1. Basic Computing Concepts
(8) Social Implications of Computing

8 Social Implications

In this section we will discuss the following aspects of the social implications of computing:

- Computer Crime
- Privacy of Data
- Data Protection Act
- Web 2.0
- Plagiarism

8.1 Computer Crime

Malware (MALicious softWARE) is software designed to destroy data, steal information or aggravate the user. There are many forms of malware. Some are listed below.

8.1.1 Virus

A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. All computer viruses are man-made.

After the virus code is written, it is buried within an existing program. Once that program is executed, the virus code is activated and attaches copies of itself to other programs in the system. Infected programs copy the virus to other programs.

A virus is not inserted into data. Macro viruses, although hidden within documents (data), are still programs. It is in the execution of the macro that the damage is done.

Files attached to e-mail messages are a common way of infecting a computer when the recipient is not aware of file types that are potentially harmful. For example, files with extensions such as .EXE, .BAT and .COM can perform any operation within the computer and should never be clicked unless the user is expecting the attachment.

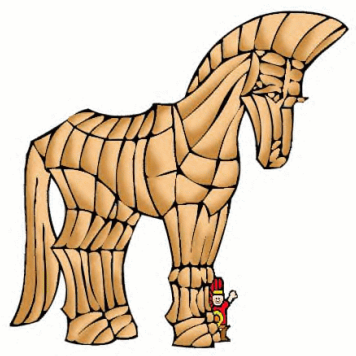
8.1.2 Worm

A worm is a destructive program that replicates itself throughout a single computer or across a network, both wired and wireless. It can do damage by sheer reproduction, consuming internal disk and memory resources within a single computer or by exhausting network bandwidth. It can also deposit. Very often, the terms "worm" and "virus" are used synonymously; however, worm implies an automatic method for reproducing itself in other computers.

It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks.

8.1.3 Trojan Horse

A Trojan Horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.



8.1.4 Spam

Spam is most often considered to be electronic junk mail or junk newsgroup postings. Real spam is generally email advertising for some product sent to a mailing list or newsgroup.

In addition to wasting people's time with unwanted e-mail, spam also eats up a lot of network bandwidth. Consequently, there are many organizations, as well as individuals, who have taken it upon themselves to fight spam with a variety of techniques. But because the Internet is public, there is really little that can be done to prevent spam, just as it is

impossible to prevent junk mail. However, some online services have instituted policies to prevent spammers from spamming their subscribers.

8.1.5 Logic Bomb

A logic bomb (also called slag code) is programming code added to the software of an application or operating system that lies dormant until a predetermined period of time (i.e., a period of latency) or event occurs, triggering the code into action. Logic bombs typically are malicious in intent, acting in the same ways as a virus or Trojan horse once activated. In fact, viruses that are set to be released at a certain time are considered logic bombs. They can perform such actions as reformatting a hard drive and/or deleting, altering or corrupting data.

8.1.6 Adware

Adware is the common name used to describe software that is given to the user with advertisements embedded in the application. Adware is considered a legitimate alternative offered to consumers who do not wish to pay for software. There are many ad-supported programs, games or utilities that are distributed as adware (or freeware). Today we have a growing number of software developers who offer their goods as "sponsored" freeware (adware) until you pay to register. If you're using legitimate adware, when you stop running the software, the ads should disappear, and you always have the option of disabling the ads by purchasing a registration key. Another use of the phrase adware is to describe a form of spyware that collects information about the user in order to display advertisements in the Web browser. Unfortunately, some applications that contain adware track your Internet surfing habits in order to serve ads related to you. When the adware becomes intrusive like this, then we move it into the spyware category and it then becomes something you should avoid for privacy and security reasons.

8.1.7 Spyware

Spyware is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Spyware is similar to a Trojan horse in that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Spyware programs are able to monitor keystrokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors, install other spyware programs, read cookies, change the default home page on the Web browser, consistently relaying this information back to the spyware author who will either use it for advertising/marketing purposes or sell the information to another party.

Licensing agreements that accompany software downloads sometimes warn the user that a spyware program will be installed along with the requested software, but the licensing agreements may not always be read completely because the notice of a spyware installation is often couched in obtuse, hard-to-read legal disclaimers.

