CS-27: Cyber Security

Prepared By: Prof. Harsh Joshi

Unit-1
Introduction to Cyber Security

What is Cyber Space?

Cyberspace is defined as the dynamic and virtual space that connects the different computer systems.

An analogy can be drawn between cyberspace and the human brain. Like there are innumerable neurons present in the brain, cyberspace has countless connections and networks that exist between the computer systems.

The term was first introduced in the Wiliam Gibson's science fiction book Necromancer. After that, the term found a place in many English dictionaries as the virtual space with no mass, gravity or boundaries.

Overview of Web-technology:

Web Technology can be Classified into the Following Sections:
World Wide Web (WWW): The World Wide Web is based on several different technologies: Web browsers, Hypertext Markup Language (HTML), and Hypertext Transfer Protocol (HTTP).
Web Browser: The web browser is an application software to explore www (World Wide Web). It provides an interface between the server and the client and requests to the server for web documents and services.
Web Server: Web server is a program which processes the network requests of the users and serves them with files that create web pages. This exchange takes place using Hypertext Transfer Protocol (HTTP).
Web Pages: A webpage is a digital document that is linked to the World Wide Web and viewable by anyone connected to the internet has a web browser.
Web Development: Web development refers to the building, creating, and maintaining of websites. It includes aspects such as web design, web publishing, web programming, and database management. It is the creation of an application that works over the internet i.e. websites.

Prepared By: Prof. Harsh Joshi

Architecture of Cyber Space

"Cyberspace" refers to the interconnected digital environment where computer systems, networks, and data interact. It is a conceptual space created by the interdependence of these digital elements.
Understanding the architecture of cyberspace involves examining the components, protocols, and interactions that shape the digital landscape.
The architecture of cyberspace is a multifaceted and evolving landscape, encompassing physical and virtual components, protocols, security layers, and emerging technologies. Understanding and managing this complex environment is essential for individuals, businesses, and governments to navigate the digital realm securely and responsibly. As technology continues to advance, the architecture of cyberspace will undoubtedly undergo further transformations, requiring ongoing adaptation and innovation in cybersecurity and digital governance.

Infrastructure:

At the core of cyberspace architecture is its infrastructure, which includes both physical and virtual components.

Physical Infrastructure:

- Data Centers: These centralized facilities house servers, storage systems, and network equipment that support the processing and storage of vast amounts of digital data.
- Network Cables and Fiber Optics: Physical connections that enable the transmission of data between devices and across the internet.
- Satellites and Submarine Cables: Global communication relies on satellites for wireless transmission and submarine cables for intercontinental data exchange.

Virtual Infrastructure:

- Cloud Computing: Virtualized computing resources, including servers, storage, and networking, delivered as services over the internet.

Prepared By: Prof. Harsh Joshi

- Virtual Machines and Containers: Technologies that enable the creation and deployment of isolated and portable computing environments.

Protocols and Standards:

Cyberspace relies on a set of protocols and standards to facilitate communication and ensure interoperability.

- **TCP/IP (Transmission Control Protocol/Internet Protocol):**

The foundational suite of protocols for internet communication, defining how data is packetized, addressed, transmitted, routed, and received.

- **HTTP/HTTPS (Hypertext Transfer Protocol/Secure):**

Protocols for transmitting hypertext requests and responses, fundamental to web communication.

- **DNS (Domain Name System):**

Resolves human-readable domain names into IP addresses, facilitating web address translation.

- **SSL/TLS (Secure Sockets Layer/Transport Layer Security):**

Encryption protocols that secure data transmission, commonly used for secure web connections (HTTPS).

Standards:

- **IEEE Standards:**

The Institute of Electrical and Electronics Engineers establishes standards for various technologies, including networking, wireless communication, and cybersecurity.

- **ISO/IEC Standards:**

International standards that cover a broad range of information technology areas, ensuring global consistency in practices and products.

Layers of the Internet:

The architecture of cyberspace can be conceptualized through the layers of the internet model.

OSI Model (Open Systems Interconnection):

1. **Physical Layer:** Concerned with the transmission and reception of raw bit streams over a physical medium.

2. **Data Link Layer:** Manages access to the physical medium, providing error detection and correction.
3. **Network Layer:** Responsible for logical addressing, routing, and forwarding of data packets.
4. **Transport Layer:** Ensures end-to-end communication, reliability, and error recovery.
5. **Session Layer:** Establishes, maintains, and terminates connections between applications.
6. **Presentation Layer:** Translates data between the application layer and the lower layers, handling encryption and compression.
7. **Application Layer:** Interacts directly with end-user applications.

TCP/IP Model:

1. **Link Layer:** Equivalent to OSI's Data Link and Physical Layers.
2. **Internet Layer:** Corresponds to OSI's Network Layer, handling IP addressing and routing.
3. **Transport Layer:** Combines aspects of OSI's Transport and Session Layers, providing connection-oriented communication.
4. **Application Layer:** Merges functions of the OSI Presentation and Application Layers, interacting directly with end-user applications.

Cybersecurity Layers:

Given the ever-present threat landscape, cybersecurity is an integral layer in the architecture of cyberspace.

1. **Perimeter Security:** Controls access to the network, often implemented through firewalls and intrusion detection/prevention systems.
2. **Network Security:** Involves monitoring and securing the internal network, detecting and preventing unauthorized activities.
3. **Endpoint Security:** Focuses on individual devices (endpoints), safeguarding against malware, unauthorized access, and data breaches.
4. **Application Security**: Ensures the security of software applications, including web applications, through secure coding practices and regular audits.

Prepared By: Prof. Harsh Joshi

5. **Data Security:** Involves protecting sensitive data through encryption, access controls, and data loss prevention measures.

Virtual Environments:

The digital realm includes virtual spaces that simulate physical environments or create entirely new ones.

- **Virtual Reality (VR):** Immersive experiences that replicate or enhance reality using computer-generated environments.
- **Augmented Reality (AR):** Overlays digital information onto the real world, enhancing the user's perception.
- **Digital Twins:** Digital replicas of physical entities, enabling real-time monitoring and analysis.

Cryptography:

Cryptography plays a crucial role in securing data and communications within cyberspace.

- **Encryption Algorithms:** Algorithms like AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman) secure data at rest and in transit.
- **Public-Key Infrastructure (PKI):** Manages digital keys and certificates, facilitating secure communication and authentication.

Artificial Intelligence (AI) and Machine Learning (ML):

AI and ML technologies are increasingly integrated into the architecture of cyberspace.

- **Threat Detection:** ML algorithms analyze patterns and anomalies to detect potential cyber threats.
- **Behavioral Analysis:** AI is employed for analyzing user and system behaviors to identify unusual activities.
- **Automated Responses:** AI-driven systems can autonomously respond to certain cybersecurity incidents.

Governance and Regulation:

Governance and regulatory frameworks guide responsible and ethical behavior within cyberspace.

- **Data Protection Laws:** Regulations like GDPR (General Data Protection Regulation) mandate the responsible handling of personal data.
- **Cybersecurity Standards:** Compliance with standards such as ISO/IEC 27001 demonstrates adherence to best practices.
- **International Cooperation:** Cybersecurity efforts often involve collaboration between nations to address global threats.

Future Considerations:

The architecture of cyberspace is dynamic, and future developments will shape its evolution.

- **5G Technology:** The rollout of 5G networks will bring higher speeds and lower latency, impacting the architecture of cyberspace.
- **Quantum Computing:** The advent of quantum computing poses both challenges and opportunities for encryption and security.
- **Biometric Authentication:** Advancements in biometric technologies may play a significant role in enhancing digital identity and access control.

World Wide Web (WWW):

World Wide Web (WWW), byname Web, is leading information retrieval service of web (the worldwide computer network). Online gives users access to a huge array of documents that are connected to every other by means of hypertext or hypermedia links—i.e., hyperlinks, electronic connections that link related pieces of data so as to permit a user quick access to them. Hypertext allows the user to pick a word or phrase from text and thereby access other documents that contain additional information concerning that word or phrase.

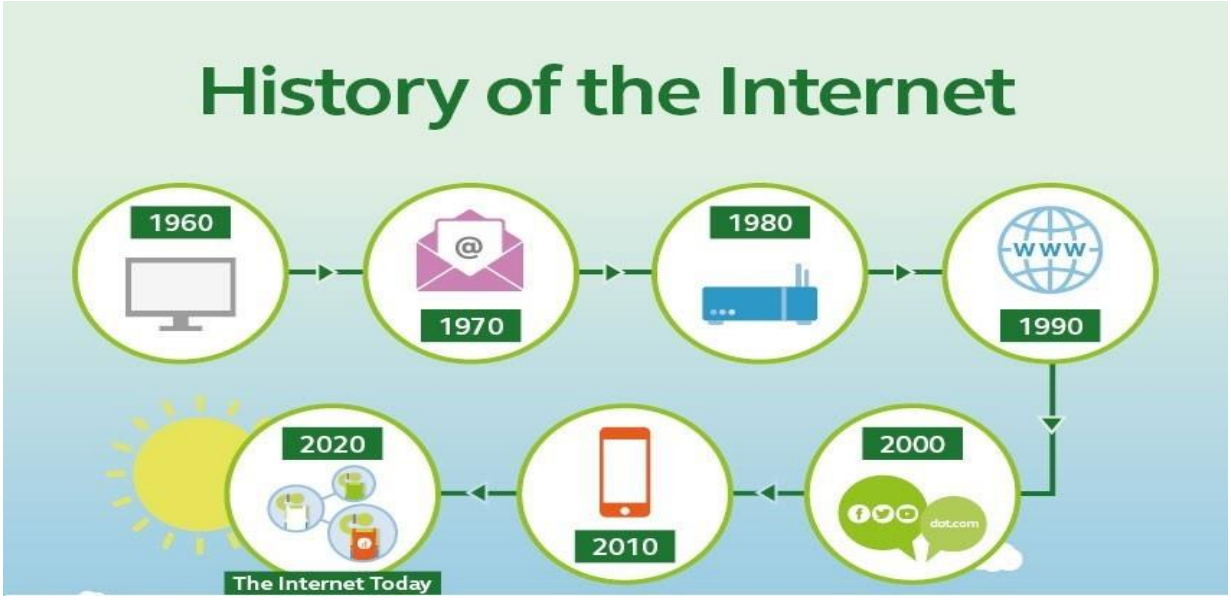
Advent of internet

Initially in the 1960s, the **Internet was started** as a medium for sharing information with government researchers. During the time computers were larger in size and were immovable. In case anyone had to access the information stored in any computer, they had to travel to the location of the computer or the other way to

have magnetic computer tapes that could be transported through the postal system of that time.

