Cyber Threats

Module 2

CONTENTS

- What are Cyber Security Threats?
- Common Sources of Cyber Threats,
- Types of Cyber security
- Threats-Malware attacks,
- Social Engineering attacks,
- Supply chain attacks,
- Man-in-the middle Attack,
- Threat Detection Tools,
- Cyber Defense for Individuals.

Introduction

- The internet in India is growing rapidly. It has given rise to new opportunities in every field we can think of— be it entertainment, business, sports or education.
- There are two sides to a coin. Internet also has its own disadvantages. One of the major disadvantages is Cyber crime — illegal activity committed on the internet

- Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access.
- It requires an understanding of potential information threats, such as viruses and other malicious code.
- Effective cyber security reduces the risk of cyber attacks, and protects organizations and individuals from the unauthorized exploitation of systems, networks and technologies.

- Cyber security is important because government, corporate and medical organizations collect, process and store unprecedented amounts of data on computers and other devices.
- The core functionality of cybersecurity involves protecting information and systems from major cyberthreats.
- Some of the common threats are outlined below in more detail:
- Cyber terrorism
- Cyber warfare
- Cyber espionage

- Cyber terrorism - The disruptive use of information technology by terrorist groups to further their ideological or political agenda. This takes the form of attacks on networks, computer systems and telecommunication infrastructures.
- Cyber warfare - It involves nation-states using information technology to penetrate another nation's networks to cause damage or disruption.
- Cyber espionage - It is the practice of using information technology to obtain secret information without permission from its owners or holders.

The key concept of cyber security

- The cyber security on a whole is very broad term but is based on three fundamental concepts known as "The CIA triad"

- Confidentiality:- ensures that data exchanged is not accessible to unauthorized users. The users could be applications, processes, other systems and/or humans

- Integrity:- is the ability to ensure that a system and its data has not suffered unauthorized modification. Integrity protection protects not only data, but also operating systems, applications and hardware from being altered by unauthorized individuals.

- Availability:- Availability guarantees that systems, applications and data are available to users when they need them. The most common attack that impacts availability is denial-of-service in which the attacker interrupts access to information, system, devices or other network resources.

Cyber Threats

- A Cyber threat is any malicious act that attempts to gain access to a computer network without authorization or permission from the owners.
- It refers to the wide range of malicious activities that can damage or disrupt a computer system, a network or the information it contain.
- Most common cyber threats: Social Engineered Trojans, Unpatched Software, Phishing, Network worms, etc.

Sources of Cyber Threats

Cyber threats can come from a wide variety of sources, some notable examples include:

- National governments.
- Terrorists.
- Industrial secret agents.
- Rogue employees.
- Hackers.
- Business competitors.
- Organization insiders.

- Nation states—hostile countries can launch cyber attacks against local companies and institutions, aiming to interfere with communications, cause disorder, and inflict damage.
- Terrorist organizations—terrorists conduct cyber attacks aimed at destroying or abusing critical infrastructure, threaten national security, disrupt economies, and cause bodily harm to citizens.

- Criminal groups—organized groups of hackers aim to break into computing systems for economic benefit. These groups use phishing, spam, spyware and malware for extortion, theft of private information, and online scams.
- Malicious insiders—an employee who has legitimate access to company assets, and abuses their privileges to steal information or damage computing systems for economic or personal gain. Insiders may be employees, contractors, suppliers, or partners of the target organization. They can also be outsiders who have compromised a privileged account and are impersonating its owner.

Impacts of Cyber Attacks

A successful cyber attack can cause major damage to organizations or systems, as well as to business reputation and consumer trust.

Some potential results include:

- Financial loss. –
- Direct theft: Cybercriminals can directly steal money from bank accounts or use stolen credit card details for fraudulent transactions.
- Ransomware: Attacks where attackers encrypt critical data and demand payment to restore access, leading to significant financial losses and operational disruption.

- Reputational damage.
- Loss of customer trust: When sensitive customer data is compromised, customers may lose trust in the company, leading to decreased business.
- Negative publicity: News of a cyber attack can generate negative press, damaging the company's image and brand reputation.
- Impact on stakeholder relations: Investors and business partners may lose confidence in a company with poor cybersecurity practices.

