6. Introduction to Cyber Security

1.Write short notes on:-

i) Malware:-

- Malware is software that gets into the system without user consent to steal the user's private and confidential data, including bank details and passwords.
- They also generate annoying pop-up ads and change system settings. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware, and other malicious programs.
- Individuals and organizations need to be aware of the different types of malware and take steps to protect their systems, such as using antivirus software, keeping software and systems up-to-date, and being cautious when opening email attachments or downloading software from the internet.

Types of Malware:-

1. **Viruses** – Malicious code attached to executable files; spreads when infected files are shared. Can damage or delete data.
2. **Worms** – Self-replicating programs that spread over networks without needing a host file. Can slow down systems.
3. **Trojan Horse** – Disguised as useful software but performs harmful tasks. Often hides in non-executable files.
4. **Ransomware** – Encrypts user data and demands payment for its release.
5. **Adware** – Displays unwanted ads and pop-ups, often bundled with free software.
6. **Spyware** – Secretly collects and sends user information to attackers.
7. **Logic Bombs** – Malicious code triggered by a specific event, causing damage upon activation.

ii) Phishing:-

- **Definition**: Phishing is a cyberattack where attackers trick users into clicking fake links or websites to steal personal data.
- **Origin of Term**: Derived from "fishing" — attackers bait users just like fish to trap them.
- **Purpose**: To collect sensitive information like passwords, credit card details, social security numbers, etc.
- **Common Method**: Spam emails with fake links that look like legitimate websites or services.
- **Example**: A fake site mimicking YouTube with a misleading URL (like supertube.com), lures users to click.

How Phishing Happens

- **Unknown Files or Attachments**: Opening suspicious files may install malware or ask for personal info.
- **Free/Open Wi-Fi**: Attackers control data shared over unsecured networks.
- **Social Media Requests**: Fake accounts use social engineering to collect sensitive info.
- **Fake Ads or Links**: Clicking unknown ads or links can lead to phishing sites.

Types of Phishing Attacks

1. **Email Phishing**: Mass emails imitating trusted sources to steal data.
2. **Spear Phishing**: Targeted attack on individuals using personalized emails.
3. **Whaling**: Targets high-profile individuals like CEOs with urgent fake emails.
4. **Smishing**: Phishing through SMS containing malicious links or prompts.
5. **Vishing**: Voice calls with fake caller IDs pretending to be from trusted entities.
6. **Clone Phishing**: Replicates a real email, replacing links or attachments with malicious ones.

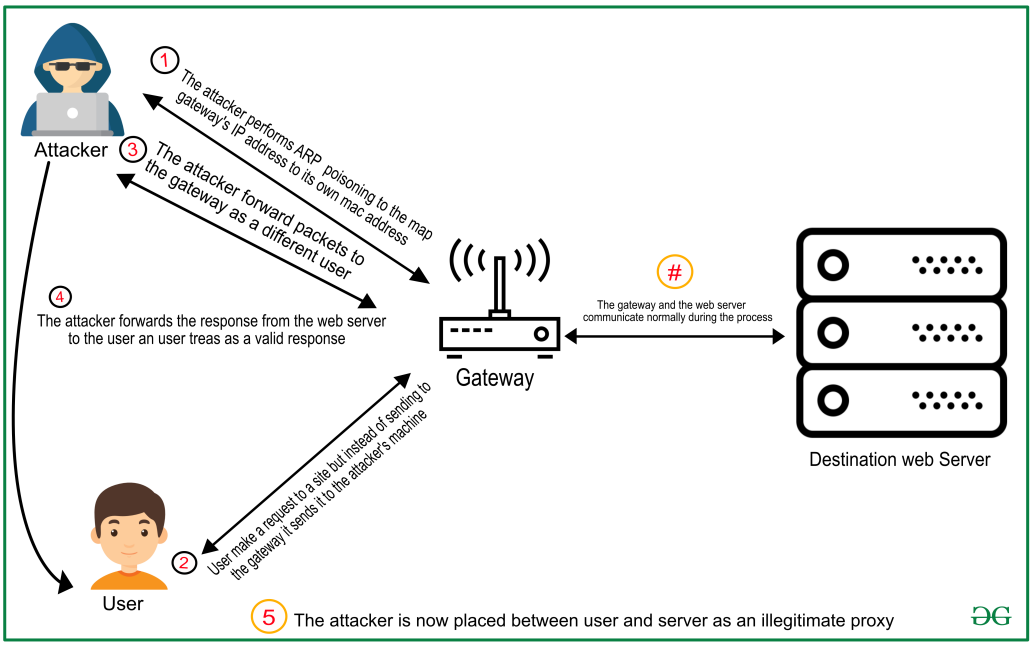
Impacts of Phishing

- **Financial Loss**: Unauthorized purchases or bank fraud using stolen info.
- **Identity Theft**: Misuse of personal information for illegal purposes.
- **Reputation Damage**: Loss of trust in organizations that are breached.
- **Business Disruption**: Compromised accounts or networks affect operations.