Alongside, Escalated Cold War played a major role in the **creation of the internet**. The Soviet Union had deployed the Sputnik satellite which led the Defense Department of the United States to examine the possibilities of communicating information despite nuclear. The situation resulted in the development of **ARPANET** (Advanced Research Projects Agency Network), which, later on, **evolved into the Internet**. In the initial days, ARPANET became a huge success with restricted participation where it was accessible to academic and research institutions that had contracts with the US Defense Department. The scenario led to the formation of new networks in order to facilitate the need for information sharing with other people.

Earlier there wasn't any standard mechanism for the computer networks that would enable them to communicate with each other. Transfer Control Protocol (TCP/IP) which was developed in 1970, was adopted as a new communication protocol for ARPANET in 1983. The technology enabled various computers on different networks to communicate with each other and this is **how the Internet was officially born** on January 1, 1983.



What is DNS?

DNS is short for **Domain Name System**. It functions as the internet's version of a phone book, converting difficult-to-remember IP addresses into simple names. Cheaper technology and the introduction of desktop computers in the early 1980s facilitated the rapid development of local area networks (LANs). As the number of

machines on the network grew, it became impossible to keep track of all the different IP addresses.

The **development of the Domain Name System (DNS)** in 1983 solved this problem. DNS was invented at the University of Southern California by Paul Mockapetris and Jon Postel. It was one of the breakthrough inventions that helped in paving the way for the World Wide Web.

Internet infrastructure for Data Transfer and Governance

Internet infrastructure plays a pivotal role in the seamless transfer of data and governance in the digital age. Internet infrastructure for data transfer and governance is a multifaceted ecosystem that intertwines technical components with regulatory frameworks. The seamless transfer of data relies on a robust infrastructure comprising submarine cables, data centers, IXPs, and more. Mechanisms like TCP/IP, HTTPS, and VPNs ensure secure and efficient data transfer.

In the realm of governance, organizations such as ICANN and regulatory frameworks play a crucial role in maintaining the internet's stability and addressing issues like cybersecurity, network neutrality, and the digital divide. As emerging technologies reshape the digital landscape, future considerations must encompass the implications of 5G, AI, IoT, and decentralized technologies on both data transfer and governance. Striking the right balance between innovation, accessibility, and security remains a central challenge for the continued evolution of the internet and its governance.

Internet Infrastructure Components:

- **Submarine Cables:**

Submarine cables form the backbone of international internet connectivity. These fiber-optic cables laid on the ocean floor facilitate high-speed data transmission between continents. The global network of submarine cables ensures the interconnectivity of regions, enabling the transfer of vast amounts of data.

- **Internet Exchange Points (IXPs):**

IXPs serve as critical hubs where different internet service providers (ISPs) and networks interconnect. These points facilitate the exchange of internet traffic,

optimizing routing efficiency and reducing latency. Major IXPs play a crucial role in enhancing the overall resilience and performance of the internet.

- **Data Centers:**

Data centers are centralized facilities that house networked computer systems and storage used for processing, storing, and managing data. They play a fundamental role in supporting internet services, ensuring reliability, scalability, and accessibility. Cloud computing services often leverage data centers to deliver on-demand computing resources.

- **Content Delivery Networks (CDNs):**

CDNs are distributed networks of servers strategically located to deliver web content efficiently. By caching content closer to end-users, CDNs reduce latency and enhance the speed of data transfer. This is particularly crucial for delivering multimedia content and improving the user experience.

- **Domain Name System (DNS):**

The DNS translates human-readable domain names into IP addresses, allowing users to access websites using memorable names. This hierarchical system ensures the proper routing of data on the internet. DNS plays a pivotal role in internet governance by managing the global distribution of domain names.

- **Internet Service Providers (ISPs):**

ISPs provide users with internet access, connecting them to the broader network. These providers deploy various technologies, including broadband, DSL, and fiber-optic connections, to enable users to transfer data over the internet. ISPs are key stakeholders in both the technical and regulatory aspects of internet governance.

Mechanisms for Data Transfer:

- **Transmission Control Protocol/Internet Protocol (TCP/IP):**

TCP/IP is the foundational protocol suite governing internet communication. It ensures reliable and orderly data transfer by breaking data into packets, which are then transmitted and reassembled at the destination. TCP/IP is fundamental to the functioning of the internet and is integral to its governance.

- **Hypertext Transfer Protocol (HTTP) and HTTPS:**

HTTP and its secure counterpart, HTTPS, are protocols for transferring hypertext and other data on the World Wide Web. HTTPS, with its added layer of security through encryption, is vital for secure data transfer, particularly in sensitive transactions. The adoption of HTTPS is encouraged by internet governance bodies to enhance user privacy and security.

- **File Transfer Protocol (FTP):**

FTP enables the transfer of files between computers on a network. While less commonly used for general internet users today, FTP remains crucial for specific applications, especially in scenarios where large files need to be exchanged securely.

- **Internet Protocol version 6 (IPv6):**

IPv6 addresses the limitation of IPv4 in providing unique IP addresses due to the growing number of devices connected to the internet. IPv6 facilitates the continued expansion of the internet by offering a more extensive pool of addresses, ensuring the seamless transfer of data.

- **Virtual Private Networks (VPNs):**

VPNs create secure, encrypted connections over the internet, allowing users to transmit data privately. They play a significant role in ensuring data privacy and security, particularly in the context of internet governance and regulatory compliance.

Governance Implications:

- **Internet Governance Organizations:**

Multiple organizations contribute to the governance of the internet, setting standards, addressing technical challenges, and ensuring its stable operation. Key entities include the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), and the World Wide Web Consortium (W3C). These organizations collaborate to maintain the integrity and interoperability of the internet.

- **Cybersecurity and Data Protection:**

Internet governance encompasses cybersecurity measures to protect data from cyber threats. Robust cybersecurity policies and practices are essential for safeguarding sensitive information. Additionally, data protection regulations, such as the General Data Protection Regulation (GDPR), dictate how personal data is handled, impacting both data transfer mechanisms and internet governance.

Prepared By: Prof. Harsh Joshi

- **Network Neutrality:**

Network neutrality is a governance principle advocating for equal treatment of all data on the internet. It ensures that ISPs do not discriminate against specific types of content or services. The debate over network neutrality involves discussions about fair access to the internet and preventing potential abuse of power by ISPs.

- **Digital Divide:**

Internet governance is tasked with addressing the digital divide — the gap between those who have access to modern information and communication technology and those who do not. Bridging this divide involves policy initiatives, infrastructure development, and ensuring affordable access for underserved communities.

- **Regulatory Compliance:**

Governments worldwide contribute to internet governance through regulatory frameworks. These frameworks address issues like data privacy, online content regulation, and telecommunications policies. Navigating the balance between enabling innovation and protecting users' rights poses an ongoing challenge in internet governance.

Emerging Trends and Future Considerations:

- **Edge Computing:**

Edge computing involves processing data closer to the source of generation rather than relying on centralized data centers. This trend enhances the efficiency of data transfer, reduces latency, and has implications for how internet infrastructure is designed and managed.

- **5G Technology:**

The rollout of 5G networks promises faster data transfer speeds and lower latency, enabling the proliferation of advanced applications. It poses challenges and opportunities for internet governance, particularly regarding privacy, security, and equitable access.

- **Artificial Intelligence (AI):**

AI applications, including machine learning algorithms, are increasingly integrated into internet services. Governance considerations include ethical use, bias mitigation, and ensuring transparency in AI-driven decision-making processes.

- **Internet of Things (IoT):**

The exponential growth of IoT devices introduces new challenges in data transfer and governance. Issues related to data security, privacy, and interoperability become critical considerations for both technical and policy frameworks.

- **Decentralized Technologies:**

Blockchain and decentralized technologies challenge traditional models of internet governance. These technologies offer enhanced security and user control, but their widespread adoption requires addressing regulatory and interoperability challenges.

Internet society

We are a global charitable organization empowering people to keep the Internet a force for good: open, globally connected, secure, and trustworthy. We are the Internet Society. People are at the heart of our mission.

Regulation in Cyberspace

The resilience of the private sector in the world of cyber has a decisive impact on national security. This sector is usually the weakest link through which cyberattacks develop and serves as a springboard for attackers who are interested in harming state targets.

In addition, built-in market failures lead to a lack of sufficient organizational investment in proper cybersecurity. Negative externalization of cyber damage in organizations, the difficulty in quantifying the benefit of investing in cybersecurity, the lack of responsibility of software and hardware providers for their products' security vulnerabilities, and a competitive market that rewards innovation and progress over proper cyber protection create a gap that requires state intervention.

A review of cyber protection regulation regimes in the Western world reveals a lack of systematic solutions for the business sector and a gap in mapping out national security threats that could result from potential cyber damage in this sector.

This memorandum, which is based on world events in the field of cyber and in other areas of regulation, offers a multi-layer regulatory model for cybersecurity in the private sector.

Prepared By: Prof. Harsh Joshi

The memorandum suggests an integrated model for a state regulatory alternative that includes mandatory regulations, the creation of monitoring mechanisms for supervising self-regulation, and providing incentives for encouraging organizations to protect themselves.

In an era of widespread use of linked devices, the entry of artificial intelligence into all aspects of life, and the creation of an insurance market for cybersecurity, regulating the business sector is a vital national interest.

Concept of cyber security

Cybersecurity is the practice of protecting internet-connected devices, networks, and programs from cyberattacks.

These attacks are often intended to access, change, or destroy sensitive information, extort money, or disrupt business processes.

