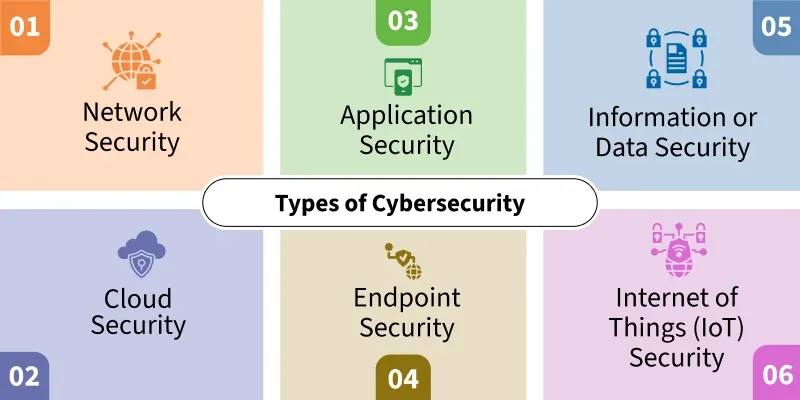
**CYBERSECURITY**

* **Cybersecurity** is the practice of protecting digital devices, networks, and sensitive data from cyber threats such as hacking, malware, and phishing attacks."
* It involves a range of strategies, technologies, and best practices designed to safeguard computers, networks, and data from **cyberattacks.**
* Cybersecurity involves using specialised tools to detect and remove harmful software while also learning to identify and avoid online scams.
* Practising good cybersecurity habits helps keep your data private and ensures a safe online experience.
* It's also referred to as **Information Security (INFOSEC), Information Assurance (IA),** or **System Security.**
* Cyberattacks happen every day worldwide, and without basic protection, anyone, individuals or companies, can become a victim. That’s why understanding cybersecurity is as important as locking your house.
* A key part of cybersecurity is [**encryption**](https://www.geeksforgeeks.org/computer-networks/what-is-data-encryption/), which keeps sensitive information private and accessible only to authorised users. It’s vital for protecting financial transactions, personal messages, and corporate data from theft or misuse.
* In short, cybersecurity keeps your online world safe by ensuring your information stays confidential, secure, and only available to the right people

# **Types of Cybersecurity**

There are seven types of cyber security, each explained below in detail with uses and functions:



**1. Network Security**

* It focuses on securing **computer networks** from unauthorized access, data breaches, and other network-based threats.
* This involves implementing technologies such as [**Firewalls**](https://www.geeksforgeeks.org/computer-networks/introduction-of-firewall-in-computer-network/), [**Intrusion detection systems** (IDS)](https://www.geeksforgeeks.org/ethical-hacking/intrusion-detection-system-ids/), **Virtual private networks** (VPNs), and **Network segmentation** as well as deploying [antivirus software](https://www.geeksforgeeks.org/computer-science-fundamentals/what-is-antivirus-software/)
* Using public Wi-Fi in locations like cafes and malls poses significant security risks. Malicious actors on the same network can potentially intercept your online activity, including sensitive information.
* If you use payment gateways on these unsecured networks, your financial data could be compromised because these open networks don’t have proper **security layers**, which means anyone—even hackers—can watch what you're doing online.
* So, use a **secure private network** or **VPN** to protect your **internal network** from outside threats

**2. Application Security**

* Concerned with **securing software applications** and preventing vulnerabilities that attackers could exploit.
* It involves secure coding practices, regular software updates and patches, and application-level firewalls.
* Most of the Apps that we use on our cell phones are secured and work under the rules and regulations of the Google Play Store.
* There are 3.553 million applications in Google Play, Apple App Store has 1.642 million, and Amazon App Store has 483 million available for users to download. With so many choices, it’s easy to assume all apps are safe—but that’s not true.
* Some apps pretend to be secure, but once installed, they collect personal data and secretly share it with third-party companies.
* The app must be installed from a trustworthy platform, not from some 3rd party website in the form of an APK (Android Application Package).