8.1.8 Denial of Service

The goal of denial-of-service attacks is not to gain unauthorized access to machines or data, but to prevent legitimate users of a service from using it. A denial-of-service attack can come in many forms. Attackers may "flood" a network with large volumes of data or deliberately consume a scarce or limited resource, such as process control blocks or pending

network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data.

8.1.9 Email Spoofing

Email spoofing means forging an e-mail header to make it appear as if it came from somewhere or someone other than the actual source. The main protocol that is used when sending e-mail -- SMTP -- does not include a way to authenticate. There is an SMTP service extension (RFC 2554) that allows an SMTP client to negotiate a security level with a mail server. But if this precaution is not taken anyone with the know-how can connect to the server and use it to send spoofed messages by altering the header information.

8.1.10 Phishing

Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organizations site by mimicking the HTML code, the scam counted on people being tricked into thinking they were actually being contacted by eBay and were subsequently going to eBay's site to update their account information. By spamming large groups of people, the "phisher" counted on the e-mail being

read by a percentage of people who actually had listed credit card numbers with eBay legitimately.

Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting.

8.1.11 Windows vs. Mac

Almost all Windows users install an antivirus program in their computers, while most Mac users do not, at least as of 2011. Windows computers are attacked constantly, because they make up the huge majority of personal computers and are therefore the low-hanging fruit. In addition, the Mac is a Unix-based machine, and the Unix architecture separates the operating system from the applications, which makes it harder to crack. Although the overwhelming majority of Mac users do not use antivirus software, Apple's official position is that it is always prudent to be cautious.

8.1.12 Anti-Malware Strategies

Some Anti-Malware strategies are the following:

- Anti-virus
- Firewall
- Backup
- Recovery methods

8.1.12.1 Antivirus Program

Antivirus program searches for known viruses. It is also known as a "virus scanner." As new viruses are discovered by the antivirus vendor, their binary patterns are added to a signature database that is downloaded periodically to the user's antivirus program via the Web. Popular antivirus programs are Norton, McAfee, Sophos, AVG and Kaspersky.

Antivirus programs are used almost exclusively on Windows machines. Although available, the greater majority of Mac users, as well as desktop Linux users, do not use antivirus. The reason is simple. Mac and Linux make up approximately 10% of the desktop computer market, and, since they are all Unix-based operating systems, they are more difficult to crack.

Antivirus programs work two ways. The more common method scans the file against all known viruses each time the file is opened. The second method, such as used by Sophos, takes a blueprint of every file ahead of time. It computes a checksum of each file's contents and stores it in a database. The next time a file is opened, the software re-computes the checksum and compares it to the one in the database to see if the file has changed. If it has, the program scans the file for viruses. If not, the file is considered virus free. Since most files are virus free, this method is faster because re-computing a checksum is considerably faster than comparing the file to all the binary signatures.

8.1.12.2 Firewall

A firewall is the primary method for keeping a computer secure from intruders. A firewall allows or blocks traffic into and out of a private network or the user's computer. Firewalls are widely used to give users secure access to the Internet as well as to separate a company's public Web server from its internal network. Firewalls are also used to keep internal network segments secure; for example, the accounting network might be vulnerable to snooping from within the enterprise.

In the home, a personal firewall typically comes with or is installed in the user's computer. Personal firewalls may also detect outbound traffic to guard against spyware, which could be sending your surfing habits to a Web site.

In the organization, a firewall can be a stand-alone machine or software in a router or server. It can be as simple as a single router that filters out unwanted packets, or it may comprise a combination of routers and servers each performing some type of firewall processing.