Cyberattacks can be carried out by hackers, spammers, and cybercriminals, and can include phishing schemes, ransomware attacks, identity theft, data breaches, and financial losses.

A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe.

In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber attacks.

A unified threat management system can automate integrations across select Cisco Security products and accelerate key security operations functions: detection, investigation, and remediation.

People

Users must understand and comply with basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data.

Processes

Organizations must have a framework for how they deal with both attempted and successful cyber attacks. One well-respected framework can guide you. It explains

how you can identify attacks, protect systems, detect and respond to threats, and recover from successful attacks.

Technology

Technology is essential to giving organizations and individuals the computer security tools needed to protect themselves from cyber attacks. Three main entities must be protected: endpoint devices like computers, smart devices, and routers; networks; and the cloud. Common technology used to protect these entities include next-generation firewalls, DNS filtering, malware protection, antivirus software, and email security solutions.

Issues and challenges of cyber security

- Ransomware

  A type of malware that uses encryption to block or limit access to data until a ransom is paid.

- Phishing

  Responsible for more than 80% of reported security incidents and about 90% of data breaches.

- Cyber warfare

  A serious national security challenge for government agencies that store and send sensitive information across networks.

- Insider attacks

  A widely accepted issue that requires special detection systems to identify malicious insiders.

- IoT attacks

  Gaining access to IoT devices can compromise sensitive user data and open the door for other malicious attacks.

- Malware

  A common challenge that can cause data breaches, hardware failures, and inoperable systems that can be costly to recover.

- Cloud attacks
  Attackers can exploit weaknesses in cloud environments to gain access, steal data, disrupt services, or launch other malicious activities.

UNIT-2
Cyber Crime and Cyber law

Classification of Cyber Crimes

- Here are two common ways of classification for Cyber Crimes:
- **By Target**
- **Crimes against Individuals:** These target the people and their private data. Examples are:
    1. **Identity Theft:** Stealing personal information from someone in order to fraud them or impersonate them
    2. **Cyberstalking:** Using technology to cause fear or annoy someone.
    3. **Cyberbullying:** Abuse someone online through electronic means.
    4. **Online Scams:** tricking them into exposing their personal information or money.
- **Crimes against Organizations:** These target businesses and organizations. Examples are:
    1. **Data Breaches:** Sensitive data theft and unauthorized access.
    2. **Denial-of-Service (DoS) Attacks:** overloading a network or website with so much traffic that it becomes unavailable.
    3. **Hacking:** Unauthorized interruption into a computer system or network.
    4. **Malware Attacks:** Installing malicious software on computers in order to steal information, interfere with operations, or do harm.
    5. **Cyber Espionage:** Stealing private data from a government organization or rival.
- **Crimes against Society at Large:** They can cause significant disruption and target towards society as a whole. Examples are:
    1. **Cyberterrorism:** Launching attacks through computer networks that harm people physically or damage critical systems.
    2. **Disinformation Campaigns**: Spreading incorrect or misleading information in an attempt to create conflict or manipulate public opinion.
    3. **Social Engineering Attacks:** misleading someone into clicking on harmful websites or exposing private information.
    4. **Crimes against Critical Infrastructure:** Targeting networks of transportation or electricity systems, or other systems necessary for a society to function.
- **By Nature of the Crime:**
    1. **Financial Crimes:** The aim of these crimes is to steal money or bank data. Online banking frauds, credit card fraud, and identity theft are a few examples.

Prepared By: Prof. Harsh Joshi

2. **Content-Related Crimes:** These offences include producing or spreading prohibited content, such as copyrighted or child pornographic materials.
3. **Disruption and Destruction:** The goal of these crimes is to interfere with or harm networks or computer systems. Malware and DoS attacks are two examples.
4. **Privacy Violations:** These offences include the unapproved entry, gathering, or application of private data. Cyberstalking and data breaches are two examples.

Common Cyber Crimes

<u>Cyber Crime Targeting Computers and Mobiles</u>

- Cybercriminals are continuously on searching for methods for finding gaps in computers and mobile devices. The following is an overview of some of the most frequent cybercrimes that target these devices:

- **Infection by Malicious Software (Malware):**
    1. Viruses: This self-replicate and spread from one device to another, erasing or damaging data.
    2. Worms: Though they resemble viruses, they spread quickly by taking advantage of network vulnerabilities.
    3. Trojan Horses: They trick users into installing them by pretending to be legitimate software, after which they steal data or damage the device.
    4. Spyware: Quietly monitors your activities in the background, gathering passwords and browsing history.
    5. Ransomware: This malicious software encrypts your files, making them unreadable, and requests a ransom to unlock.
- **Tricking You into Giving Up Information:**
    1. **Phishing Attacks:** Deceptive email or messages that pretend to be from a reliable source (bank, social networking site) aim to obtain your personal information or login credentials.
    2. **Smishing:** Like phishing, except using SMS texts in place of emails.
- **Exploiting Weaknesses in Devices and Software:**
    1. **Zero-Day Attacks:** These are extremely dangerous because they take use of weaknesses in software that not even the developers are aware of yet.
    2. **Unpatched Software:** Vulnerabilities in outdated software make it an ideal target for hackers.
- **Social Engineering Tactics:**

1. **Vishing:** Similar to phishing, but phones you and tricks you into giving private information.
2. **Pretexting:** creating a situation in order to obtain your trust and obtain personal data. For instance, a con artist may phone and pose as a tech support representative.

- **Mobile-Specific Threats:**
    1. **Malicious Apps:** These apps—which you may download from unknown sources—can track your location, steal data, or show annoying commercials.
    2. **Unsecured Wi-Fi**: If you use public Wi-Fi without a VPN, you run the risk of having your data stolen.

Cyber Crime against Women and Children

- Some common Cyber Crimes against women and children are as follows:

1. **Cyberstalking:** Repeatedly harassing or following a woman or child online through texts, social media, or other electronic means. For the victim, this can be highly upsetting and terrifying.
2. **Cyberbullying:** Bullying a woman or child online with technology by sending them messages, making posts on social media, or excluding them from online communities.
3. **Online Harassment:** Sending a woman or child abusive or threatening messages via the internet.
4. **Cyber Threats:** Threatening a woman or child online with violence or other damage.
5. **Online Grooming**: Adults making online friends with children in order to get their trust for sexual purpose.

Financial Frauds

- Financial fraud happens when someone steals your money or other financial assets through dishonest or illegal means. There are many different types of financial fraud, but some of the most common ones include:
    1. **Identity theft:** This is when someone steals your personal information, such as your Social Security number or credit card number, and uses it to open new accounts or make purchases in your name.
    2. **Investment fraud:** This is when someone tries to trick you into investing in a fake or risky investment. This can include things like Ponzi schemes and pyramid schemes.

3. **Credit card fraud:** This is when someone uses your credit card number to make unauthorized purchases. This can happen if your card is lost or stolen, or if someone steals your credit card information online.
4. **Bank fraud:** This is when someone steals money from your bank account. This can be done through things like check forgery, ATM skimming, or wire transfer fraud.

Social Engineering Attacks

- Social engineering attacks are the digital equivalent of a sophisticated con artist. Rather than depending on complex hacking methods, they take use of human psychology to trick you into giving private information or doing activities that compromise your security. Here's how it works:
- **Psychological Manipulation:** Attackers trick you using a variety of strategies. They could play on your interest or helpfulness, create a sense of urgency or panic, or even pose as a reliable source like your bank or employer.
    1. **Information Gathering:** Attackers frequently conduct preliminary research to learn more about you. This may include information from public records, social media profiles, or even phishing emails you have previously clicked on. Here are some common types of social engineering attacks:
    2. **Phishing:** Probably the most well-known is this one. You get a message or email (by SMS or social media) that seems to be from a reliable source, such as a tech business or your bank. It may alert you to an issue with your account or present an offer that seems too good to be true. If you click on a link or attachment in the message, malware may download or you may be redirected to a fraudulent website where your login information is being stolen.
    3. **Pretexting:** The hacker creates a fictitious situation, or "pretext," in an effort to win your confidence and obtain data. For instance, they might phone you claiming to be from your IT department and asking for assistance with a computer problem.
    4. **Baiting:** It's similar like holding out a carrot in front of you. In exchange for your personal information, the attacker may offer you free software or special access to a website.

Malware and Ransomware Attacks

- Although both ransomware and malware are harmful software that can cause havoc on your computer or network, they operate slightly differently:

- Any software that is intended to cause harm to a system is referred to as malware. Here are some ways malware can cause problems:
    1. **Stealing Data:** Malware can be created with the intention of monitoring your online activities and stealing private data, such as credit card numbers, passwords, and personal documents.
    2. **Corrupting Files:** Your vital files may be damaged or erased by malware, rendering them unusable or inaccessible.
    3. **Disrupting Operations:** Malware may affect the functionality of your computer, resulting in slowdowns, crashes, or the inability to use specific applications or features.
    4. **Downloading More Malware:** Certain malware can serve as a portal for additional harmful programs to be downloaded, which can lead to a more serious infection.
- There are many different types of malware, including:
    1. **Viruses:** These self-replicates and spread from one device to another, erasing or damaging data.
    2. **Worms:** Though they resemble viruses, they spread quickly by taking advantage of network vulnerabilities.
    3. **Trojan Horses:** They trick users into installing them by pretending to be legitimate software, after which they steal data or damage the device.
    4. **Spyware:** Quietly monitors your activities in the background, gathering passwords and browsing history.
- One particular kind of malware that aims to extract money from you is called ransomware. This is how it operates:
    1. **Infection:** Malicious websites, phishing emails, corrupted software downloads, and other methods are common ways for ransomware to attack your system.
    2. **Encryption:** Ransomware encrypts your files after it's installed, rendering them unreadable and inaccessible.
    3. **Ransom Demand:** Then, a notice demanding payment for a ransom is displayed by the attacker in exchange for a decryption key that unlocks your files. Usually demanded in cryptocurrencies such as Bitcoin, this ransom makes it hard to track down.
- Attacks using ransomware have the potential to be disastrous, particularly for companies whose everyday operations depend on data. Here are a few more things to think about:
- **No Guarantee of Recovery:** There is no assurance that you will have your files returned, even if you manage to pay the ransom.
- **Increased Risk of Data Leaks:** Before encrypting data, some ransomware gangs take it and threaten to make it public if the ransom isn't paid.