- Legal consequences.
- Data privacy laws: Companies can face lawsuits from individuals whose personal data is compromised in a breach, depending on the jurisdiction and applicable data protection laws.
- Non-compliance penalties: Failure to adhere to cybersecurity regulations can result in significant fines from regulatory bodies.
- Class-action lawsuits: In some cases, large groups of affected individuals may file class-action lawsuits against a company following a data breach.


Types of Cyber Security Threats
Spyware
Malware
Computer Viruses
Phishing
Data Breaches

Types of Cyber Threats

- Phishing attack
- SQL Injection threat
- Man-in-the-middle attack
- Malware
- Zero-day attack
- Cross-site-scripting
- Advanced persistent threats
- Password attack
- Drive by attack

Phishing Attack

- Phishing is the technique to steal a user's data from the internet or computer-connected device.
- Types of Phishing attacks
  - **Phishing Email**: when cybercriminals send deceptive emails that appear to be from legitimate sources like banks, social media platforms, or government agencies.
  - **Domain spoofing**: when cyber criminals fake a website name or email domain to try to fool users.
  - **Voice phishing**: or Vishing is the use of fraudulent phone calls to trick people into giving money or revealing personal information.

Phishing Attack

- **SMS phishing**: Smishing involves fraudulent SMS messages designed to steal user information by urging them to click on malicious links or call fake customer service numbers.
- **Clone phishing**: distributed email containing attachments of links
- **Typo squatting**: For example → tailspintoy.com instead of tailspintoys.com
- **Evil Twin**: a fake Wi-Fi network is set up to steal information or further infiltrate a connecting device.
- **Whale phishing**: Whale Picking, a victim to share highly sensitive information or send a wire transfer to a fraudulent account

Phishing Attack

Ways to prevent Phishing attack:

- Know what a phishing scam looks like
- Don't click on a random link
- Get free anti-phishing add-ons
- Don't give your information to an unsecured site
- Change passwords regularly
- install firewall

SQL injection threat

- Injection attacks exploit a variety of vulnerabilities to directly insert malicious input into the code of a web application.
- Successful attacks may expose sensitive information, execute a DoS attack or compromise the entire system.
- In the SQL injection threat, the attacker sends malicious query to the device or a server. The server is then forced to expose sensitive information.
- A new variant on this attack is NoSQL attacks, targeted against databases that do not use a relational data structure.

- Ways to prevent SQL injection threat:-
  - **Validate user inputs**: ensures that only expected data types and values are accepted
  - **Sanitize data by limiting special characters**: Attackers often inject SQL commands using special characters like ', --, and ;. Sanitizing inputs removes or escapes these characters.
  - **Use stored procedures in the database**: precompiled SQL statements that reduce direct interaction with user inputs.
  - **Establish appropriate privileges and strict access control**: Grant database users only the necessary permissions to limit the impact of SQL injection.

Man-in-the-middle attack

The man-in-the-middle attack is a security breach where cybercriminals place themselves between the communication system of a client and the server.

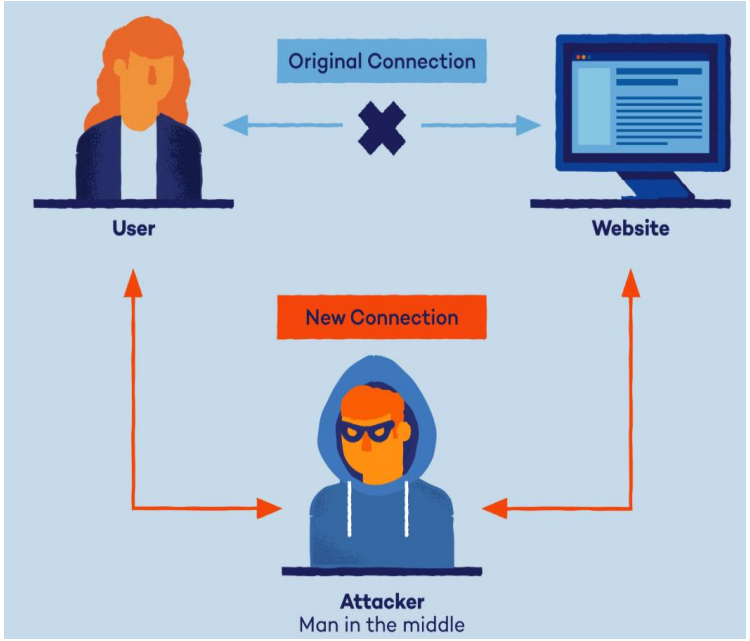
Types of Man-in-the-middle attack

- **Session hijacking**: gain the access of a target's computer or online account and exploit the whole web session control mechanism.
- **IP Spoofing**: intruder sends message to a computer system with an IP address indicating message is coming from a different IP address than its actually coming from.
- **Replay**: a type of network attack in which an attacker captures a valid network transmission and then re-transmit it later.

