CAPACITARTE

Es ser líder de tu vida

Computer security

Computer security (Also known as cybersecurity or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from **unintended or unauthorized** access, change or destruction. Computer security also includes protection from unplanned events and natural disasters.

Security means allowing things you do want, while stopping things you don't want from happening. Parts of this include **authentication and validation** (making sure you are who you claim to be), **encryption** (making sure data gets where you want to go, without others being able to observe it) and **physical security**.

Authentication and and Validation

One method of authentication protection is passwords. A **password** or **watchword** is a form of authentication used to guard or control a "resource" (usually used to protect electronic data). Despite the name, a password is usually an alphanumeric (letters and numbers) phrase entered to grant a user access to data that he/she is only permitted access. A password with numbers could be better described as a "**passcode**". A good password is one that's hard to guess, yet easy to remember. No password is perfect, they can all be decrypted if given enough time. However, as the password encryption increase in size, the possible combination increases and makes it more difficult to break.

Another method of authentication is **Biometrics**. Biometrics is the science of measuring human physical or behavioral characteristics. It is used to identify and compare some specific people's characteristics such as voice, fingerprints, hand geometry, eye or facial characteristics.

Malware

Malware is any software specifically designed to damage a computer system without owner knowledge. The examples of malware are worms, viruses, Trojan horses and etc. Some normal computer users are unfamiliar with the term and never use it. Instead the term: "computer virus" is used. It describes all kinds of malware, though not all malware are viruses. It is short for “malicious software”.

Viruses

- A virus appears when there is a "deviant" program stored on a computer floppy disk, hard drive, or CD, that can cause unexpected and often undesirable effects such as destroying or corrupting data. An example of a virus was the "Love Bug" which started in the Philippines in May 2000 and caused approximately $10 billion in damage.

Trojan Horse

- It is program that is packaged with a useful application, usually free, such as a screen or game saver, but carries a destructive virus, that creates problems for your computer without your knowledge. Once the program initiates, the **camouflaged virus** is released creating havoc and mayhem. This virus is named after the mythical Trojan horse that was left as a gift to the Trojan people from the Achaeans as a trick. A trojan horse is one of the biggest threats to computer security as they cannot be identified easily.

Worms

- A worm is a type of malicious software that copies itself repeatedly into a computer memory (RAM) using up all available RAM. It also can copy on to a disk drive so it can load into RAM again. It spreads through a network to infect the RAM on other connected computers. A worm can infect your computer through email (the worm is disguised by pretending it came from somewhere it did not). When you open the email attachment the worm looks through your Windows Outlook and other address books choosing names at random. Using built-in software, the worm sends copies of itself to many names in the address books. It will take over ram on a computer and will take over ram on others computers that the original computer is **hooked up to**.

Adware

- It is used for advertising purposes. It works by automatically downloading an advertisement to a computer that is accessing a specific website. Although it is often legal and used by big companies and it can be used by illegitimate companies promoting pornography or gambling. In addition, Adware is often downloaded with software. This causes the advertisements to automatically **pop up** when the program is in use. Adware usually exploits the **cookie tracker** to monitor what sites you're going to and record your browsing habit for marketing purposes. Examples of Adware programs include Ad-Aware and Spybot Search & Destroy.

Spyware

- It is misleading software that is secretly installed on a computer through the web. Confidential information can be obtained by the installer such as passwords, keystrokes and email addresses. Too much spyware can slow down the operation of a computer

Web page can take over your Router

- Web Page can take over your Router by this way: The victim would visit a malicious Web page that would use JavaScript code to **trick** the browser into making changes on the Web-based router configuration page. The JavaScript could tell the router to let the bad guys remotely administer the device, or it could force the router to download new firmware, again putting the router under the hacker's control. The attacker would be able to control his victim's Internet communications.

The boot sector virus

- It replaces the boot instructions on the system software with its own. When the computer is booting this virus **sneaks into** the main memory before the OS. This then allows the virus to infect other files. Any diskette used on this computer becomes infected. When this disk is moved to another computer this contagion continues.

Macro virus

- It takes advantage of a task where miniature programs (a.k.a. macros) are rooted in regular data files (files made through emails, spreadsheets...) which are sent over computer networks. Example: a virus that hides in a power point presentation sent over email.

A logic bomb

- It appears when there is a piece of code that has been placed intentionally into a software system. When specific conditions are met (like a date or a certain combination of keys being pressed), this code will set off harmful activities within your computer. For example, a programmer may place a logic bomb in the software so that when he leaves the company he is working for, all the information on his computer will be destroyed.

Denial of Service (DOS)

- This happens when a webserver cannot handle all of the requests asked. It "can" happen legitimately when lots of people go to that website, but it usually happens because many computers have been **zombied** by a logic bomb virus to go to a specific website at the same time.

Physical security

There are Hardware and software mistakes which can affect computer security.