Prepared By: Prof. Harsh Joshi

Zero Day and Zero Click Attacks

- Hackers can use both zero-day and zero-click attacks to secretly take advantage of computer systems, although they target weaknesses differently:
- **Zero-Day Attack:**
- **Fresh Flaw:** A zero-day attack takes advantage of a flaw (vulnerability) in firmware, hardware, or software that was just recently found. The software developer or manufacturer has "zero days" to build a repair (patch) because this vulnerability is so new that they aren't even aware of it.
- **Hacker's Advantage:** Attackers can use this vulnerability to initiate their attack before anyone is aware of it because there isn't a fix available. They are particularly deadly because of this.
- **Targets:** Zero-day attacks are frequently employed against well-known systems or businesses that hold significant data, such as vital infrastructure, financial institutions, or governments.
- **Zero-Click Attack:**
- **No User Needed:** In contrast to conventional attacks, which include clicking on a malicious link or opening an infected file, a zero-click attack eliminates all user input.
- **Exploiting Weaknesses:** These attacks depend on pre-existing vulnerabilities in software that you may be familiar with, such as your web browser, operating system, or even a particular application.
- **Silent Strike:** Zero-click attacks are challenging to identify and stop as they don't need your involvement.
- Here's a table summarizing the key differences:

Feature	**Zero – Day Attack**	**Zero – Click Attack**
User Interaction	Not Required (after initial infection)	Not Required
Vulnerability	New, undiscovered	Existing, known
Patch Status	No patch available	Patch may be available

Prepared By: Prof. Harsh Joshi

Difficulty to Detect	Moderate	High

Difference Between Zero-Day Attack & Zero-Click Attack

- Zero-day attacks are more dangerous but less frequent. Their uniqueness makes them more difficult to counter.
- Attacks with zero clicks are increasing in frequency. These kinds of attacks represent a serious concern as additional vulnerabilities are found and exploited by attackers.

Cybercriminals Modus-Operandi

- Although cybercriminals have a script, it is always changing in parallel with technological advancements and security protocols. Below is an explanation of their standard operating procedure:
- 1. **Preparation:**
  - **Target Selection:** Because of the possibility for money, criminals frequently target certain people or organizations. This might be done for disruptive purposes (like attacking vital infrastructure) or for financial gain (like stealing financial data).
  - **Reconnaissance:** They may use a variety of techniques, including as social media profiling, data breaches, or malware infections on target computers, to learn more about their target.
- 2. **Attack:**
  - **Delivery:** They use a variety of techniques to get their malicious code or tools onto the target system, such as phishing emails with malicious attachments, zero-day attacks, or social engineering.
  - **Exploitation:** Once they have a grip, they take advantage of user errors or vulnerabilities they have found to install malware, steal data, or interfere with normal operations.
- 3. **Control and Profit:**
  - **Maintaining Access:** Criminals may try to establish persistent access to the system to get control, carry out more attacks and steal data over time.
  - **Reaching the Objective:** The final objective will change based on the kind of attack. Theft of intellectual property, interruption caused by denial-of-service attacks, and financial gain through ransomware or data theft are all possibilities.

- 4. **Escape and Evasion:**
    - **Covering Tracks:** To prevent discovery, cybercriminals frequently attempt to remove their digital traces. This might include utilizing anonymizing software, erasing logs, or encrypting stolen data.
    - **Cashing Out:** After they've accomplished their objectives, they'll attempt to turn stolen data into money. This can entail utilizing it for illegal transactions, putting it up for sale on the dark web, or requesting ransom payments.
- **Cybercrime is a business:** These thieves are frequently well-organized organizations with specialized knowledge who are always searching for new ways to take advantage of vulnerabilities.
- **There are a variety of motivations:** Monetary gain is a typical one, but there may also be other factors, such as state-sponsored attacks intended to cause disruption or espionage.
- **Maintaining security is a constant effort:** There is no foolproof way to halt cybercrime. Both individuals and businesses must maintain a constant state of alertness and update their defenses.

Reporting of Cyber Crimes

- Reporting cybercrime can take many forms based on the sort of crime and where you live, but here are some broad guidelines to get you started:
    - **Local Law Enforcement:**
        - In cases of crimes like identity theft, internet harassment, or financial frauds, this is frequently the initial point of contact.
        - Head to your local police Go to the police station in your local area and ask about reporting cybercrime. They might collaborate with federal agencies on investigations or establish a separate team dedicated to cybercrime.
    - **Federal Agencies (US Specific):**
        - **Internet Crime Complaint Center (IC3):** This is a central FBI resource for reporting cybercrime. File a complaint online at https://www.ic3.gov/.
        - **Other Agencies:** You may also want to report the specific crime to regulatory bodies such as the Securities and Exchange Commission (SEC) for investment fraud or the Federal Trade Commission (FTC) for identity theft. You can find instructions on how to file a report on their websites.
    - **Specialized Reporting Sites:**
        - There may be national cybercrime reporting portals in some nations.

        - A National Cyber Crime Reporting Portal is available in India, for instance (https://cybercrime.gov.in/).
        - To find such resources in your area, check the websites of your local government or cyber security organizations.
    - **Gather Evidence:**
        - Your case will be stronger the more proof you can offer. For example:
            - Screenshots of malicious emails, texts, or websites
            - Logs or digital footprints connected to the attack
            - Copies of any financial transactions or stolen papers
            - Any other material that may help investigators in understanding the crime
    - **Be Specific in Your Report:**
        - When filing a report, be as detailed as possible about the incident. Include:
        - Dates and times of the crime
        - Websites or online platforms involved
        - Usernames, email addresses, or IP addresses (if known)
        - A clear description of what happened and how you were impacted
    - **Report Immediately:**
        - The sooner you report a crime, the easier it will be for law enforcement to investigate.
        - Don't delay in reporting, as evidence can become harder to recover over time.
    - **Seek Additional Help:**
        - If you've been a victim of cybercrime, there are resources available to help you recover. You can contact:
            - Your local consumer protection agency
            - Non-profit organizations specializing in cybercrime assistance
            - National Cyber Security Alliance: https://staysafeonline.org/

Remedial and Mitigation Measures

- While both remedial and mitigation actions attempt to address security threats, they do so in different ways:
- **Remediation:**
    - **Focus:** Attempt to completely remove the security risk or weakness entirely.

    - **Action:** This involves fixing the issue at its source. For instance, fixing a software fault, changing credentials that have been hacked, or cleaning a system of malware.
    - **Ideal Outcome:** The security risk is totally eliminated, avoiding such attacks in the future.
- **Mitigation:**
    - **Focus:** Tries to decrease a security threat's effects, even if it can't be totally removed.
    - **Action:** This refers to taking steps that prevent the success of attackers or limit the harm they can do. Stronger access controls, data encryption, and user education initiatives on cybersecurity awareness are a few examples.
    - **Ideal Outcome:** Although the security danger is not totally eliminated, its ability to cause harm is significantly reduced. Although an attack might still be feasible, it might be harder to initiate or deal less damage.
- Here's a table summarizing the key differences:

Feature	Remediation	Mitigation
Goal	Eliminate the threat	Reduce impact of threat
Action	Fix the root cause	Implement safeguards
Ideal Outcome	Threat completely gone	Reduced risk of attack

- The optimal strategy is based upon the particular circumstances:
- Give remediation first priority, if you can. The best course of action is always to completely eliminate the threat, if that is possible.
- If full remediation is not an option, mitigation is required. This could be the result of a system vulnerability for which there is currently no patch or both. While a long-term remedy is being researched, mitigation can buy some time.

Prepared By: Prof. Harsh Joshi

- Strong security practices (mitigation) combined with vulnerability fixing (remediation) result in a stronger security posture.
- Here are some additional points to consider:
- Documentation and testing of remediation activities are necessary. Make sure the patch resolves the vulnerability and doesn't cause any new issues.
- It is necessary to routinely assess and adjust mitigation techniques. Your mitigation strategies should also change as threats do.

Legal Perspective of Cyber Crime

- The way that the law interprets and addresses criminal activity involving computers or the internet is known as the legal perspective on cybercrime. In essence, this is how the legal system and law enforcement handle offenses of this nature.
- Due to its ever-changing nature, cybercrime presents a special challenge to judicial systems worldwide. An overview of the legal viewpoint on cybercrime is provided below:
- **Types of Cyber Crimes:**
- Two primary categories can be used to broadly classify cybercrime:
    - Crimes where the computer is used as a tool: These are standard crimes carried out online or through computers, such as fraud, theft, or forgeries.
    - Crimes against computers: These include hacking, virus distribution, and denial-of-service attacks that aim to harm the computer system directly.
- **Legal Frameworks:**
- Several nations have passed specialized laws to fight cybercrime. These laws usually encompass the following:
    - Unauthorized computer system access
    - Data breaches and theft
    - Identity theft and cyber fraud
    - Online harassment and defamation
    - Content related to child sexual abuse and cyberbullying
- **Difficulties with Cybercrime Law:**
    - **Jurisdiction:** Since cybercrime can cross national boundaries, it can be challenging to decide which nation's laws apply.
    - **Quick Evolution:** Cybercriminals are often coming up with new strategies, so it's hard for the law to stay up.
    - Digital Evidence: Collecting and preserving digital evidence for legal purposes is a complicated process that calls for experience.

Examples of Legal Responses:

- The Computer Fraud and Abuse Act (CFAA) and other state-level statutes are in place in the United States.
- The General Data Protection Regulation (GDPR), which is centred on data security and privacy, was established by the European Union.
- The Information Technology Act (2000), which covers a variety of cybercrimes, was passed in India.