**3. Information or Data Security**

* Focuses on protecting sensitive information from unauthorized access, disclosure, alteration, or destruction.
* It includes **Encryption**, **Access controls**, **Data classification**, and **Data loss prevention (DLP) measures**.
* Incident response refers to the process of detecting, analyzing, and responding to security incidents promptly.
* Promoting security awareness among users is essential for maintaining information security. It involves educating individuals about common security risks, best practices for handling sensitive information, and how to identify and respond to potential threats like phishing attacks or social engineering attempts.
* Encryption is the process of converting information into an unreadable format (ciphertext) to protect it from unauthorized access.

**4. Cloud Security**

* It involves securing data, applications, and infrastructure hosted on cloud platforms, and ensuring appropriate access controls, data protection, and compliance.
* It uses various cloud service providers such as [**AWS**](https://www.geeksforgeeks.org/devops/aws-tutorial/), [**Azure**](https://www.geeksforgeeks.org/devops/microsoft-azure/), [**Google Cloud**](https://www.geeksforgeeks.org/devops/google-cloud-platform-tutorial/), etc., to ensure security against multiple threats.
* Cloud-based data storage has become a popular option over the last decade. It enhances privacy if configured and managed correctly and saves data on the cloud, making it accessible from any device with proper authentication.
* These platforms offer free tiers for limited usage, and users must pay for additional storage or services
* It is a cloud service provider that offers a wide range of services, including storage, computing, and security tools.

**5. Endpoint Security**

* Refers to securing individual devices such as computers, laptops, smartphones, and IoT devices.
* It includes antivirus software, intrusion prevention systems (IPS), device encryption, and regular software updates.
* **Antivirus**and [**Anti-malware**](https://www.geeksforgeeks.org/general-knowledge/what-is-anti-malware/)software that scans and detects malicious software, such as [**Viruses**](https://www.geeksforgeeks.org/ethical-hacking/what-is-a-computer-virus/), [**Worms**](https://www.geeksforgeeks.org/ethical-hacking/what-is-computer-worm/), **Trojans**, and **Ransomware**. These tools identify and eliminate or quarantine malicious files, protecting the endpoint and the network from potential harm.
* Firewalls are essential components of endpoint security. They monitor and control incoming and outgoing network traffic, filtering out potentially malicious data packets.
* Keeping software and operating systems up to date with the latest security patches and updates is crucial for endpoint security.

**6. Operational Security**

* Refers to the processes and policies organizations implement to protect sensitive data from internal threats and human errors.
* It involves access controls, risk management, employee training, and monitoring activities to prevent data leaks and security breaches.
* **Access Controls** ensure that only authorized personnel can access critical systems and sensitive information. This includes role-based access, [multi-factor authentication (MFA)](https://www.geeksforgeeks.org/computer-networks/multifactor-authentication/), and least privilege principles.
* **Risk Management** involves identifying, analyzing, and mitigating security risks within an organization. It includes regular security assessments, [vulnerability testing](https://www.geeksforgeeks.org/software-testing/vulnerability-testing/), and compliance audits.
* **Employee Training** is crucial for preventing insider threats and social engineering attacks. Organizations conduct cybersecurity awareness programs to educate employees on phishing scams, password security, and data handling best practices.
* **Monitoring & Incident Response** includes tracking user activity, detecting suspicious behavior, and responding to security incidents in real time. Security Information and Event Management (SIEM) tools help organizations analyze and mitigate threats effectively.

**7. Internet of Things (IoT) Security**

Refers to protecting internet-connected devices such as smart home gadgets, industrial sensors, medical equipment, and wearable technology from [cyber threats](https://www.geeksforgeeks.org/blogs/cybersecurity-threats/). IoT security ensures that these devices do not become entry points for hackers to exploit networks and steal sensitive data.

