# What is Computer Security?

By Lakshay Mor

Last updated on Jul 8, 20203792

https://www.simplilearn.com/what-is-computer-security-article

Technology is growing every day, and as it grows, it transforms our digital world. Internet use is increasing exponentially, making us correspondingly more vulnerable to cyber-attacks. By learning how cybercriminals attack and how to secure our systems and data against those attacks, you will be able to minimize the risk of data breaches and the devastation they bring with them.

Computer security deals with the protection of computer systems and information from harm, theft, and unauthorized use. The main reason users get attacked frequently is that they lack adequate defenses to keep out intruders, and cybercriminals are quick to exploit such weaknesses. Computer security ensures the confidentiality, integrity, and availability of your computers and their stored data.

The following topics will be covered in this article:

* Why do users get attacked?
* Types of attacks
* What to secure?
* How do you secure your computer?

**Why Do Users Get Attacked?**

Before getting into how to secure data from breaches, we must try to understand the motives behind these attacks. By knowing the motives behind the attacks, it’s easy for cybersecurity professionals to secure the systems. The main motives for attacking an organization’s or individual’s computer are:

* Disrupting a business’ continuity: If a business is disrupted, it causes great harm to the organization in the form of lost profits, fraud, and damage to its reputation.
* Information theft and manipulating data: Hackers take confidential information that they steal from organizations and sell it to individuals or groups on the black market.
* Creating chaos and fear by disrupting critical infrastructure: Cyber terrorists attack a company or a government body to disrupt their services, doing damage that can potentially affect an entire nation.
* Financial loss to the target: Hackers attack an organization or business and disrupt their services in such a way that the target has to allocate substantial funds to repair the damage.
* Achieving a state’s military objectives: Rival nations continuously keep an eye on each other and sometimes employ cybercriminal tactics to steal military secrets.
* Demanding ransom: The hackers employ ransomware to block a website or servers, releasing control only after a ransom is paid.
* Damaging the reputation of target: The hacker may have personal reasons to attack an organization or individual so that their reputation suffers.
* Propagating religious or political beliefs: Hackers may infiltrate websites to promote religious dogma or a certain political agenda, usually to sway voters to vote a certain way.

**Types of Attacks**

There are many kinds of attacks available to the dedicated hacker. These are among the most famous and frequent types of attacks.

1. Denial of service (DDoS): This is an attack used to restrict the user’s access to the system resources by flooding the server with useless traffic. The botmaster commands all the bots to access a resource at the same time so that the resource gets hopelessly jammed up. Then, if a legitimate user wants to access that same resource, they will not be able to do so.

2. Malware attack: This is a malicious program that disrupts or damages the computer. There are four main types of malware:

* Keylogger: Keylogger records all the hits on the targeted keyboard. Most hackers use it to get passwords and account details.
* Virus: A computer virus is a malicious code that replicates by copying itself to another program or document and changes how a computer works. The virus, such as the Melissa virus, requires someone to knowingly or unknowingly spread the infection without the knowledge or permission of a user or system administrator.
* Worms: This is a standalone program that runs independently and infects the system. One of the more popular examples is W32.Alcra. F. The worm propagates itself through network share devices.
* Trojan horse: This is a malicious code that takes over your computer. This code can damage or steal information from your computer.

3. Man in the middle: Say, for example, you want to do an online transaction. You connect to your bank and conduct the payment. Simple, right?

Now, while you are doing a transaction, you have to enter the details of your card and the PIN. The cyber attacker spoofs you and monitors your transaction. As soon as you enter your details, he will have access to all of that information, as shown in the below image:

4. Phishing: The attacker sends bait, often in the form of an email. It encourages people to share their details.

If someone is a customer of ABC bank, he would probably open the link and enter the details. But these kinds of emails are always phishing. Banks do not send emails like this.

5. Eavesdropping: Attacker observes traffic on your system and the work you are doing. The attacker can monitor you in three ways:

* Email monitoring
* Which websites you visit
* What items you download

6. SQL injection: As the name suggests, an SQL injection vulnerability allows an attacker to inject malicious input into a SQL statement. This type of attack happens only on websites. The best example would be www.facebook.com. There is a database stored on the facebook website. The hackers get into that database and sign in using someone else's username and password.

7. Password attack: To crack a password or find a password, hackers employ these following techniques:

* Dictionary attack: In this method, they handle every password that is possible through the dictionary
* Brute force: It is a trial and error method used to decode the password or data. This attack takes the most amount of time.
* Keylogger: As the name suggests, keylogger records all the hits on the keyboard. Most people use it to get passwords and account details
* Shoulder surfing: The attackers observe the user’s keyboard by looking over the user’s shoulder.
* Rainbow table: There are rainbow tables that contain precomputed hash values. Attackers use this table to find the user’s password.

8. Social engineering: Attackers create social situations that encourage you to share your password. For example, let’s say that you are out of your office, and you get a call. The person says that he is from the IT department and they have found out that your system has been compromised. He asks you to share your password. You might believe him and share your password. However, the caller was, in fact, a hacker, and now he has your password. Now that he has access, he can compromise your organization's data. The best way to avoid the effects of social engineering is to learn your organization’s protocol regarding password sharing.

**What to Secure?**

The security of any organization starts with three principles: confidentiality, integrity, and availability. This is called CIA (no relation to the American spy organization!). CIA has served as the industry standard for computer security since the advent of the first mainframes.

* Confidentiality: The principles of confidentiality assert that information and functions can be accessed only by authorized parties. Example: military secrets.
* Integrity: The principles of integrity assert that information and functions can be added, altered, or removed only by authorized people and means. Example: incorrect data entered by a user in the database.
* Availability: The principles of availability assert that systems, functions, and data must be available on-demand according to agreed-upon parameters based on levels of service.

**How Do You Secure Your Computer?**

1. Two-way authentication: Two-factor authentication adds a layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts. For example, when you make online payments, you first have to confirm your card’s cvv number, then you undergo a second confirmation by providing your mobile number.

2. Secure passwords: Create strong passwords so that no one will be able to hack or guess your password. The best passwords include:

* At least 15 characters.
* Capital letters.
* Special characters. Example: @#$%.
* Numbers.

3. Regular updates: Always keep your system and all its software updated. Many updates contain additional defenses against cyber-attacks.

4. Antivirus: Antivirus is a computer program used to prevent, detect, and remove malware. Examples of antivirus include Norton, Quickheal, and McAfee.

5. Firewalls: Firewalls prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.

6. Anti-phishing tactics: When you get an email that looks suspicious or has no relation to you, then do the following:

* Do not click on the link in the email.
* Do not provide any personal details if asked.
* Do not open the attached files.

7. Encryption: This is the process of converting ordinary plain text into unintelligible text and vice-versa. Encryption is used in many applications like:

* Banking transactions.
* Computer passwords.
* E-commerce transactions.

Unfortunately, cybercrime is increasing daily, so it’s imperative to have a solid grasp of the best cybersecurity practices. While the internet is transforming and improving our lives, the vast network and its associated technologies have become a lucrative hunting ground for a growing number of cybercriminals, agents from which individuals and businesses must protect themselves.

SQL – Structured Query Language, an international standard for database manipulation –

язык структурированных запросов, язык SQL

hash value - значение хеш-функции

CVV = Card Verification Value

• Rainbow table - радужная таблица - (mathematics) - а table of surjective functions used to decrypt a text that was coded using a hash table