IT Act 2000 and Its Amendments

- In India, the main regulation addressing cybercrime and electronic commerce is the Information Technology Act, 2000 (IT Act). It created a legal structure for dealing with cybercrimes, e-governance, and electronic commerce.
- **Features of the IT Act of 2000:**
    - Legal Recognition for Electronic Transactions: Under the Act, digital signatures and electronic records are granted the same legal standing as handwritten signatures and paper-based documents.
    - **E-commerce Facilitation:** By offering a legal framework for digital signatures, online contracts, and safe online transactions, it encourages electronic trade.
    - **Definitions and Penalties of Cybercrimes:** The Act lists a number of cybercrimes, including data theft, hacking, and online harassment. It specifies punishments for various violations.
    - **Cyber Appellate Tribunal:** To settle disagreements resulting from the IT Act, a Cyber Appellate Tribunal was established.
    - **Amendments:** To address new issues, the IT Act has undergone multiple amendments. Among the noteworthy changes are:
        - **Section 66A (subsequently overturned):** This contentious provision addressed the penalties for using communication services to convey “offensive” communications. Its wide wording and potential for abuse drew criticism. In 2015, the Indian Supreme Court ruled that it was unconstitutional.
        - **Initiatives for Data Protection:** Changes have been undertaken to address privacy issues with data and to provide a framework for data protection. A thorough data protection law is still being developed, nevertheless.

Cyber Crime and Offences

- Criminal activity involving computers and networks is known as cybercrime. In these acts, the computer can be either a tool used for the crime or the very target of the crime itself.
- The Indian government's Information Technology Act, 2000 (IT Act) lists a number of offences associated with cybercrime. Below is a summary of some important sections:
    1. **Against Data and Systems:**
        - Section 43: Includes downloading, copying, destroying, or interfering with computer systems or data without authorization.
        - Section 65: Covers tampering with computer source documents, which are the underlying codes and instructions for software.
    2. **Online Content:**
        - Section 66A: Punishes the spread of objectionable content via social media or email.
        - Section 67: Focuses on the spread of pornographic content via electronic means.
        - Section 67A: Focuses on the transmission or publication of content that includes explicit sexual actions.
    3. **Identity and Privacy:**
        - Section 66B: Makes it illegal to obtain or hold onto stolen communication or computer equipment.
        - Section 66C: Penalizes identity theft, which is the act of posing online as someone else.
        - Section 72: Prohibits the leaking of information in violation of valid contracts, so violating privacy and confidentiality.
    4. **Other Offences:**
        - Section 71: Punishes fraud, which includes the transmission of misleading information online.
        - Section 73: Penalizes the publication of a bogus electronic signature certificate.
        - Section 74: Focusing on distributing data for misleading ends.
- The IT Act can be applied to offences committed outside India if they impact a computer system located in India.
- The Act also allows for confiscation of computer equipment used in cybercrimes.

Prepared By: Prof. Harsh Joshi

Organizations Dealing with Cyber Crime and Cyber Security in India

- Here are some of the important organizations dealing with Cyber Crime and Cyber Security in India:
- **Government Agencies**:
  - **Indian Computer Emergency Response Team (CERT-In):** The national nodal agency for cyber security incidents and threats. It is responsible for handling cyber security emergencies, issuing advisories and vulnerabilities, and coordinating cyber security efforts.
  - **National Critical Information Infrastructure Protection Centre (NCIIPC):** A designated authority to protect Critical Information Infrastructure (CII) in India. It works towards securing CII assets and promoting a culture of cyber security.
  - **Indian Cyber Crime Coordination Centre (I4C):** A national initiative to combat cybercrime in India. It facilitates reporting of cybercrimes, coordinates investigation efforts of various law enforcement agencies, and provides training and resources to improve cybercrime investigation capabilities.
- **Industry Bodies:**
  - **Data Security Council of India (DSCI):** A non-profit industry body focused on promoting data protection in India. It provides best practices, standards, and initiatives to help organizations implement effective data security measures.
  - **Cyber Security Association of India (CSAI):** A not-for-profit organization working towards creating a secure cyber space in India. It brings together stakeholders from government, industry, and academia to collaborate on cyber security issues.

Prepared By: Prof. Harsh Joshi

UNIT-3
Social Media Overview and Security

Social Networks:
In the context of technology and the internet, refer to online platforms that enable users to connect, communicate, and share information with one another. These networks facilitate the creation and maintenance of relationships, both personal and professional, in a virtual space. Users typically create profiles, share content, and engage with others through various features provided by the platform.

Components of Social Networks:

- **User Profiles:**

Users create personal profiles containing information such as their name, photo, bio, and interests. These profiles serve as digital representations of individuals on the platform.

- **Connections and Friends:**

Users can connect with or "friend" others on the platform, establishing a network of connections. This allows them to see and interact with each other's content.

- **Content Sharing:**

Social networks enable users to share various types of content, including text posts, photos, videos, links, and more. This content is often shared on users' profiles or in designated spaces like timelines or feeds.

- **Communication Features:**

Most social networks offer communication features such as messaging, comments, and likes. These tools allow users to interact with each other's content and have private conversations.

- **Privacy Settings:**

Users have control over the visibility of their content and personal information through privacy settings. They can choose to share content publicly, with specific groups, or privately with selected individuals.

- **Groups and Communities:**

Many social networks allow users to join or create groups based on shared interests, affiliations, or goals. These communities provide a space for like-minded individuals to connect and engage.

- **Notifications:**

Users receive notifications for various activities, such as new friend requests, comments on their posts, or updates from groups they follow. Notifications help users stay informed about their online interactions.

Prepared By: Prof. Harsh Joshi

Types of Social Networks:

- **Facebook:**

One of the earliest and most widely used social networks, Facebook allows users to connect with friends, share updates, and join groups.

- **Instagram:**

A platform focused on visual content, Instagram allows users to share photos and videos, follow others, and discover content through hashtags.

- **Twitter:**

Known for its microblogging format, Twitter enables users to share short text-based posts called tweets. It is often used for real-time updates and discussions.

- **LinkedIn:**

Geared towards professionals, LinkedIn is a platform for networking, job searching, and professional content sharing.

- **Snapchat**:

Popular among younger users, Snapchat allows for the sharing of ephemeral photos and videos that disappear after a short time.

- **WhatsApp:**

A messaging app that also supports the sharing of status updates, photos, and videos. It is widely used for personal and group communication.

- **YouTube:**

While primarily a video-sharing platform, YouTube incorporates social features such as comments, likes, and subscriptions, fostering a community around content creators.

Social Networks and Society

- **Communication:**

Social networks have transformed the way people communicate, allowing for instant and global interactions.

- **Information Sharing:**

Users can share and consume vast amounts of information on diverse topics, contributing to the democratization of information.

- **Community Building:**

Social networks enable the formation of communities and support groups, connecting individuals with shared interests or experiences.

- **Business and Marketing:**

Businesses use social networks for marketing, customer engagement, and building brand awareness.

Prepared By: Prof. Harsh Joshi

Social Media Monitoring

Social media monitoring, also known as social media listening or social media intelligence, involves the process of tracking and analyzing social media channels for mentions, discussions, and sentiments related to a brand, product, service, or specific topics.

Aspects:

- **Brand Reputation Management:**

Organizations use social media monitoring to track mentions of their brand and manage their online reputation. This helps in addressing customer concerns and engaging with the audience.

- **Competitor Analysis:**

Monitoring social media allows businesses to keep an eye on their competitors, understanding market trends, customer sentiments, and potential areas for improvement.

- **Customer Engagement:**

Companies can use social media monitoring to identify and engage with their target audience, respond to customer inquiries, and gain insights into customer preferences.

- **Crisis Management:**

Real-time monitoring enables organizations to identify potential crises, such as negative sentiment spikes, allowing for prompt responses and crisis mitigation.

- **Market Research:**

Social media monitoring provides valuable data for market research, helping businesses understand consumer behavior, preferences, and emerging trends.

Hashtags:

Hashtags are keywords or phrases preceded by the '#' symbol used on social media platforms to categorize content and make it discoverable by users interested in a specific topic.

Aspects:

- **Content Categorization:**

Hashtags help organize content, making it easier for users to find and participate in discussions related to specific themes or events.

- **Trend Identification:**

Trending hashtags reflect popular topics and discussions on social media. Businesses leverage trending hashtags for marketing campaigns and brand visibility.

- **Campaigns and Movements:**

Hashtags are often used to promote campaigns, events, and social movements, encouraging users to contribute and share content related to a specific cause.

Prepared By: Prof. Harsh Joshi

- **Branding:**

Unique and memorable hashtags can be used as part of a brand's identity, helping users associate the hashtag with the brand and fostering engagement.

- **Community Building:**

Hashtags contribute to the formation of online communities, enabling like-minded individuals to connect and share content on common interests.

Viral Content

Definition: Viral content refers to online content—such as videos, images, or articles—that spreads rapidly across the internet, reaching a large audience in a short period. Virality often occurs through social media sharing.

Aspects:

- **Sharability:**

Viral content is highly shareable, often invoking emotional responses or providing valuable and entertaining information that compels users to share with their networks.

- **User-Generated Content:**

Viral content is not always created by brands; it often originates from users sharing content they find interesting, humorous, or relatable.

- **Platform-Specific Strategies:**

Different social media platforms have unique features and algorithms that can contribute to content going viral. Understanding these nuances is crucial for creating shareable content.

- **Influencer Impact:**

Influencers can play a significant role in making content go viral. Their large following and audience trust can amplify the reach of content.

- **Trend Riding:**

Viral content often aligns with current trends, cultural moments, or relevant events. Creating content that taps into popular trends can increase its likelihood of going viral.

Prepared By: Prof. Harsh Joshi

Social media Privacy & Challenges

Social media has become an integral part of daily life, connecting people globally and facilitating communication, collaboration, and information sharing. However, this interconnectedness brings forth a myriad of challenges, particularly concerning social media privacy.

- **Defining Social Media Privacy:**

Social media privacy refers to the control individuals have over their personal information shared on social networking platforms. It encompasses the safeguarding of sensitive data, such as personal details, location information, and communication exchanges, from unauthorized access, misuse, or exploitation.

Components of Social Media Privacy:

1. **Profile Privacy Settings:**

Users can often customize the visibility of their profiles, choosing who can view their information and posts. This includes options for public, friends-only, or custom settings.