Man-in-the-middle attack

Ways to prevent Man-in-the-middle attack

- Strong router login credentials
- Virtual private network
- Strong encryption on access points

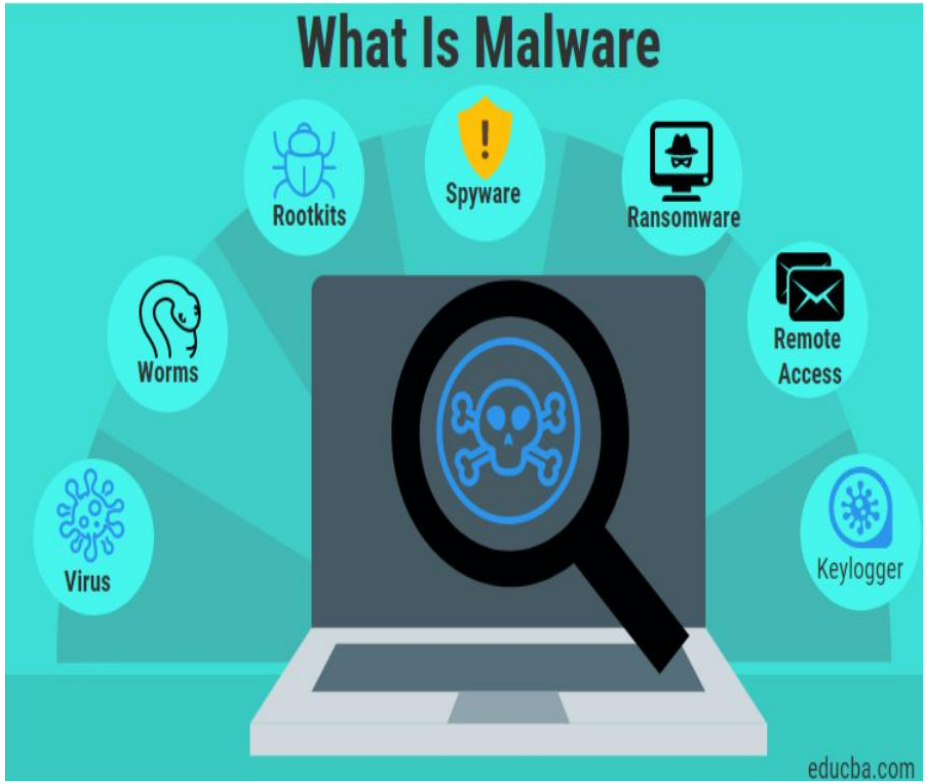


Malware

Malware is a malicious software which gets installed into the system when the user clicks on a dangerous link or an email.

Types of Malware:

- **Viruses**: replicates itself by modifying other computer programs
- **Trojans**: downloads onto a computer disguised as a legitimate program.
- **Worms**: to self-replicate and infect other computers while remaining active on infected systems
- **Ransomware**: permanently block access to the victim's personal data unless a ransom is paid

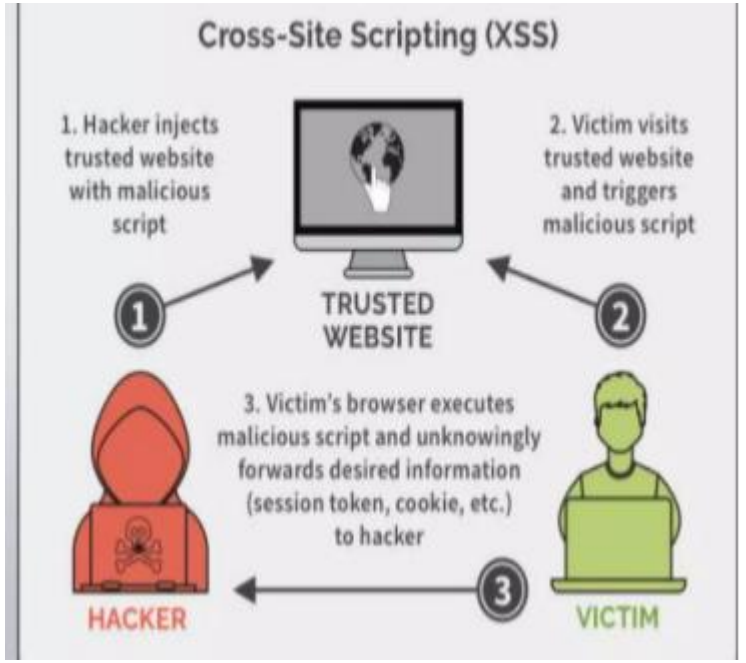


Ways to prevent Malware:

