**What is Cybersecurity?**

Cybersecurity is the practice of protecting systems, networks, and programs from cyberattacks by malicious actors that are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

**What is a Cyberattack?**

A cyberattack is any type of offensive action that targets computer information systems, infrastructures, computer networks or personal computer devices, using various methods to steal, alter or destroy data or information systems.

**Few Common Cyberattacks:**

* Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks.
* Man-in-the-middle (MitM) attacks.
* Phishing and Spear Phishing attacks.
* Sql Injection attacks.
* Malware attacks.

1. **DoS and DDoS Attacks:**

**DoS:** In computing, a denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by sending a massive amount of traffic to a victim’s computer, temporarily or indefinitely disrupting services of a host connected to the Internet.

**DDoS:** DDoSattack involves multiple connected online devices, collectively known as a botnet, which are used to overwhelm a target website with fake traffic. This attack is carried out on a large scale usually by hacking groups. Example: Anonymous Group (Search about them on Internet, they’re very famous!!)

1. **Man In The Middle Attack:**

man-in-the-middle (MitM) attack is a type of cyberattack in which the attacker secretly intercepts and relays messages between two parties who believe they are communicating directly with each other. The attack is a type of eavesdropping in which the attacker intercepts and then controls the entire conversation.

1. **Phishing and Spear Phishing Attacks:**

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

1. **SQL Injection Attacks:**

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details.

1. **Malware Attacks:**

A malware attack is a common cyberattack where malware (normally malicious software) executes unauthorized actions on the victim's system. The malicious software (a.k.a. virus) encompasses many specific types of attacks such as ransomware, spyware, command and control, and more.

(Here I you want you can talk about the most infamous ransomware attack WANNACRY)

<https://en.wikipedia.org/wiki/WannaCry_ransomware_attack> (Click Here)

**Methods to Prevent against Cyberattacks:**

1. **Multi-Factor Authentication:** Implement multi-factor authentication (like 2FA) on your accounts and make it significantly less likely you’ll get hacked.
2. **Choosing a Strong Password:** Use strong passwords, and ideally a password manager to generate and store unique passwords. Never use the same password for all your accounts. Having the same password setup for everything can be dangerous. Once a hacker figures out your password, they now have access to everything in your system and any application you use. **Having different passwords setup for every application you use is a real benefit to your security,** and changing them often will maintain a high level of protection against external and internal threats.
3. **Employee awareness is vital:** One of the most common ways cyber criminals get access to your data **is through your employees.** They’ll send fraudulent emails impersonating someone in your organisation and will either ask for personal details or for access to certain files. Links often seem legitimate to an untrained eye and it’s easy to fall into the trap.
4. **Keep your Software and System fully up to date:** Often cyberattacks happen**because your systems or software aren’t fully up to date, leaving weaknesses.** So cybercriminals exploit these weaknesses to gain access to your network. Once they are in – it’s often too late to take preventative action.
5. **Install a Firewall: Putting your network behind a firewall is one of the most effective ways to defend yourself from any cyberattack.** A firewall system will block any brute force attacks made on your network and/or systems before it can do any damage.
6. **Data Backup is a good practice:** In the event of a cyberattack (or any disaster)**you must have your data backed up to avoid serious downtime, loss of data and serious financial loss.**
7. **Control Access to your Systems: one of the attacks that you can receive on your systems can be physical, having control over who can access your network is really important.**Somebody can simply walk into your office or enterprise and plug in a USB key containing infected files into one of your computers allowing them access to your entire network or infect it. **Having a perimeter security system installed is a very good way to stop cybercrime as much as break ins!**
8. **Securing Wi-Fi: Securing your Wi-Fi networks and hiding them is one of the safest things you can do for you systems.** With wireless technology developing more and more everyday there’s thousands of devices that can connect to your network and compromise you.
9. **Employee Personal Accounts: In almost all businesses every employee needs their own login for every application and program.** Several users connecting under the same credentials can put your business at risk. Having separate logins for each staff member will help you reduce the number of attack fronts. Users only log in once each day and will only use their own set of logins.
10. **Be Aware of Phishing Attacks:** Phishing is a cyberattack that involves the use of camouflaged email. The aim is to trick you as a customer to believe that the message is important like a request from a bank, and you may be needed to click a link or download an attachment. Phishing attackers pretend to be a trusted entity of certain nature, mostly a real or imitates a real person or an organization you are doing business with.