iii) MITA attack:-

- A **Man-in-the-Middle (MITM) attack** occurs when a malicious actor secretly intercepts and possibly alters the communication between two parties without their knowledge. This "middleman" can read, capture, or modify data being transmitted, such as passwords or banking information.

- **Example:**
  On a shared Wi-Fi network, an attacker uses rogue ARP packets to redirect your device's data through their machine. They can then capture and manipulate your sensitive data (e.g., bank login details) before forwarding it to the real destination.



Common MITM Attack Methods

- **ARP Spoofing:** Faking IP-to-MAC address mappings to intercept local network traffic.
- **DNS Spoofing:** Redirecting traffic by corrupting DNS responses.
- **Rogue Wi-Fi Access Point:** Creating fake Wi-Fi hotspots to lure users and intercept data.
- **Email Phishing:** Sending fraudulent emails to steal credentials.
- **Router Spoofing:** Imitating legitimate routers to capture data.

Techniques Used in MITM Attacks

- **Packet Sniffing:** Capturing network data to analyze and steal information.
- **Packet Injection:** Adding malicious data packets into legitimate communication.
- **SSL Stripping:** Downgrading HTTPS to HTTP to intercept unencrypted data.
- **Eavesdropping:** Listening in on active communications.

How to Detect MITM Attacks

- Visiting **fake websites** or seeing suspicious URLs.
- **Unusual network activity** or spikes in data usage.
- Browser warnings about **invalid or suspicious certificates**.
- Unexpected requests for **credentials** or frequent login errors.
- Unexpected **pop-ups** or notifications.

How to Prevent MITM Attacks

- Use **trusted and secure networks**; avoid open Wi-Fi.
- Ensure **SSL/TLS (HTTPS)** is properly used on websites.
- Keep software and browsers **updated**.
- Avoid logging into sensitive sites on **public or unknown devices**.
- Check for **rogue certificates** and suspicious hosts file entries on public computers.
- Use tools like **VPNs** to encrypt your traffic.
- Use **nonce values** or other anti-replay mechanisms in web apps to prevent replay attacks.

iv) Threats in Information Security:-

- Threats are actions by bad people (like hackers) who want to steal your data, break your computer, or cause problems. They look for weaknesses in your computer or network to get in and cause harm.
- These threats can include things like viruses, hackers trying to guess your passwords, or someone stealing your personal information.
- Knowing about these threats helps you protect your data and keep your computer safe. If you understand the dangers, you can take steps to stop bad people from causing trouble.

Common Threats:-

1. Virus:
Malware that attaches to files/programs and spreads by replicating itself, damaging files or systems.
Example: Creeper Virus.

2. Worms:
Self-replicating malware that spreads over networks without attaching to files, often slowing down systems.

3. Bots:
Automated programs that connect infected computers to a central server, forming a botnet used for attacks or spam.

4. Adware:
Software that displays unwanted ads and tracks user behavior, potentially compromising privacy.

5. Spyware:
Software that secretly monitors user activities and sends data to attackers.
Example: Keylogger records keystrokes.

6. Ransomware:
Malware that locks or encrypts files, demanding ransom to restore access.

7. Scareware:
Fake software that tricks users into paying for bogus fixes, while actually harming the system.

8. Rootkits:
Tools that hide malware by gaining administrative control over a system.

9. Zombies:
Infected machines controlled remotely by hackers to carry out attacks, without spying on users.

V) Vulnerability in Information Security:-

- A **vulnerability** in information security is a weakness or flaw in a system, software, network, or process that can be exploited by attackers to gain unauthorized access, cause damage, or steal data.

- It can arise from coding errors, misconfigurations, human mistakes, or design flaws, making the system less secure and open to threats.

1. Hardware Vulnerabilities

These are weaknesses in physical devices like computers, servers, or routers. Hackers can exploit them by physically tampering with the device or by exploiting flaws in the device's firmware (software built into hardware).
Example: Someone stealing a laptop to access sensitive data or exploiting outdated firmware to take control of a device.