- Regularly update your computer and software
- Be careful while opening unknown email attachments or images

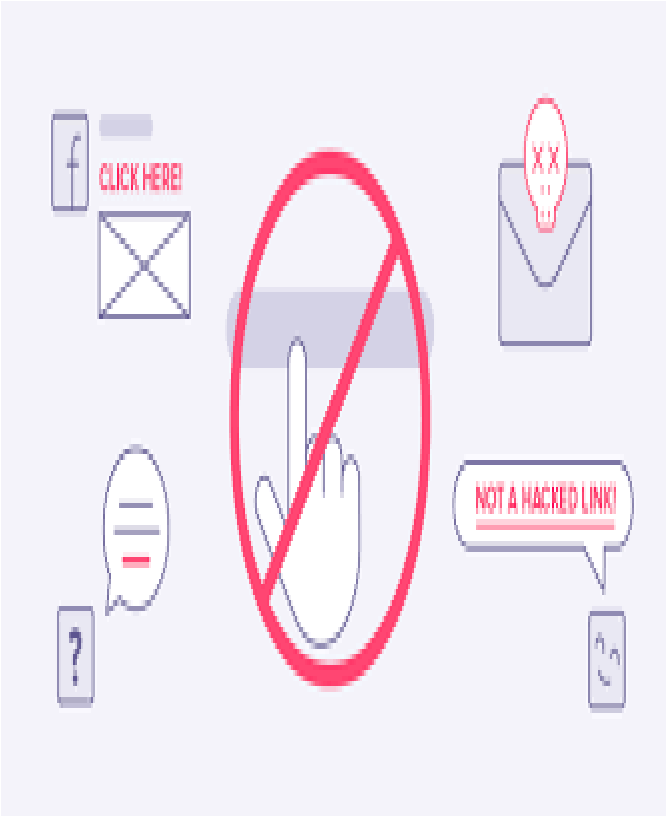
Cross-site scripting

- Cross-site scripting is a cyber-attack where an attacker sends malicious code to a reputable website



Ways to prevent Cross-site-scripting:-

- Filter input on arrival.
- Encode data on output.
- Use appropriate response headers.
- Content security policy.



Advanced persistent threat

- An advanced persistent threat occurs when an attacker gains unauthorized access to a system or network and remains undetected for a long duration

Ways to prevent Advanced persistent threats:-

- Install a firewall
- Enable a web application firewall
- Install an antivirus
- Implement intrusion prevention systems

Password attacks

- Password attack is an attempt to steal passwords from a user.

Two common techniques used to get user's password

- Brute-force guessing - Brute-force guessing attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.
- Dictionary attack - a type of brute force attack where hackers try to guess a user's password to their online accounts by quickly running through a list of commonly used words, phrases, and number combinations.

Ways to prevent Password attack

- Use strong password
- Multi-factor authentication- MFA: For example, along with the password, users might be asked to enter a code sent to their email, answer a secret question, or scan a fingerprint.

Social Engineering Attacks

- Social engineering is the term used for a broad range of malicious activities accomplished through human interactions.
- It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
- Social engineering attacks happen in one or more steps.
- The attacker first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack.
- Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

Social Engineering Attack Lifecycle

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Closing the interaction,
ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

Social engineering attack techniques

- Baiting - As its name implies, baiting attacks use a false promise to provoke a victim's greed or curiosity. They lure users into a trap that steals their personal information or inflicts their systems with malware.
- Scareware - Scareware involves victims being bombarded with false alarms and fictitious threats. Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit or is malware itself.