Line down (also known as "Data Down" or loss of data Prevention) is an example of computer problems which can affect your computer system security. In this case, you need to use various backup methods to ensure data is safe and a **disk redundancy** whereby you use multiple hard drives to ensure data safety.

Another example is **Power failure**, also known as power cut, power failure, power loss, or blackout. It is the loss of the electricity supply to an area, which can affect computer security. It is highly recommended the use of **UPSs** (uninterrupted power supply) which are high end power generating or backup power systems that don't allow a break in power.

Pentium bugs (errors) have the potential to crash Pentium computers and could be used for sabotage. The bug is apparently coded as a single illegal instruction and not something that would be deliberately coded into a software program.

A **software bug** (or just "bug") is an error, flaw or mistake in a computer program that prevents it from behaving as intended (for example: producing an incorrect result). Most bugs are from mistakes made by people in the program's source code or its design. Some are from compliers producing incorrect codes. Y2K bug is the most famous example of a software bug. Another famous software bug was found in the world famous video game POKEMON, the Missing bug allowed the gamer to surf around an island and receive free items for doing so. The original bug was actually a moth that was caught between relays. Bugs are a major concern as it opens up opportunities for intenders to exploit those bugs. Bugs are countered with updates and **patches** released by the software company to address those issues. That's why it's important to keep your OS up to date. Serious bugs can cause programs to **crash** or **freeze** leading to a denial of service.

A computer system is no more secure than the human systems responsible for its operation. **Malicious individuals** have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals, or by deliberately deceiving them, for example sending messages that they are the system administrator and asking for passwords. This deception is known as **Social engineering**. Social engineering and **direct computer access** (physical) attacks can only be prevented by non-computer means, which can be difficult to enforce, relative to the sensitivity of the information. Even in a highly disciplined environment, such as in military organizations, social engineering attacks can still be difficult to foresee and prevent.

Network security

Private networks can be attacked by intruders who attempt to obtain private personal information. To protect crucial data, companies hire security consultants who analyse the risks and provide solutions. The most common methods of protection are **passwords** for access control, **firewalls** and **encryption** and **decryption** systems. Encryption changes data into a secret code so that only someone with a key can read it. Decryption converts encrypted data back into its original form.

Internet Security

The Internet provide a wide variety of opportunities for communication, but unfortunately it has its dark side. Crackers (or black hat hackers) are computer criminals who use technology to perform a variety of crimes using emails or websites.

Cybercrimes

Cyber stalking,	when there is online harassment or abuse via chat rooms or newsgroups. Distribution of *indecent or offensive material*
Scam,	which is an email fraud to obtain money or valuable
Webjack,	which allows an individual to assume the owner ship of a web site domain name belonging to another person. By doing so, Hackers redirect users to their own website (related to pornography or gambling)
Piracy,	the illegal copy and distribution of copyrighted software, games or music files.

Theft of Intellectual Property,	pretending that someone else's work is your own. *Spreading of malicious software*
Phising (password harvest fishing),	getting passwords for online bank accounts or credit card numbers by using emails that look like they are from real organizations, but are in fact fake. People believe the message is from their bank and send their security details.
IP spoofing,	making one computer look like another in order to gain unauthorized access.

Security is crucial when you send **confidential information** online. For example, when you have to type your credit card number into an order form which passes from computer to computer on its ways to the online bookstore, if one of the intermediary computers is infiltrated by hackers, your data can be copied. To avoid risks, you should set all **security alerts** to high on your web browser. It displays **a lock** when the website is secure and allows you to **disable** or **delete cookies**. If you use online banking, make sure they use **digital certificates** (digital identification cards which identify users and webservers. Also be sure to use a browser that is compliant with **SSl** (Secure Sockets Layer), a protocol which provides secure transactions.

Email Security

To be protected when using your email account, you can take the following measures:

- You can obtain **spam filters** that spare the hassle of junk mail, ads etc. Spam can also be called "bulk e-mail" or "junk e-mail".
- You need to be alert against **Phishing**. It takes place when someone attempts to acquire sensitive information by asking to enter that information onto a website which they are stolen from, using highly advanced imitation websites (by stealing digital information), or simple messages like emails requesting bank information disguised as a desperate cry for financial help or a random donation from a wealthy individual.
- You also need to protect your computer against the next level of phishing, evil twin attack, **Wifi-phishing**. In this case, someone sets up a spot near your home

network - and then he/she logs onto your wireless network- in order to steal your private or personal information as you send it to a secure website.

Preventive tips for Computer Security

There follow some tips to protect computer systems:

- Don't open email attachments from unknown people, check the file extension.
- Run and update **antivirus programs.**
- Install a **firewall** (a program to prevent spyware from gaining access to the internal network).
- Make **backup copies** of your files regularly.
- Don't accept files from high-risk sources.
- Use a **digital certificate**, an electronic way of proving your identity, avoid giving credit card numbers.
- Don't believe everything you read on the Net. Have a suspicious attitude toward its contents.