- **Data Collection and Sharing:**

Social media platforms collect vast amounts of user data to personalize content and ads. Privacy concerns arise when platforms share this data with third parties without explicit consent.

- **Communication Privacy:**

The privacy of messages and conversations is crucial. End-to-end encryption in messaging apps enhances the confidentiality of private communications.

- **Geolocation Services:**

Many social media platforms offer geotagging features, indicating users' physical locations. Managing geolocation settings is vital for protecting personal safety and privacy.

- **Third-Party Applications:**

Users often integrate third-party applications with social media accounts for additional functionalities. Privacy risks emerge when these apps access excessive user data.

- **User-generated Content:**

Privacy concerns arise when users share content, including photos, videos, and status updates, without considering potential implications for their personal privacy.

Challenges in Social Media Privacy:

- **Data Breaches:**

Data breaches pose a significant threat to social media privacy. When platforms experience security vulnerabilities, user data, including personal information, login credentials, and communication history, may be compromised. These breaches can have severe consequences, leading to identity theft, financial loss, and reputational damage.

Prepared By: Prof. Harsh Joshi

- **User Awareness and Education:**

Many users lack awareness of the privacy settings and features offered by social media platforms. Inadequate understanding of these settings results in unintentional oversharing and exposure of sensitive information. Education initiatives are crucial to empower users to make informed privacy decisions.

- **Default Settings and Opt-Out Models:**

Social media platforms often set default privacy settings that prioritize visibility and data collection. Users may need to actively opt-out or customize settings for enhanced privacy, leading to a situation where individuals inadvertently share more than intended.

- **User Tracking and Profiling:**

Social media platforms employ sophisticated algorithms to track user behavior, preferences, and interactions. This data is used to create detailed user profiles for targeted advertising. While this enhances the user experience, concerns arise regarding the extent of user profiling and the potential for manipulation.

- **Invasive Advertising Practices:**

Social media platforms leverage user data to deliver personalized advertisements. While targeted advertising is common, concerns arise when platforms share user data with advertisers without clear consent or when ads become excessively intrusive, impacting user experience.

6. **Social Engineering and Phishing Attacks:**

Cybercriminals often exploit social media to conduct social engineering attacks, manipulating users into divulging sensitive information. Phishing attempts through fake profiles or deceptive messages pose threats to user privacy and security.

7. **Cross-platform Data Sharing:**

Users often connect multiple social media accounts and third-party apps, leading to cross-platform data sharing. The interconnectedness poses challenges in controlling the flow of information between platforms, increasing the risk of data exposure.

8. **Public vs. Private Information:**

Determining what information is public or private on social media platforms can be challenging. Users may unintentionally share personal details, assuming certain information is private when it is, in fact, accessible to a broader audience.

9. **Regulatory Compliance:**

Navigating the landscape of privacy regulations and ensuring compliance is a complex challenge for social media platforms. Adhering to evolving privacy laws, such as the General Data Protection Regulation (GDPR), requires continuous updates and robust systems.

10. **Deepfake Technology:**

Advancements in deepfake technology pose a threat to user privacy on social media. Deepfakes, manipulated media content that appears authentic, can be used

to create misleading or harmful content, impacting individuals' reputations and trust.

Protecting Social Media Privacy:

- **Privacy Settings and Controls:**

Users should regularly review and customize their privacy settings on social media platforms. Adjusting visibility preferences, limiting data sharing, and enabling two-factor authentication contribute to enhanced privacy.

- **User Education:**

Platforms should invest in user education initiatives to raise awareness about privacy settings, potential risks, and best practices. Providing clear and accessible information empowers users to make informed decisions.

- **Transparent Data Policies:**

Social media platforms should maintain transparent data policies, clearly outlining how user data is collected, processed, and shared. Transparent communication builds trust and allows users to make informed choices.

- **Consent Mechanisms:**

Platforms must implement robust consent mechanisms, ensuring users have clear options to opt-in or opt-out of data sharing practices. Providing granular control over permissions enhances user trust and privacy.

- **Enhanced Security Measures:**

Platforms should prioritize cybersecurity measures to protect against data breaches. Implementing encryption protocols, regular security audits, and swift response mechanisms to address vulnerabilities are critical.

- **Ethical Advertising Practices:**

Social media platforms should adopt ethical advertising practices, ensuring that targeted advertising respects user privacy. Striking a balance between personalized advertising and user consent is essential.

- **Cross-platform Integration Safeguards:**

Platforms should enhance safeguards for cross-platform data sharing. Implementing clear guidelines and restrictions on third-party app integrations minimizes the risk of unintended data exposure.

- **Privacy by Design:**

Adopting a privacy-by-design approach involves integrating privacy considerations into the development of social media features and functionalities. This ensures that privacy is a fundamental aspect of the user experience.

- **Strengthening Regulatory Compliance:**

Social media platforms should stay abreast of evolving privacy regulations and proactively implement measures to comply with legal requirements. Collaborating with regulatory bodies and stakeholders fosters a culture of responsible data handling.

- **Combatting Deepfakes:**

Platforms should invest in advanced technology to detect and combat deepfake content. Implementing measures to authenticate media content and raising user awareness about the existence of deepfakes can mitigate their impact.

Future of Social Media Privacy:

- **Privacy-Centric Platforms:**

There is a growing trend toward privacy-centric social media platforms that prioritize user data protection. These platforms emphasize end-to-end encryption, reduced data collection, and enhanced user control over privacy settings.

- **Decentralized Identity and Blockchain:**

The integration of blockchain technology and decentralized identity systems holds promise for enhancing social media privacy. These technologies offer secure and transparent mechanisms for managing user identities and data.

- **Enhanced Privacy Laws:**

As privacy concerns escalate, regulatory bodies are likely to introduce and strengthen privacy laws. This includes stricter regulations on data collection, transparency requirements, and severe penalties for non-compliance.

- **User Empowerment:**

The future will witness a shift toward empowering users with more control over their data. Features that allow users to track and manage how their data is utilized, shared, and accessed will become standard.

- **Technological Solutions:**

Advancements in privacy-preserving technologies, such as homomorphic encryption and differential privacy, may play a crucial role in mitigating privacy risks. These technologies enable data analysis without compromising individual privacy.

- **Global Collaboration:**

Addressing social media privacy challenges requires global collaboration. Governments, tech companies, and international organizations will likely work together to establish common standards and frameworks for protecting user privacy.

- **Privacy Audits and Certification:**

Privacy audits and certification processes may become more prevalent, with platforms undergoing regular assessments to demonstrate their adherence to privacy principles. Users may prioritize platforms with verified privacy certifications.

Opportunities and pitfalls in online Social network

Online Social networks have become integral to modern communication, connecting individuals across the globe and shaping how people interact, share information, and build relationships. While these platforms offer numerous opportunities, they also present pitfalls that can impact individuals, communities, and societies.

Online social networks offer a plethora of opportunities for connection, expression, and collaboration. However, acknowledging and addressing the associated pitfalls is crucial for creating a digital landscape that is both empowering and responsible. By fostering a culture of digital literacy, user empowerment, and ethical design, online social networks can evolve into spaces that amplify positive opportunities while mitigating potential harms. Balancing the benefits and challenges requires a collective effort from users, platforms, regulators, and society at large.

Opportunities

1. **Global Connectivity:**

Online social networks break down geographical barriers, allowing people to connect with others globally. This facilitates cross-cultural communication, collaboration, and the exchange of ideas on an unprecedented scale.

2. **Information Sharing and Awareness:**

Social networks are powerful tools for disseminating information, raising awareness about important issues, and fostering discussions on topics ranging from social justice to scientific advancements.

3. **Business and Professional Networking:**

Platforms like LinkedIn provide opportunities for professional networking, job searches, and skill development. Businesses leverage social networks for marketing, customer engagement, and building brand loyalty.

4. **Community Building:**

Online communities on social networks allow like-minded individuals to come together, share experiences, and support one another. These communities can be centered around hobbies, causes, or shared identities.

5. **Educational Resources:**

Social networks serve as platforms for educational content, facilitating learning through videos, articles, and discussions. This democratization of information enhances access to diverse educational resources.

6. **Activism and Social Movements:**

Social networks play a pivotal role in organizing and amplifying activism and social movements. They provide a platform for marginalized voices, enabling them to reach a wider audience and effect societal change.

Prepared By: Prof. Harsh Joshi

7. **Creativity and Expression:**

Platforms like Instagram, YouTube, and TikTok empower individuals to showcase their creativity. Users can express themselves through visual content, music, and various forms of digital art.

8. **Real–Time Communication:**

Social networks enable instant communication through messaging features, keeping people connected in real-time. This facilitates quick information sharing and strengthens personal and professional relationships.

Pitfalls

1. **Privacy Concerns:**

Privacy breaches and concerns about the misuse of personal data are prevalent. Users may inadvertently share sensitive information, and the platforms themselves may face scrutiny for their data-handling practices.

2. **Cyberbullying and Harassment:**

Online social networks can become platforms for cyberbullying and harassment. Users may experience targeted attacks, leading to mental health issues and a toxic online environment.

3. **Spread of Misinformation:**

The rapid dissemination of information on social networks can lead to the spread of misinformation and fake news. This poses risks to public discourse, trust, and even public safety.

4. **Filter Bubbles and Echo Chambers:**

Algorithms that curate content based on user preferences may contribute to filter bubbles and echo chambers. Users may be exposed only to information that aligns with their existing beliefs, limiting diverse perspectives.

5. **Addiction and Mental Health Impact:**

Excessive use of social networks can contribute to addiction and negatively impact mental health. The constant need for validation, comparison, and fear of missing out (FOMO) are common challenges.

6. **Exploitation of Vulnerable Users:**

Vulnerable individuals, including minors, may be susceptible to exploitation on social networks. This includes online grooming, identity theft, and exposure to inappropriate content.

7. **Online Radicalization:**

Extremist ideologies and radicalization can find fertile ground on social networks. Platforms may inadvertently become spaces for the recruitment and spread of extremist content.