- Pretexting - Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by an attacker pretending to need sensitive information from a victim so as to perform a critical task.
- Phishing

Social engineering prevention

- Don’t open emails and attachments from suspicious sources
- Use multifactor authentication
- Be wary of tempting offers
- Keep your antivirus/antimalware software updated

Supply Chain Attacks

- A supply chain is the network of people, organizations, and technology involved in making and selling a product.
- A supply chain attack is a cyberattack that targets a company's supply chain to steal data or disrupt operations.
- A supply chain attack uses third-party tools or services — collectively referred to as a ‘supply chain’ — to infiltrate a target’s system or network.
- These attacks are sometimes called “value-chain attacks” or “third-party attacks.”

- In a supply chain attack, an attacker might target a cybersecurity vendor and add malicious code (or ‘malware’) to their software, which is then sent out in a system update to that vendor’s clients.
- When the clients download the update, believing it to be from a trusted source, the malware grants attackers' access to those clients’ systems and information.

- Before a supply chain attack can be carried out, attackers need to gain access to the third-party system, application, or tool they plan to exploit.
- This may be done by using stolen credentials, targeting vendors with temporary access to an organization's system, or exploiting an unknown software vulnerability, among other methods.
- Once access to this third-party dependency has been secured, the attack that reaches the ultimate target, often via their browser or device — can be carried out in a variety of ways.

Types of Supply Chain Attacks

Supply chain attacks may target hardware, software, applications, or devices that are managed by third parties. Some common attack types include the following:

- Browser-based attacks: run malicious code on end-user browsers.
- Software attacks: disguise malware in software updates.
- Open-source attacks exploit vulnerabilities in open-source code.

Supply Chain Attacks Prevention

- Organizations typically work with a variety of outside vendors, each of whom may use dozens of dependencies in their tools and services.
- Run a third-party risk assessment: This may include testing third-party software prior to deployment, requiring vendors to adhere to specific security policies
- Implement Zero Trust: Zero Trust ensures that every user — from employees to contractors and vendors — is subject to continuous validation and monitoring inside an organization's network. Verifying user and device identity and privileges helps ensure that attackers cannot infiltrate an organization simply by stealing legitimate user credentials

- Use malware prevention: Malware prevention tools, like antivirus software, automatically scan devices for malicious code in order to prevent it from executing.

Zero Day Exploit/ Attack

- "Zero-day" is a broad term that describes recently discovered security vulnerabilities that hackers can use to attack systems.
- The term "zero-day" refers to the fact that the vendor or developer has only just learned of the flaw – which means they have “zero days” to fix it.
- A zero-day attack takes place when hackers exploit the flaw before developers have a chance to address it.

- Software often has security vulnerabilities that hackers can exploit to cause havoc.
- Software developers are always looking out for vulnerabilities to "patch" – that is, develop a solution that they release in a new update.
- However, sometimes hackers or malicious actors spot the vulnerability before the software developers do.
- While the vulnerability is still open, attackers can write and implement a code to take advantage of it. This is known as exploit code.

Detection strategies of 0 day attack

Some of the zero-day detection techniques include:

- Using existing databases of malware and how they behave as a reference.
- Alternatively, some techniques look for zero-day malware characteristics based on how they interact with the target system. Rather than examining the code of incoming files, this technique looks at the interactions they have with existing software and tries to determine if they result from malicious actions.
- Increasingly, machine learning is used to detect data from previously recorded exploits to establish a baseline for safe system behavior based on data of past and current interactions with the system.

Prevention against 0-day exploits

- Keep all software and operating systems up to date.
- Use only essential applications.
- Use a firewall.
- Within organizations, educate users.
- Use of antivirus software solution.

Threat of a Vulnerability

- A vulnerability is a future threat to an organization's security. If an attacker identifies and exploits the vulnerability, then the costs to the organization and its customers can be significant.
- Identifying vulnerabilities before they are exploited by an attacker is a much more cost-effective approach to vulnerability management.
- The sooner that vulnerabilities are identified and remediated in the Software Development Lifecycle (SDLC), the lower the cost to the organization.

Threat Detection and Response (TDR)

- Threat detection and response is a cybersecurity process for identifying cyberthreats to an organization's digital assets and taking steps to mitigate them as quickly as possible.
- To address cyberthreats and other security issues, many organizations set up a security operations center (SOC), which is a centralized function or team responsible for improving an organization's cybersecurity posture and preventing, detecting, and responding to threats.
- In addition to monitoring and responding to ongoing cyberattacks, a SOC also does proactive work to identify emerging cyberthreats and organizational vulnerabilities.
- Most SOC teams, which may be onsite or outsourced, operate around the clock, seven days a week.