2. Software Vulnerabilities

These are flaws or bugs in software programs, apps, or operating systems that attackers exploit to break into systems or cause damage. These vulnerabilities often happen because of coding mistakes or failure to update software.
Example: A hacker uses a bug in a web application to inject malicious code (SQL injection) or exploits an unpatched software bug to gain access.

3. Network Vulnerabilities

These are weaknesses in the way networks are designed or configured, which attackers can exploit to intercept data, access systems, or disrupt communication.
Example: An open Wi-Fi network without encryption allows attackers to connect and steal data.

4. Procedural Vulnerabilities

These happen when organizational processes or rules are weak or poorly followed. For example, using default passwords or not monitoring user activity can let attackers bypass security.
Example: Leaving default admin passwords unchanged on devices or not tracking login attempts, allowing attackers easy access.

5. Human Vulnerabilities

These arise from mistakes or poor security habits by people, like falling for phishing scams, using weak passwords, or accidentally sharing sensitive info. Humans are often the easiest target for attackers.
Example: An employee clicks on a phishing email link, giving attackers access to company systems.

vi) SQL Injection:-

- **SQL Injection** is a security flaw in **web applications** where attackers insert harmful **SQL** code through user inputs.
- This can allow them to access sensitive data, change database contents or even take control of the system. It's important to know about SQL Injection to keep web applications secure.
- For example, if a web application takes user input (e.g., a username or password) and directly inserts it into an SQL query without **proper sanitization**, an attacker can manipulate the query to perform unintended actions.

Types of SQL Injection:-

1. In-band SQL Injection

In-band SQL Injection is the most common type, where the attacker sends **malicious SQL queries** directly through the application interface. This method allows attackers to extract sensitive information or manipulate the database.

Example:

```
SELECT * FROM users WHERE id = 1; -- OR 1=1 --
```

This query would retrieve all users in the database because 1=1 is always true.

2. Error-based SQL Injection

This type of SQL injection exploits error messages generated by the database. Attackers can use the information provided in error messages to learn about the database structure and craft more sophisticated attacks.

Example:

```
SELECT * FROM users WHERE id = 1' -- ;
```

An error message could reveal details about the database schema, allowing the attacker to refine their attack.

3. Blind SQL Injection

In blind SQL injection, the attacker does not receive error messages but can infer information about the database by observing the behavior of the application. The attacker uses boolean conditions to test various aspects of the database.

Example:

```
SELECT * FROM users WHERE id = 1 AND 1=1;
```

If the response is different when 1=1 is changed to 1=0, the attacker can infer information about the database.

4. Out-of-band SQL Injection

Out-of-band SQL injection relies on the attacker using a different communication channel to exfiltrate data from the database. This type of attack is less common but can be very effective.

Example:

```
SELECT * FROM users WHERE id = 1; -- ;
```

The attacker might direct the database to send a DNS request or HTTP request with the extracted data.

5. Time-based Blind SQL Injection

In this form of blind SQL injection, the attacker sends a query that causes a time delay (e.g., using SLEEP), allowing them to infer whether the query was true or false based on the response time.

Example:

```
SELECT * FROM users WHERE id = 1 AND 1=1 SLEEP(5);
```

If the query takes 5 seconds to execute, the attacker knows that the query is true.

Impact of SQL Injection Attacks

- Unauthorized access to sensitive data:
- Data integrity issues:
- Privilege escalation:
- Service downtime:
- Reputation damage:

Prevent SQL Injection:

1. **Validate and Sanitize User Input:**

   Make sure user input only includes what is expected (e.g., no special characters).

2. **Use Web Application Firewalls (WAF):**

   These can detect and block SQL injection attempts.

3. **Limit Database Permissions:**

   Do not allow the web application to have full access to the database if it's not necessary.