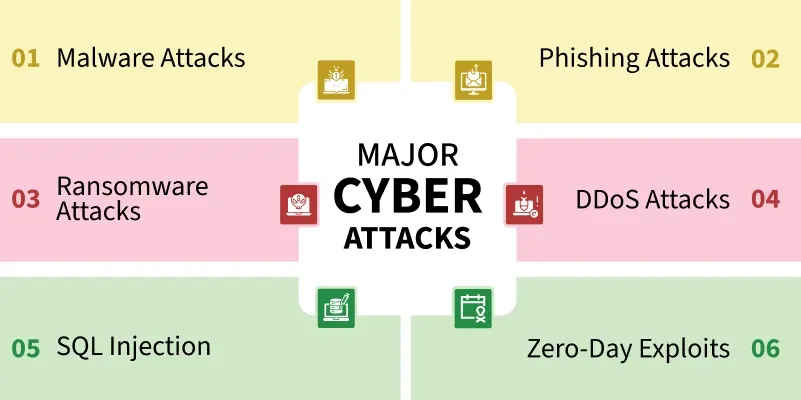
* **Device Authentication & Encryption** ensures that only authorized devices can connect to networks. Encryption protects data transmitted between IoT devices and servers from interception.
* **Firmware & Software Updates** are crucial to patch security vulnerabilities. Regular updates help prevent exploitation by [cybercriminals](https://www.geeksforgeeks.org/ethical-hacking/cyber-criminals-and-its-types/) who target outdated IoT firmware.
* **Network Segmentation** isolates IoT devices from critical systems, reducing the risk of widespread attacks if one device is compromised. This approach limits unauthorized access and lateral movement within a network.
* **IoT Security Standards & Compliance** include implementing industry security frameworks like [Zero Trust Architecture (ZTA)](https://www.geeksforgeeks.org/ethical-hacking/zero-trust-architecture-in-security/) and following best practices such as strong password policies, secure APIs, and endpoint protection to enhance IoT device security.

# **Why is Cybersecurity is Important?**

* Cybersecurity is important because the government, corporations, and medical organisations collect military, financial, process, and store unprecedented amounts of data on computers and other properties like personal information, and this private information could have negative consequences.
* In 1972, when the internet was just starting (called ARPANET at the time), a test virus named **Creeper** was created—and then another program called **Reaper** was made to remove it.
* This early experiment showed why **digital security** was needed and helped start what we now call **cybersecurity**.

# **Major Cybersecurity Threats & Attacks**

* Hackers use advanced techniques to find weaknesses in systems, steal or change data, and break into networks without permission.
* Below are the most common cybersecurity threats that target businesses, cloud storage, and personal devices:



**1. Malware Attacks**

* [Malware](https://www.geeksforgeeks.org/ethical-hacking/malware-and-its-types/) is a type of harmful software created to enter, attack, and compromise systems. It includes **trojans**, **rootkits**, and **spyware**.
* Hackers use **payload obfuscation**, **polymorphic techniques**, and **zero-day exploits** to bypass **intrusion detection systems (IDS)** and **endpoint protection platforms (EPP)**.

**2. Phishing & Spear Phishing Attacks**

* Phishing uses **tricks and manipulation** to steal login details, session tokens, and financial information. [**Spear phishing**](https://www.geeksforgeeks.org/computer-networks/spear-phishing-attack/) is a more targeted version that uses **open-source intelligence (OSINT)** to create personalized fake messages.
* Hackers use **domain spoofing**, **homograph attacks**, and **malicious macros** to bypass security and trick users into revealing sensitive data.