Prepared By: Prof. Harsh Joshi

8. **Erosion of Face-to-Face Interaction:**

Overreliance on online communication may contribute to a decline in face-to-face interaction. This can impact social skills, empathy, and the depth of interpersonal relationships.

Balancing Opportunities and Pitfalls

1. **User Education:**

Promote user education on privacy settings, digital literacy, and responsible online behavior. Empower users to critically evaluate information and navigate potential pitfalls.

2. **Algorithmic Transparency:**

Advocate for greater transparency in algorithms to mitigate filter bubbles and ensure diverse content exposure. Platforms should disclose how content is curated and recommend resources that challenge users' perspectives.

3. **Digital Well-being Features:**

Platforms can implement features that promote digital well-being, such as usage tracking, reminders for breaks, and tools to limit notifications. Prioritizing mental health support is essential.

4. **Stricter Regulation and Oversight:**

Governments and regulatory bodies should establish and enforce stricter regulations on data privacy, online content, and user protection. Oversight can help hold platforms accountable for their impact on users and society.

5. **Community Moderation:**

Implement robust community moderation policies to combat cyberbullying, harassment, and the spread of harmful content. Encourage users to report violations and foster a safe online environment.

6. **Diverse Representation:**

Promote diverse representation on social networks to ensure that voices from all backgrounds are heard. Platforms should actively address issues of discrimination and bias.

7. **Ethical Design Principles:**

Adopt ethical design principles that prioritize user well-being. This includes minimizing addictive features, providing clear privacy choices, and designing interfaces that prioritize user agency.

8. **Collaboration and Research:**

Encourage collaborative efforts between platforms, researchers, and advocacy groups to address emerging challenges. Conduct research on the impact of social networks on society and implement evidence-based solutions.

Prepared By: Prof. Harsh Joshi

Flagging and reporting of inappropriate content

Flagging and reporting systems play a crucial role in maintaining a safe and respectful online environment. These systems empower users to identify and report content that violates community guidelines or standards.

Social Media Platforms:

1. **Facebook:**

- **Flagging Process:**
  - Click on the three dots next to the post or comment.
  - Select "Find support or report post."
  - Follow the on-screen instructions to report the content.
- **Reporting Process:**
  - Visit the user's profile.
  - Click on the three dots on their cover photo.
  - Select "Find support or report profile."
  - Follow the instructions to report the account.

2. **Twitter:**

- **Flagging Process:**
  - Click on the down arrow next to the tweet.
  - Select "Report Tweet."
  - Choose the reason for reporting and follow the instructions.
- **Reporting Process:**
  - Visit the user's profile.
  - Click on the three dots next to their profile.
  - Select "Report."
  - Choose the reason for reporting and follow the instructions.

3. **Instagram:**

- **Flagging Process:**
  - Click on the three dots above the post.
  - Select "Report."
  - Choose the reason for reporting and follow the instructions.
- **Reporting Process:**
  - Visit the user's profile.
  - Click on the three dots in the top right.
  - Select "Report."
  - Choose the reason for reporting and follow the instructions.

4. **LinkedIn:**

- **Flagging Process:**
  - Click on the three dots next to the post or comment.
  - Select "Report this."
  - Choose the reason for reporting and follow the instructions.
- **Reporting Process:**

Prepared By: Prof. Harsh Joshi

- Visit the user's profile.
- Click on the three dots next to their profile.
- Select "Report/Block."
- Choose the reason for reporting and follow the instructions.

Video Sharing Platforms:

1. **YouTube:**

- **Flagging Process:**
  - Click on the three dots below the video.
  - Select "Report."
  - Choose the reason for reporting and follow the instructions.
- **Reporting Process:**
  - Visit the user's channel.
  - Click on the flag icon.
  - Choose the reason for reporting and follow the instructions.

2. **TikTok:**

- **Flagging Process:**
  - Click on the arrow in the bottom right of the video.
  - Select "Report."
  - Choose the reason for reporting and follow the instructions.
- **Reporting Process:**
  - Visit the user's profile.
  - Click on the three dots in the top right.
  - Select "Report" and follow the instructions.

Online Forums:

1. **Reddit:**

- **Flagging Process:**
  - Click on "Report" below the post or comment.
  - Choose the reason for reporting and follow the instructions.
- **Reporting Process:**
  - Visit the user's profile.
  - Click on the three dots in the top right.
  - Select "Report user" and follow the instructions.

2. **Quora:**

- **Flagging Process:**
  - Click on the three dots next to the content.
  - Select "Report."
  - Choose the reason for reporting and follow the instructions.
- **Reporting Process:**
  - Visit the user's profile.
  - Click on the three dots next to their profile.
  - Select "Report."
  - Choose the reason for reporting and follow the instructions.

General Guidelines:

- **Choose the Appropriate Category:**

Platforms often provide a list of categories or reasons for reporting. Select the most accurate category that describes the issue.

- **Provide Details:**

When reporting, include specific details about the inappropriate content or behavior. This helps the platform assess the report more effectively.

- **Anonymous Reporting:**

Some platforms allow users to report content anonymously to protect the reporter's identity.

- **Follow Platform Policies:**

Familiarize yourself with the platform's community guidelines to understand what constitutes inappropriate content.

- **Feedback on Reports:**

Some platforms provide feedback on the status of reported content, informing users about actions taken.

Laws regarding posting of inappropriate content in India

India, like many countries, has established legal frameworks to address the posting of inappropriate content, especially in the digital realm. With the growing influence of social media and online platforms, the need for robust laws to govern online behavior has become increasingly evident.

India's legal framework concerning the posting of inappropriate content reflects a mix of traditional laws and specific regulations tailored for the digital age. As technology continues to evolve, lawmakers, legal practitioners, and digital platforms must collaborate to address emerging challenges and ensure a fair, just, and secure online environment. Balancing the protection of individuals from online harm with the preservation of fundamental rights remains an ongoing task in this dynamic landscape.

Defamation Laws:

- **Indian Penal Code (IPC) Sections 499 and 500:**

Defamation laws in India are primarily governed by Sections 499 and 500 of the IPC. These sections criminalize the act of intentionally defaming a person, either through spoken or written words or any other form of communication. Posting false and damaging information about an individual on digital platforms can fall under the purview of these provisions.

- **Section 66A of the Information Technology (IT) Act (Repealed):**

While Section 66A of the IT Act was widely criticized for being vague and overbroad, it was initially aimed at addressing offensive or menacing messages sent through communication services. However, the Supreme Court of India, in 2015,

struck down Section 66A, stating that it violated the right to freedom of speech and expression.

Obscenity Laws:

- **Section 67 of the Information Technology (IT) Act:**

This section deals with the publishing or transmitting of obscene material in electronic form. It specifically addresses the digital dissemination of sexually explicit content. Posting, sharing, or distributing obscene material online can lead to legal consequences under this provision.

- **Section 292 of the Indian Penal Code (IPC):**

Section 292 of the IPC criminalizes the sale, distribution, or public exhibition of obscene materials, including books, pamphlets, and any other objects. While this section is not specific to online content, it can be applied to inappropriate digital content that falls under the definition of obscenity.

Cyberbullying Laws:

- **Section 66E of the Information Technology (IT) Act:**

This section addresses the violation of privacy by capturing, publishing, or transmitting the image of a private area of any person without their consent. It aims to protect individuals from online harassment involving the non-consensual sharing of intimate images, commonly known as "revenge porn."

- **Section 354D of the Indian Penal Code (IPC):**

This section, added through the Criminal Law (Amendment) Act, 2013, deals with the offense of stalking. Cyberstalking, which involves persistent unwanted online attention and communication, can be punishable under this provision.

Hate Speech and Incitement to Violence:

- **Section 153A and 505 of the Indian Penal Code (IPC):**

These sections address offenses related to promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc. Posting content that constitutes hate speech and has the potential to incite violence or disharmony may attract legal consequences under these sections.

Online Harassment and Threats:

- **Section 509 of the Indian Penal Code (IPC):**

Section 509 deals with the offense of insulting the modesty of a woman, including online harassment. Posting sexually colored remarks, gestures, or any other act that intrudes upon the privacy of women can be punishable under this provision.

- **Section 506 of the Indian Penal Code (IPC):**

This section addresses criminal intimidation, including online threats. Any communication that causes fear for one's safety or property can fall under the ambit of this provision.

Child Sexual Abuse Material (CSAM) Laws:

- **Protection of Children from Sexual Offences (POCSO) Act:**

The POCSO Act, 2012, is a dedicated legislation to address sexual offenses against children. Posting, sharing, or distributing child sexual abuse material online is a severe offense under this Act, with stringent penalties.

- **Section 67B of the Information Technology (IT) Act:**

This section deals specifically with the punishment for publishing, transmitting, or causing the publication or transmission of material depicting children in sexually explicit acts. It complements the provisions of the POCSO Act in the digital domain.

Liability of Intermediaries:

- **Section 79 of the Information Technology (IT) Act:**

This section provides safe harbor provisions for intermediaries, such as social media platforms, as long as they comply with due diligence requirements. However, intermediaries can lose their immunity if they fail to observe the prescribed guidelines and knowingly host or publish unlawful content.

Legal Framework for Content Takedowns:

- **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021:**

Enacted in February 2021, these rules provide a comprehensive framework for digital media and online intermediaries. They outline procedures for content takedowns, the appointment of grievance officers, and compliance with a code of ethics. Failure to comply with these rules can result in the loss of intermediary immunity.

Challenges and Criticisms:

While these laws provide a legal framework to address inappropriate content, challenges and criticisms persist:

- **Ambiguity and Vagueness:**

Some laws, such as those related to hate speech, have been criticized for their ambiguity, potentially leading to overreach.

- **Slow Legal Processes:**

Legal proceedings can be slow, and the backlog of cases may hinder timely justice.

- **Freedom of Expression Concerns:**

Balancing the need to curb inappropriate content with the protection of freedom of expression remains a challenge.

- **Global Platforms and Jurisdictional Issues:**

The global nature of online platforms raises questions about jurisdiction and enforcement, especially when platforms are based outside India.