4. **Keep Software Updated:**

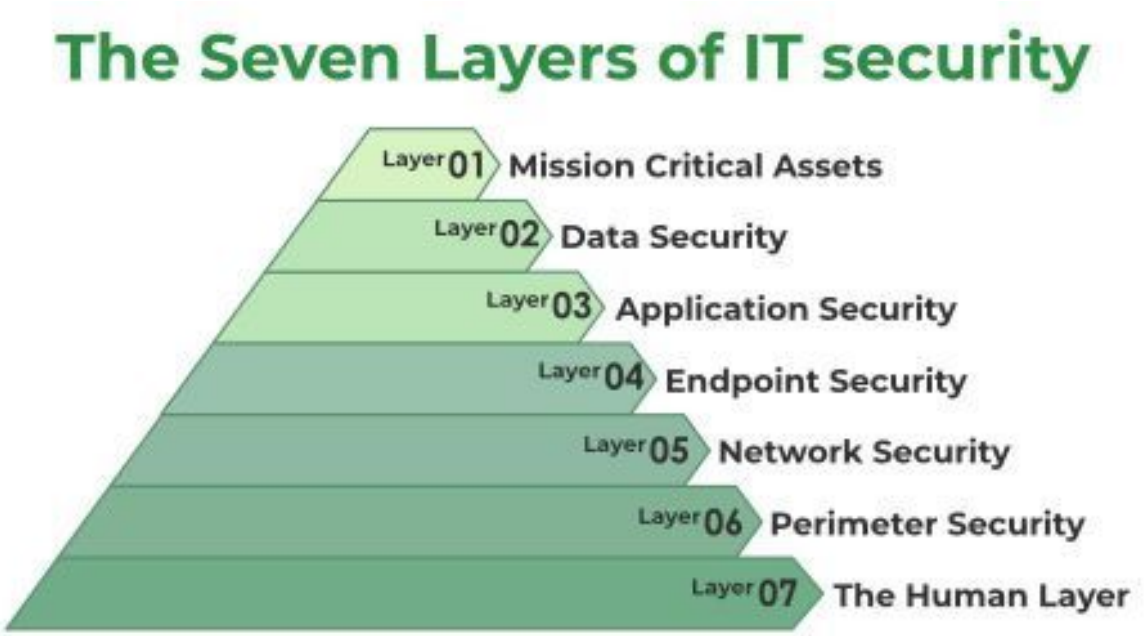
   Use the latest versions of your web server, database software, and frameworks.

2. Software attacks & hardware attacks:-

Aspect	Hardware Attack	Software Attack
Definition	Attacks targeting physical devices or embedded components.	Attacks targeting software applications and systems.
Access Needed	Usually requires physical access or close proximity.	Often launched remotely or via user interaction.
Common Techniques	Theft, tampering, side-channel attacks, firmware hacking.	Malware, SQL injection, buffer overflow, phishing.
Examples	- Stealing a laptop to access data.	- Ransomware encrypting files demanding payment.
	- Side-channel attack extracting encryption keys from a smart card.	- SQL injection exploiting web forms to steal data.
	- Installing malicious firmware on a router.	- Phishing emails tricking users into revealing passwords.
Prevention	Physical locks, device encryption, firmware updates.	Software patches, antivirus, secure coding, user training.

3. 7 Layers of Cyber Security:-

The **7 Layers of Cyber Security** represent a multi-layered defense strategy to protect systems, networks, and data from cyber threats. Each layer addresses a specific area of vulnerability.



1. Human Layer

This layer is about people. Most cyber-attacks happen because someone makes a mistake, like clicking on a fake email. Training employees to recognize scams, use strong passwords, and be careful online helps protect the organization.

Example:
An employee avoids a phishing scam because they were trained to spot fake emails.

2. Perimeter Security Layer

This is the outer wall of a company's digital space. It protects the company's internal network from threats coming from outside, like the internet. Tools like firewalls and filters stop bad traffic from getting in.

Example:
A firewall blocks a hacker from trying to access the network from the internet.

3. Network Security Layer

This layer keeps the internal network safe. Even if an attacker gets in, this layer makes it hard for them to move around. It watches network traffic and blocks anything suspicious.

Example:
The system notices a strange connection between computers and stops a virus from spreading.

4. Endpoint Security Layer

This is about protecting individual devices like computers, phones, or tablets. These are often targets for malware. Antivirus and regular updates help keep each device safe.

Example:
An employee's laptop blocks a virus after antivirus software detects it.

5. Application Security Layer

This layer protects software and apps from hackers. If apps have weak code or are not updated, they can be attacked. Secure coding and regular updates are important here.

Example:
A web app is protected from hackers by using strong code and keeping it updated.

6. Data Security Layer

This protects the actual information. It makes sure only the right people can see or change the data. Encryption and access controls keep the data safe from theft or leaks.

Example:
Even if someone steals a laptop, they can’t read the files because they’re encrypted.

7. Physical Security Layer

This is about protecting the physical equipment—like computers, servers, and storage—from being stolen or tampered with. Locks, cameras, and security staff help stop physical break-ins.