Threat detection and response typically includes the following stages:

1. **Detection**. Security tools that monitor endpoints, identities, networks, apps, and clouds help surface risks and potential breaches.
2. **Investigation**. Once a risk is identified, the SOC uses AI and other tools to confirm the cyberthreat is real, determine how it happened, and assess what company assets are affected.
3. **Containment**. To stop the spread of a cyberattack, cybersecurity teams and automated tools isolate infected devices, identities, and networks from the rest of the organization's assets.
4. **Eradication**. Teams eliminate the root cause of a security incident with the goal of evicting the bad actor completely from the environment. They also mitigate vulnerabilities that may put the organization at risk of a similar cyberattack.

5. **Recovery**. After teams are reasonably confident that a cyberthreat or vulnerability has been removed, they bring back any isolated systems online.
6. **Report**. Depending on the severity of the incident, security teams will document and brief leaders, executives, and/or the board on what happened and how it was resolved.
7. **Risk mitigation**. To prevent a similar breach from happening again and to improve response in the future, teams study the incident and identify changes to make to the environment and processes.

What is Cyber Defence ?

- As cyber attacks continue to rise in size, frequency, and complexity, cyber defense is one of the most integral and difficult pieces of any organization's cybersecurity strategy.
- Cyber defense is a coordinated act of resistance that guards information, systems, and networks from cyber attacks by implementing protective procedures such as firewalls, network detection and response (NDR), endpoint detection and response (EDR) to identify, analyze, and report incidents that occur within a network.
- Still, cyber defense teams are faced with a near impossible task of securing all an organization's vulnerabilities, and a big part of that means being able to deeply understand the tactics, capabilities, and motives of attackers.

How has cyber defence evolved ?

- The beginning of cyber attacks can be traced back to the early 1970s when the first computer worm, CREEPER, was released on the ARPANET.
- It was quickly followed by REAPER, the first antivirus software, paving the way for the much more sophisticated cyber defense we know today.
- As the internet became a ubiquitous part of our daily lives, cyber defense has needed to move at breakneck speed just to keep up.

- But with each new defense, the enemy created a way around it.
- After CREEPER, hackers moved beyond simple worms to more advanced, more sinister malware such as polymorphic viruses, phishing schemes, ransomware, and zero-day attacks.
- And with each followed more effective cyber defenses such as commercial antivirus software, firewall technology, and, more recently, end-point detection and network detection and response.

Cyber Defence vs. cybersecurity

- Cybersecurity and cyber defense often get used synonymously. While they are related, there are distinct, important differences.
- Cybersecurity is a set of solutions or strategies an organization employs to avoid danger and threats in cyberspace.
- Cyber threat defense is a key component of any cybersecurity strategy, which should incorporate cyber offense, compliance, and more. Cyber defense solutions focus on actively resisting an attack.

Some common cyber defense activities:

- Installing and maintaining the hardware and software for your security infrastructure.
- Analyzing, identifying, and patching system vulnerabilities within your network.
- Implementing real-time solutions to diffuse zero-day attacks.
- Recovering from partially or fully successful attack campaigns.

Cyber Defence Matrix

- The Cyber Defense Matrix helps cyber defense teams understand a wide range of cybersecurity practices by following a clearly defined structure to discern multiple cybersecurity tools to meet their security needs.
- The matrix has two main components aligned vertically and horizontally on a 5-by-5 grid.
- The first is the NIST Cybersecurity Framework's five operational functions: identify, protect, detect, respond, and recover.
- The second component centers on the assets cyber defense teams need to secure: devices, apps, networks, data, and users.

	Identify	Protect	Detect	Respond	Recover
Devices	○	○	○	○	○
Apps	○	●	○	●	○
Networks	○	○	●	○	●
Data	●	○	○	○	●
Users	○	○	○	○	●

Conclusion

- Cyber threats continue to evolve, requiring constant vigilance and proactive defense strategies.
- Understanding various cyber threats—malware, phishing, supply chain attacks, and zero-day exploits—is crucial for prevention.
- Effective cybersecurity measures include strong authentication, encryption, regular updates, and user awareness training.
- Organizations must implement multi-layered defenses, including intrusion detection, endpoint security, and cyber intelligence.
- A combination of technological solutions and human awareness is key to mitigating cyber risks.
- "Cybersecurity is not a one-time solution but an ongoing process of adaptation and resilience."