**3. Ransomware Attacks**

* [Ransomware](https://www.geeksforgeeks.org/computer-networks/ransomware-explained-how-it-works-and-how-to-prevent-it/) locks important system files by encrypting them using [**asymmetric cryptography**](https://www.geeksforgeeks.org/computer-networks/asymmetric-key-cryptography/) (like [RSA](https://www.geeksforgeeks.org/computer-networks/rsa-algorithm-cryptography/), ECC) or **hybrid encryption** (AES-RSA). It then demands a ransom, usually in **cryptocurrency**, to unlock the data.
* More advanced types, like **double extortion ransomware**, first **steal sensitive data** before encrypting it. Hackers then threaten to leak the stolen data on **dark web sites** if the ransom isn't paid.

**4. Distributed Denial-of-Service (DDoS) Attacks**

* DDoS attacks overload a network by flooding it with massive amounts of traffic at different levels—**volumetric, protocol, or application-layer**—causing servers to crash and making services unavailable.
* Hackers use [**botnets**](https://www.geeksforgeeks.org/ethical-hacking/what-is-botnet/), **amplification techniques** to increase attack size, and [**HTTP flood requests**](https://www.geeksforgeeks.org/ethical-hacking/http-flood-attack/) to overwhelm websites. These methods help attackers bypass **rate-limiting defenses** and take down their targets.

**5. SQL Injection (SQLi) & NoSQL Injection**

* [SQL injection attacks](https://www.geeksforgeeks.org/sql/sql-injection/) take advantage of weak web application queries by inserting **malicious SQL code** to **modify database records, steal login credentials, or run admin-level commands**.
* NoSQL injection targets **document-based databases** like **MongoDB and Firebase** by altering query parameters, allowing attackers to **bypass authentication** and gain unauthorized access to sensitive data.

**6. Zero-Day Exploits & Advanced Persistent Threats (APT)**

* [**Zero-day exploits**](https://www.geeksforgeeks.org/ethical-hacking/zero-day-exploit-cyber-security-attack/)take advantage of **unknown software vulnerabilities** before developers release security patches, making them highly dangerous.
* **Advanced Persistent Threats (APTs)** use **multi-stage attack techniques** to stay hidden in a system for a long time. These include **lateral movement**, **privilege escalation**, and **persistence mechanisms** to maintain control over compromised networks.

**7. Man-in-the-Middle (MITM) Attacks**

* [**Man-in-the-Middle (MITM) attacks**](https://www.geeksforgeeks.org/blogs/how-to-prevent-man-in-the-middle-attack/) secretly intercept and modify data exchanged between two parties by exploiting **weak encryption** or **unsecured communication channels**.
* Hackers use techniques like [**SSL**](https://www.geeksforgeeks.org/computer-networks/working-of-ssl/)**stripping**, **rogue access points**, and **ARP poisoning** to **steal login credentials, hijack user sessions, or inject malicious code** into data transmissions

**8. Insider Threats & Privilege Misuse**

* [**Insider threats**](https://www.geeksforgeeks.org/ethical-hacking/what-is-insider-attack/) occur when **compromised or malicious employees** with **high-level access** steal sensitive data, modify access permissions, or install [**backdoors**](https://www.geeksforgeeks.org/computer-networks/what-is-a-backdoor-attack/) to bypass security. Since insiders already have authorized access, they can easily evade **traditional perimeter security** measures.
* To detect and prevent insider threats, organizations use [**User and Entity Behavior Analytics (UEBA)**](https://www.geeksforgeeks.org/ethical-hacking/what-is-user-and-entity-behavior-analytics-ueba/) to track suspicious activities, [**Privilege Access Management (PAM)**](https://www.geeksforgeeks.org/linux-unix/privileged-access-management-pam-for-linux-and-unix/) to restrict sensitive access, and **zero-trust architectures** to ensure continuous verification.

**Challenges for Cybersecurity**  
Cybersecurity faces several challenges that make it a constantly evolving discipline:

* **Advanced Persistent Threats (APTs):** Skilled hackers use stealthy techniques to stay undetected for long periods.
* **Zero-Day Vulnerabilities:** Newly discovered software flaws that haven’t been patched yet.
* **Insider Threats:** Employees or partners who misuse their access rights.
* **Growing Attack Surface:** With IoT devices, cloud computing, and remote work, there are more entry points for attackers.
* **Skill Shortage:** There is a global lack of qualified cybersecurity professionals.
* **Cost and Complexity:** Implementing advanced security controls can be expensive and difficult to manage.