Example:
A server room is protected with a keypad lock, so only authorized staff can enter.

4. Explain:-

i) Cyber-Crimes:-

- **Crime** is an act or omission that violates a law and is punishable by the government. It can include anything from theft and assault to fraud and murder, depending on the law of the land.
- **Cybercrime** refers to **illegal activities involving computers, networks, or the internet** as a tool to commit offenses.
- Cybercriminals target individuals, businesses, and even government systems, leading to significant financial losses, data breaches, and security threats.

Types oF Cyber Crimes:-

1. Cybercrime Against Individuals

This type of cybercrime targets specific people, usually to steal personal information or cause emotional harm.

Description:
Criminals may use tricks like fake emails, messages, or social media to fool individuals into giving up sensitive details like passwords or bank information. They may also use the internet to bully, threaten, or stalk someone.

Examples:

- Phishing emails pretending to be from banks
- Identity theft using someone's personal info
- Cyberbullying or online harassment

2. Cybercrime Against Property

These crimes involve attacking or damaging someone's digital assets like data, files, or money.

Description:
Cybercriminals may hack systems to steal or destroy data, infect devices with ransomware, or use viruses to damage files. They may also commit financial fraud by stealing card numbers.

Examples:

- Hacking into a company's database
- Ransomware locking files for money
- Online banking fraud

3. Cybercrime Against Organizations

These attacks are aimed at businesses, educational institutions, or other organizations to disrupt services or steal valuable data.

Description:
Criminals often try to damage reputation, steal trade secrets, or stop business operations by crashing servers or spreading malware. These attacks can cause huge financial losses.

Examples:

- Distributed Denial of Service (DDoS) attacks
- Data breaches leaking customer information
- Corporate spying through digital means

4. Cybercrime Against Government

These are serious attacks on government websites, databases, or national systems that can affect public safety or national security.

Description:
These crimes are often politically or ideologically motivated and may be carried out by hackers or terrorist groups. The goal is to steal sensitive government data, spread propaganda, or disrupt important services.

Examples:

- Hacking defense or intelligence networks
- Spreading fake news to mislead citizens
- Attacks on government infrastructure systems

5. Cybercrime Against Society

These crimes harm the moral or social structure of society. They may involve illegal, offensive, or abusive content that affects people or groups at large.

Description:
Cybercriminals may promote hate, violence, or illegal activities through websites or online platforms. Such actions can cause harm to society's values and safety.

Examples:

- Sharing child pornography
- Running illegal online betting platforms
- Promoting terrorism or hate speech online

ii) Cyber Terrorism:-

- Cyber terrorism is the use of digital tools and internet technology by terrorists to carry out attacks aimed at causing harm, disruption, or fear.
- These attacks often have political or ideological motives and target critical systems like power grids, transportation, or communication networks.
- The goal can be to interrupt services, steal sensitive data, inflict physical damage, or spread panic.
- Cyber terrorists use methods such as hacking, spreading malware, launching Distributed Denial of Service (DDoS) attacks, and deploying ransomware to disrupt vital infrastructure and promote their agendas.

Examples of Cyber Terrorism:

1. **Stuxnet (2010):** Malware that damaged Iran's nuclear centrifuges by controlling their speed, delaying their nuclear program. It's one of the first cyber attacks causing physical damage.
2. **Ukraine Power Grid Attacks (2015 & 2016):** Cyber attacks on Ukraine's electricity grid causing widespread blackouts, linked to Russian hackers, highlighting vulnerabilities in critical infrastructure.
3. **Sony Pictures Hack (2014):** North Korean hackers attacked Sony in retaliation for a movie depicting their leader's assassination, leaking sensitive data and causing major disruption.
4. **WannaCry Ransomware Attack (2017):** A global ransomware attack that encrypted files and demanded Bitcoin ransom, disrupting healthcare and other essential services worldwide.
5. **NotPetya Attack (2017):** Initially disguised as ransomware, it primarily targeted Ukraine but spread globally, destroying data and crippling computer systems.
6. **Saudi Aramco Attack (2012):** A malware attack erased data on thousands of computers at Saudi Aramco, severely disrupting the company's operations and causing financial loss.

iii) Cyber Stalking:-

- Cyberstalking is when someone uses the internet or digital tools to repeatedly harass, threaten, or spy on another person.
- This can include sending unwanted messages, hacking accounts, spreading lies online, or tracking someone's activities. The goal is usually to scare, upset, or control the victim.
- Cyberstalkers often use social media, emails, fake profiles, or spyware to follow their victims closely.
- They may impersonate the victim, post false information, or send threatening messages. Sometimes, they even track the victim's location using GPS or hidden software.
- Cyberstalking is serious, illegal, and can lead to real-world harm. Victims may suffer emotional distress, privacy invasion, and damage to their reputation.

