Security aspects

The signs of spyware or adware infection are similar to the signs of a computer virus infection, but in addition to those you might get unwanted pop-up windows on your screen even if you're not browsing in the Internet, your web browser's start up page can be different than it should be or you might notice an unwanted toolbar on your web browser.

It can be difficult to detect a hacker on a computer because nothing changes to help disguise the hack. Below are the most common things that change after a computer is hacked.

- New programs installed
- Computer passwords have changed
- Increased network activity
- Unknown programs wanting access
- Security programs uninstalled
- Computer doing things by itself

ANTIVIRUS A WAY OF PROTECTION AGAINST INTERNET RISKS

WAYS OF PROTECTION

Even though the idea of having unwanted software running on your computer is scary, by following few easy steps you can keep your computer free from viruses, adware, spyware and other trouble makers.

Call the VIRUS POLICE DEPARTMENT a.k.a. "The Antivirus software"

In addition to a firewall you should install some kind of anti-virus software before connecting your computer for the first time to the Internet. Typical anti-virus software scans for the new viruses entering your computer, cleans up any viruses it finds and makes sure they can't do any more harm.

Just like firewall, your anti-virus software should be turned on at all the times so that when you start up your computer the virus scanner will also open. This ensures that viruses are caught as soon as possible. Anti-virus software will also check disks inserted in your computer, emails you receive and programs you download from the Internet for viruses.

If you receive a virus, your anti-virus software will usually notify you then will try to repair the file the virus has infected. It also isolates any files that can't be repaired and tries to rescue any files it can. Some software asks you to send the virus to the anti-virus company. If it is a new one the company will add it to their database.

Topic: 1.2.2 Security aspects

Having a functional Firewall System

An Internet firewall is a computer program or hardware appliance designed to prevent unauthorized access to private computers or networks. A Firewall can screen out viruses, worms, malware and hackers that try to access your computer over the Internet. Installing a firewall is the most effective and important first step you can take to protect your computer. Install the firewall before you access the Internet for the first time and keep it running at all times.

You can purchase a firewall for your computer from a local computer store or from the Internet. Some operating systems like Windows XP (with service pack 2) and Mac OS X have a built-in firewall.

Working of a Firewall

A firewall enforces a policy or set of rules governing the flow of data to and from the outside world. Firewalls that are used to protect home computers are usually based on packet filtering, i.e. Data packets (small units of information) are admitted or rejected according to the way these rules are configured. For the typical home user their primary function is to block uninvited incoming connections. Most firewall tools will come with a sensible set of rules by default.

Password Protection

Passwords are very important in keeping your online information safe. What is very important is the strength of the password that you choose. Your password should meet the following criteria:

- Be at least 6 - 8 characters
- Contain at least one character from ALL of the following four classes:
  Uppercase letters (e.g. A, B, C), Lower case letters (eg. a, b, c), Numbers (eg. 1, 2, 3), Punctuation symbols (e.g. ~!@#$%^&*()+-=)
- Doesn't contain your first name, your last name, your user ID, the word Optus, SingTel, a day of the week, month of the year or the word password.
- Is not a common word or keyboard sequence (e.g. 123, QWERTY, asdf, zxcv, poiuy).

You should change your password regularly and never share your password to others.

Use Updated and Valid software

As the viruses change constantly, it is very important that you keep your computer's operating system, firewall software and the anti-virus software up to date. The anti-virus software will automatically ask to be updated so make sure you do that. Many virus scanners can be obtained bundled with one year of free "updates" included. After this subscription runs out, the program will usually recommend that you re-subscribe in order to keep up-to-date with the needed protection.

Be alert of suspicious Emails

Most viruses arrive on your computer via email. Do not open an email attachment you haven't expected or if you don't recognize, even if you use an anti-virus software. Note that it is possible to get virus infected

Topic: 1.2.2 Security aspects

email also from your friends' and colleagues' email-addresses. A virus is not dangerous until the infected attachment is opened. Check that the contents of the message make sense before you open any attachments. Don't forward any attachment without being sure it is safe. Delete any email you think is infected and empty your deleted items folder regularly.

Pop Ups- The Virus Minions

Pop-up windows are windows that “pop up” on your computer screen when you open certain websites. Some websites try to fool you to accidentally download spyware or adware to your computer by clicking OK or Accept button on the pop up window. The safest way to close a pop up window is to close it from the little box with “x" on it on the top of the window.

Avoid Downloading files off unknown Internet sources

You can also get viruses, adware and spyware on your computer by downloading software and other files from the Internet. If the software is free and provided by an unknown software developer, or is an illegal "cracked" or "hacked" version of commercial software it is more likely to contain an additional and unwanted software virus than if you download or buy it from a respected and well-known software developer.

Back up your Data

To avoid losing your work in case your computer gets infected by a virus, make sure you have a recent backup of your most important work. If you usually back up the contents of your disk to an external hard drive or other writable media like floppy disks, don't plug in backup disks to your computer if you think your computer has a virus, as the virus could spread to your backups

Encryption

Encryption is called the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text* ; encrypted data is referred to as *cipher text*.