**Cybersecurity Trends**  
The cybersecurity field is rapidly evolving. Some current trends include:

* **AI and Machine Learning:** Used for threat detection, anomaly detection, and automating incident response.
* **Zero Trust Architecture:** Security model that assumes no user or device should be trusted by default.
* **Cloud Security:** Protecting data and applications hosted on cloud platforms.
* **Ransomware-as-a-Service (RaaS):** A growing underground industry where cybercriminals sell ransomware tools.
* **Biometric Authentication:** Replacing passwords with fingerprints, facial recognition, or voice patterns.
* **Regulatory Compliance:** GDPR, HIPAA, and other data protection laws are shaping how companies handle cybersecurity.

**Common Cyberattacks and Solutions**

* **Malware:** Malicious software (viruses, worms, trojans, ransomware) designed to damage systems or steal data.  
  *Solution:* Install antivirus, keep software updated, and use firewalls.
* **Phishing:** Fake emails or websites trick users into revealing personal data.  
  *Solution:* Awareness training, email filtering, and multi-factor authentication (MFA).
* **Password Attacks:** Brute force, dictionary, or credential stuffing attempts to crack passwords.  
  *Solution:* Strong password policies, MFA, and password managers.
* **DDoS (Distributed Denial of Service):** Overloading a network or website with fake traffic.  
  *Solution:* Load balancers, anti-DDoS services, and traffic filtering.
* **Man-in-the-Middle (MITM):** Intercepting communication between two parties.  
  *Solution:* End-to-end encryption (HTTPS, VPNs), secure Wi-Fi networks.
* **Drive-By Download:** Malware installed when visiting a compromised website.  
  *Solution:* Keep browsers updated, use ad blockers, and avoid suspicious sites.
* **Malvertising:** Fake or infected online ads spreading malware.  
  *Solution:* Ad blockers, updated browsers, and anti-malware tools.
* **Rogue Software (Scareware):** Fake software that tricks users into buying unnecessary services.  
  *Solution:* Verify software from trusted vendors, educate users.
* **Other Attacks:**
  + **SQL Injection:** Attackers inject malicious SQL queries into databases. *Solution:* Input validation and parameterized queries.\*
  + **Cross-Site Scripting (XSS):** Attackers inject malicious scripts into web apps. *Solution:* Web application firewalls (WAFs).\*
  + **Ransomware:** Files are encrypted until ransom is paid. *Solution:* Backup strategies, endpoint protection, user awareness.\*

**ITAM vs CSAM**

* **ITAM (IT Asset Management):** The process of managing and tracking an organization’s hardware, software, licenses, and resources. Its focus is on lifecycle management, cost optimization, and compliance. Example: Knowing how many laptops or software licenses a company owns.
* **CSAM (Cybersecurity Asset Management):** A newer, security-focused approach that identifies and protects all assets (including unmanaged devices, cloud resources, and IoT) against cyber risks. While ITAM focuses on ownership and efficiency, CSAM emphasizes visibility, security, and risk mitigation. Example: Detecting unauthorized IoT devices connected to a corporate network.

**CSAM (Cybersecurity Asset Management )**Cybersecurity Asset Management (CSAM) is the practice of continuously identifying, categorizing, and monitoring all IT assets within an organization with the specific goal of securing them. Unlike ITAM, which is business-oriented, CSAM integrates with vulnerability management, endpoint detection, and incident response tools to provide real-time visibility of risks. For example, if a shadow IT device (like an employee’s personal laptop) connects to the company’s Wi-Fi, CSAM tools detect it, classify it as unmanaged, and alert security teams. This helps in reducing attack surfaces and enforcing Zero Trust principles.