Examples of Cyberstalking:

- Sending repeated unwanted messages
- Creating fake profiles to follow or harass someone
- Tracking someone's online activity or location
- Hacking into personal accounts
- Posting private information or false rumors
- Sending threatening comments
- Using spyware or GPS to monitor someone

Types of Cyberstalking:

- **Webcam Hijacking:** Tricking someone into installing malware that lets stalkers watch through their webcam.
- **Social Media Location Tracking:** Following someone's posts with location tags to find out where they are.
- **Catfishing:** Making fake profiles to deceive or befriend the victim online.
- **Using Google Street View:** Checking out the victim's neighborhood or home address online.
- **Installing Stalkerware:** Secret software that tracks texts, calls, browsing history, and location.
- **Reading Geotags:** Extracting location info from photos posted online.

How to Protect Yourself from Cyberstalking:

- Always log out of your accounts when done using devices.
- Avoid posting your plans or locations publicly on social media.
- Use strong, unique passwords for your accounts.
- Avoid sharing sensitive info on public Wi-Fi networks.
- Use privacy settings on social media to limit who can see your info.
- Regularly check what information about you is available online.

5. Cyber Security Polycies in detail and Different challenges in internet governance:-

Different Cybersecurity Policies:- Cybersecurity policies are formal rules and guidelines that organizations or governments create to protect their information systems, data, and users from cyber threats.

1. Acceptable Use Policy (AUP)

- **Purpose:** Defines what users are allowed or not allowed to do when using an organization's network, devices, or internet resources.
- **Details:** It outlines acceptable behavior such as not accessing unauthorized websites, not installing unapproved software, and prohibiting illegal activities.
- **Example:** Employees must not download pirated software or visit risky websites that could infect the network.

2. Access Control Policy

- **Purpose:** Specifies how access to information and systems is granted, managed, and revoked.
- **Details:** It covers user authentication methods, roles and permissions, and how sensitive data access is restricted.
- **Example:** Only HR staff can access employee personal data, and multi-factor authentication (MFA) is required for access.

3. Data Protection Policy

- **Purpose:** Ensures the confidentiality, integrity, and availability of sensitive data.
- **Details:** Includes data encryption, data classification (e.g., public, confidential), and data retention schedules.
- **Example:** Customer credit card information must be encrypted both in storage and during transmission.

4. Incident Response Policy

- **Purpose:** Provides a clear plan for responding to cybersecurity incidents or breaches.
- **Details:** Defines roles and responsibilities, how to report incidents, investigation procedures, and communication protocols.
- **Example:** In case of a data breach, the IT team must immediately isolate affected systems and notify management.

5. Password Policy

- **Purpose:** Establishes rules for creating and managing passwords to reduce unauthorized access.
- **Details:** Guidelines on password length, complexity, expiration, and storage.
- **Example:** Passwords must be at least 12 characters long and include numbers, symbols, and uppercase letters.

6. Remote Access Policy

- **Purpose:** Controls how employees can securely connect to the organization's network from outside locations.
- **Details:** Specifies allowed VPNs, device requirements, and security checks for remote access.
- **Example:** Remote workers must use a company-approved VPN and have updated antivirus software before accessing internal resources.

Challenges in Internet Governance

1. Cybersecurity Threats

- Increasing cyber-attacks like hacking, malware, ransomware, and data breaches create a constant challenge to keep the internet safe for users worldwide.

2. Privacy and Data Protection

- Protecting user privacy is complicated because the internet crosses international borders.
- Different countries have different data protection laws (e.g., GDPR in Europe vs. lax regulations elsewhere), causing conflicts and inconsistencies.

3. Regulation and Control

- Balancing between free speech and regulating harmful content (hate speech, fake news, terrorism-related content) is a major challenge.

4. Domain Name System (DNS) Management

- Managing the global domain name system fairly and transparently is critical.
- Disputes over domain ownership, censorship, or access can arise, especially with politically sensitive websites.

5. Emerging Technologies

- The rapid growth of new technologies like AI, IoT, blockchain, and 5G introduces new governance challenges regarding security, privacy, and ethical use.