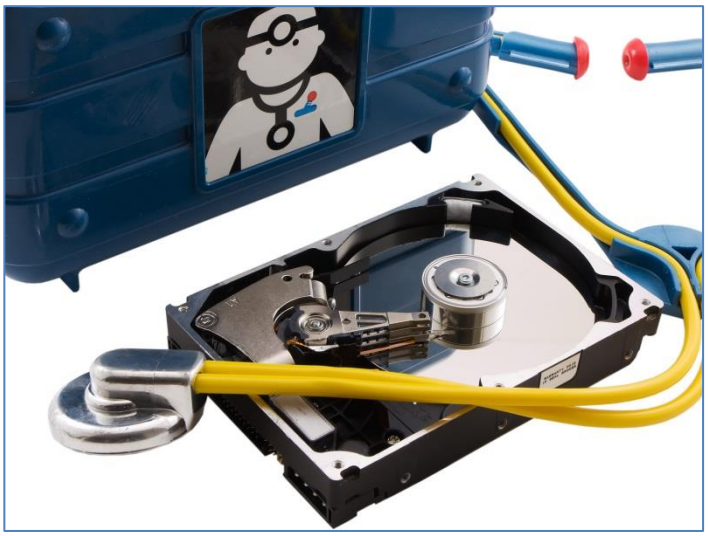
8.1.12.3 Backup

Backup is the activity of copying files or databases so that they will be preserved in case of equipment failure or other catastrophe. Backup is usually a routine part of the operation of large businesses with mainframes as well as the administrators of smaller business computers. For personal computer users, backup is also necessary but often neglected. The retrieval of files you backed up is called restoring them.

Personal computer users can consider both local backup (backup on DVDs, pen drives or external hard disk) and Internet backup (using the Cloud).
Some applications always remind users when they quit the program to backup their data. If your hard disk crashes, you'll be able to reconstruct your data.

8.1.12.4 Recovery Methods

Data recovery is the process of salvaging data from damaged, failed, corrupted, or inaccessible secondary storage media when it cannot be accessed normally. Often the data are being salvaged from storage media such as internal or external hard disk drives, solid-state drives (SSD), USB flash drive, storage tapes, CDs, DVDs, RAID, and other electronics (RAID is short for redundant array of independent (or inexpensive) disks. It is a category of disk drives that employ two or more drives in combination for fault tolerance and performance. RAID disk drives are used frequently on servers but aren't generally necessary for personal computers. RAID allows you to store the same data redundantly (in multiple paces) in a balanced way to improve overall storage performance.).



Recovery may be required due to physical damage to the storage device or logical damage to the file system.

8.2 Data Protection Act

The mission statement found at the Data Protection Commission website (http://idpc.gov.mt/) is this: "Our mission is to protect the individual's right to privacy by ensuring the correct processing of personal data." The Office of the Information and Data Protection Commissioner is committed to protect the individual's right to privacy by ensuring the correct processing of personal data. The Office aims to safeguard this fundamental human right which is enshrined in the Constitution of Malta.

The Data Protection Act of the European Parliament and of the Council was completely brought into effect on 15 July 2003. The main objectives of the law are twofold:

- the regulation of data controllers, the persons to determine the purposes and means of processing, who are obliged to process the personal data in accordance with inter alia the requirements and criteria established by law;

- the protection of privacy rights of an individual, including the right to information, the right of access and the right to rectify, block or erase personal data not processed in accordance with the Act.

In the implementation of the local legislation, the data protection supervisory authority has been vested in the Information and Data Protection Commissioner who enjoys the same independence attributed to a Judge in the local courts and acts independently without being subject to any direction or control of any other person or authority.

The Act empowers the Commissioner, among other things, with the following functions:

- to create and maintain a public register of all processing operations being notified by Data Controllers;
- to institute civil legal proceedings in cases where the provisions of the Act have been or are about to be violated;
- to encourage the drawing up of suitable codes of conduct by the various sectors;
- to order the blocking, erasure or destruction of data, to impose a temporary or definitive ban on processing, or to warn or admonish the controller;
- to collaborate with supervisory authorities of other countries to the extent necessary for the performance of his duties.

The following are the Principles of Data Protection. They are nine principles of 'good information handling'. The controller shall ensure that:

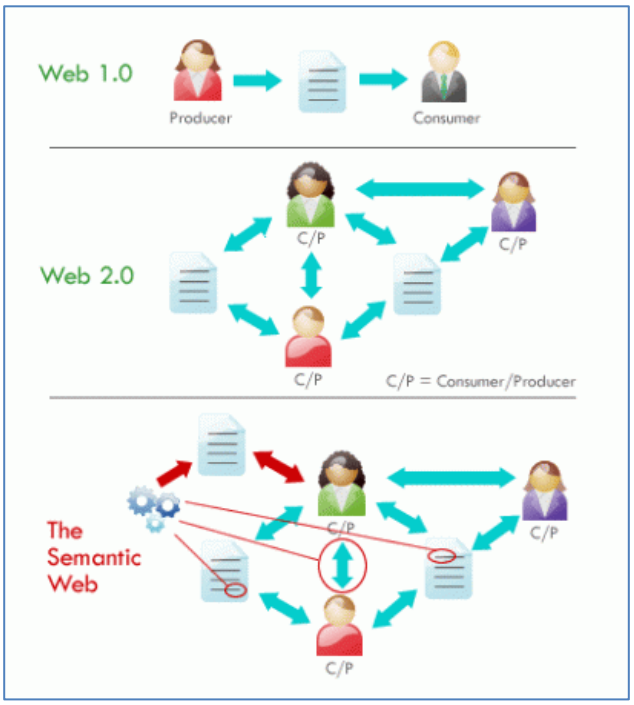
- Personal data is processed fairly and lawfully;
- Personal data is always processed in accordance with good practice;
- Personal data is only collected for specific, explicitly stated and legitimate purposes;
- Personal data is not processed for any purpose that is incompatible with that for which the information is collected;
- Personal data that is processed is adequate and relevant in relation to the purposes of the processing;
- No more personal data is processed than is necessary having regard to the purposes of the processing;
- Personal data that is processed is correct and, if necessary, up to date.
- All reasonable measures are taken to complete, correct, block or erase data to the extent that such data is incomplete or incorrect, having regard to the purposes for which they are processed;
- Personal data is not kept for a period longer than is necessary, having regard to the purposes for which they are processed.

8.3 World Wide Web

The World Wide Web is a system of Internet servers that support specially formatted documents. The documents are formatted in a markup language called HTML (HyperText Markup Language) that supports links to other documents, as well as graphics, audio, and video

files. This means you can jump from one document to another simply by clicking on hot spots. Not all Internet servers are part of the World Wide Web.

There are several applications called Web browsers that make it easy to access the World Wide Web. Examples of these are Firefox, Microsoft's Internet Explorer and Chrome.



World Wide Web is not synonymous with the Internet.

What do we mean by Web 1.0, Web 2.0 and Web 3.0? The first implementation of the web represents the Web 1.0, which, according to Berners-Lee, could be considered the "read-only web." In other words, the early web allowed us to search for information and read it. There was very little in the way of user interaction or content contribution. Shopping cart applications, which most ecommerce website owners employ in some shape or form, basically fall under the category of Web 1.0. The overall goal is to present products to potential customers, much as a catalogue.

Web 2.0 is the "read-write" web (if we stick to Berners-Lee's method of describing it). It has the ability to let users contribute with content and interact with other web users. For example, just look at YouTube and MySpace, which rely on user submissions.

Web 3.0 is also called the semantic web. It is considered a platform as a service. Here is an example: Let's say I am searching to arrange for a special evening with my wife. My goal is to find a great spot for dinner, a movie, and some fun activity all in the same general area with a budget of $125. I log on to a semantic site and type in something similar to the following: "I am looking for a great place to have dinner and see a movie in Philadelphia, Pa. for less than $125." Then I will have a conversation with the computer in real time. The system based upon my requests and previous search history will begin to suggest items of interest for me. Web 3.0 aims to bring meaning to your search with relevant, meaningful results.

8.4 Plagiarism

What is plagiarism? Many people think of plagiarism as copying another's work or borrowing someone else's original ideas. But terms like "copying" and "borrowing" can disguise the seriousness of the offense. All of the following are considered as plagiarism:

- turning in someone else's work as your own
- copying words or ideas from someone else without giving credit
- failing to put a quotation in quotation marks
- giving incorrect information about the source of a quotation
- changing words but copying the sentence structure of a source without giving credit
- copying so many words or ideas from a source that it makes up the majority of your work, whether you give credit or not (see our section on "fair use" rules)

Most cases of plagiarism can be avoided, however, by citing sources. Simply acknowledging that certain material has been borrowed and providing your audience with the information necessary to find that source is usually enough to prevent plagiarism.

By the way, this information about plagiarism was taken from the site http://plagiarism.org/. If I did not tell you so then I would have plagiarised. Plagiarism software exists. This is capable of saying the approximate percentage of plagiarism is a text.