Prepared By: Prof. Harsh Joshi

Best practices for the use of Social media

Social media has become an integral part of modern communication, offering individuals and businesses powerful tools for connection, expression, and engagement. However, the use of social media comes with responsibilities and considerations to ensure a positive and secure online experience.

Privacy Settings:

- **Regularly Review Settings:**

Periodically review and adjust your privacy settings on each social media platform. Be aware of who can see your posts, friend requests, and personal information.

- **Customize Audience:**

Tailor your audience for each post. Not every post needs to be shared with the same group of people. Use privacy settings to control who sees what.

- **Limit Personal Information:**

Be cautious about sharing sensitive personal information, such as your address or phone number, publicly on social media. Consider sharing such details privately if necessary.

Authenticity and Transparency:

- **Use Real Information:**

Provide accurate information on your profile. Authenticity builds trust, and misleading information can lead to misunderstandings.

- **Disclose Relationships:**

Clearly disclose relationships with brands, products, or services if you are endorsing or promoting them on social media. Transparency is essential for maintaining credibility.

- **Verify Information:**

Before sharing news or information, verify its accuracy. Misinformation spreads quickly on social media, and sharing false information can have real-world consequences.

Responsible Posting:

- **Think Before You Post:**

Consider the potential impact of your posts. Avoid posting content that may be offensive, discriminatory, or harmful to others.

- **Avoid Over-Sharing:**

Be mindful of oversharing personal details. Strike a balance between sharing updates and maintaining a level of privacy.

- **Respect Others' Privacy:**

Obtain consent before sharing images, tagging others, or sharing personal stories involving friends and family. Respect their privacy preferences.

Cybersecurity Practices:

- **Strong Passwords:**

Use strong, unique passwords for each social media account. Regularly update passwords and enable two-factor authentication for added security.

Prepared By: Prof. Harsh Joshi

- **Beware of Phishing:**

Be cautious of phishing attempts. Avoid clicking on suspicious links, and verify the authenticity of messages before sharing personal information.

- **Secure Mobile Devices:**

Secure your mobile devices with passwords or biometric authentication. Keep your devices updated with the latest security patches.

Mindful Engagement:

- **Positive Interaction:**

Foster positive interactions on social media. Be supportive, respectful, and constructive in your comments and replies.

- **Handle Disagreements Respectfully:**

Disagreements are natural, but handle them with respect. Avoid engaging in online arguments that can escalate quickly.

- **Report Inappropriate Content:**

If you come across inappropriate or harmful content, use platform-specific reporting mechanisms to bring it to the attention of administrators.

Time Management:

- **Set Limits:**

Set limits on your social media usage. Excessive time on these platforms can impact mental health and productivity.

- **Designate Social Media-Free Time:**

Designate specific times or areas where you won't engage with social media. This helps maintain a healthy balance between online and offline activities.

- **Be Mindful of Notifications:**

Manage notification settings to prevent constant interruptions. Consider turning off non-essential notifications.

Understand Platform Policies:

- **Read Terms of Service:**

Familiarize yourself with the terms of service and community guidelines of each social media platform you use. Adherence to these guidelines is crucial for a positive experience.

- **Stay Informed about Updates:**

Platforms regularly update their policies. Stay informed about changes to ensure continued compliance and understanding of the rules.

- **Respect Copyright:**

Respect copyright laws. Avoid using copyrighted material without permission, and give proper credit when sharing content created by others.

Professionalism for Businesses:

- **Consistent Branding:**

Maintain consistent branding across platforms. Use the same logo, color scheme, and messaging to strengthen your brand identity.

- **Respond Promptly:**

Respond promptly to customer inquiries or comments. Timely responses show professionalism and dedication to customer satisfaction.

- **Create Valuable Content:**

Share content that adds value to your audience. Educational, entertaining, and informative content contributes to a positive brand image.

Regular Audits:

- **Review Connected Apps:**

Periodically review and revoke access to third-party apps connected to your social media accounts. This helps ensure the security of your accounts.

- **Audit Your Friends/Followers:**

Regularly review your friends or followers. Remove or block accounts that seem suspicious or no longer align with your interests.

- **Update Profile Information:**

Keep your profile information up to date. Changes in employment, contact information, or interests should be reflected on your social media profiles.

Continuous Learning:

- **Stay Informed about Trends:**

Social media is dynamic. Stay informed about emerging trends, new features, and changes in algorithms to adapt your strategy accordingly.

- **Educate Yourself on Privacy Settings:**

Stay updated on privacy settings and features provided by each platform. Continuous education helps you make informed decisions about your online presence.

- **Participate in Webinars and Workshops:**

Attend webinars or workshops on social media best practices and digital literacy. Learning from experts can enhance your understanding of responsible online behavior.

Prepared By: Prof. Harsh Joshi

Unit-4
E-commerce and Digital Payments

E-Commerce: Ecommerce or "electronic commerce" is the trading of goods and services online. The internet allows individuals and businesses to buy and sell an increasing amount of physical goods, digital goods, and services electronically.

Components of E-Commerce

1. **User:** This may be individual / organization or anybody using the e-commerce platforms.

2. **E-commerce Vendors:** This is the organization/ entity providing the user, goods/ services. E.g.: www.flipkart.com.

E-commerce Vendors further needs to ensure following for better, effective and efficient transaction.

- **Suppliers and Supply Chain Management:** For effectiveness, they need to ensure that –
  - Enoughand the right goods suppliers.
  - Suppliers should be financially and operational safe.
  - Suppliers are able toprovide real-time stock inventory.
  - Order to delivery time is short.
- **Warehouse operations:** From this place online retailers pick products, pack them and prepare those products to be delivered. Many e-commerce companies are investing huge amounts of money in automating the warehouses.
- **Shipping and returns:** Shipping is supplementary and complementary to warehouse operations. Fast and safe returns is also very important for e-commerce vendors.
- **E-Commerce catalogue and product display:** Proper displayincluding product details, technical specifications, is necessary for better sales.

– Marketing and loyalty programs: Loyalty programs is to establish a long- term relationship with customer.E.g. In airline industry, customer can get good discount/ free tickets based on loyalty points accumulated.

- **Showroom and offline purchase:** Few e-commerce vendors over period have realized that their products can be sold fast if customers are able to feel / touch / see those products. These vendors have opened outlets for customer experience of their products.

Prepared By: Prof. Harsh Joshi

- **Different Ordering Methods:** These are the way customer can place his/her order, say Cash on Delivery is today most preferred method.
- **Guarantees:** The product/service guarantee associated with product/service being sold e.g. Money back guarantees.
- **Privacy Policy:** Customers are very concerned about the information that they are sharing. E - commerce vendors need to clearly explain them what the vendor plan to do with the information they have collected.
- **Security:** Vendor website needs to state that online data used to transact is safe that vendors is using appropriate security including security systems like SSL (Secure Socket Layer). This guarantees that the data provided by customer will not fall into the hand of a hacker.

3. **Technology Infrastructure:** This includes Server computers apps etc.

Computers, Servers and Database

These are the backbone for the success of the venture. They store the data/program used to run the whole operation of the organization.

Mobile Apps

- Smartphone's and tablets have become a dominant form of computing, with many more smartphones being sold than personal computers.
- Developing mobile app is expensive,and it will have to be developed on two major platform i.e. iPhone and Android. Another option is to create a website that is mobile-friendly.

Digital Libraries: Digital libraries can vary immensely in size and scope, and can be maintained by individuals, organizations, or affiliated with established physical library buildings or institutions, or with academic institutions. The digital content may be stored locally, or accessed remotely via computer networks.

Data Interchange: Data Interchange is an electronic communication of data. For ensuring the correctness of data interchange between multiple players in e-commerce, business specific protocolsare being used. There are defined standards to ensure seamless communication in e-commerce.

4. **Internet / Network:** This is the key to success of e-commerce transactions.

- Internet connectivity is important for any e-commerce transaction to go through.
- The faster net connectivityleads to better e-commerce. Many mobile companies in India have launched 4G services.

- The success of e-commerce trade depends upon the internet capability of organization. The latest communication technologies like 4G, 5G have already made in-roads in India.

5. **Web portal:** This shall provide the interface through which an individual/organization shall perform e-commerce transactions.

Web Portal is the application through which user interacts with the e- commerce vendor. The front end through which user interacts for an e- commerce transaction. These web portals can be accessed through desktops/ laptops/PDA/hand- held computing devices/ mobiles and now through smart TVs.

6. **Payment Gateway:** The payment mode through which customers shall make payments. Payment gateway represents the way e-commerce / m-commerce vendors collects their payments. Examples are :

Credit / Debit Card Payments, Online bank payments, Vendors own payment wallet, Third Party Payment wallets, like SBI BUDDY or PAYTM, Cash on Delivery (COD) and Unified Payments Interface (UPI).

Elements of Good E-Commerce Security

In order to protect information, a solid, comprehensive application security framework is needed for *analysis* and *improvement*. This application security framework should be able to list and cover all aspects of security at a basic level. It should incorporate the following six parts:

- Security elements that need to be preserved: availability, utility, integrity, authenticity, confidentiality, nonrepudiation
- Sources of loss of these elements: abuse, misuse, accidental occurrence, natural forces
- Acts that cause loss: use of false data, disclosure, interference with use, copying, misuse or failure to use
- Safeguard functionality used to protect from these acts: audit, avoidance, detection, prevention, recovery, mitigation, investigation
- Methods of safeguard functionality selection: diligence, comply with regulations and standards, meet needs
- Objectives to be achieved by the application security framework: avoid negligence, protect privacy, minimize impact on performance

The six essential security elements

In the proposed framework, six security elements are considered essential for the security of information. If one of these six elements is omitted, information security is deficient and protection of information will be at risk.

Prepared By: Prof. Harsh Joshi

Availability

Looking at the definition, availability (considering computer systems), is referring to the ability to access information or resources in a specified location and in the correct format. When a system is regularly not functioning, information and data availability is compromised and it will affect the users. Besides functionality, another factor that effects availability is time. If a computer system cannot deliver information efficiently, then availability is compromised again. Data availability can be ensured by storage, which can be local or offsite.

Utility

Considering the definition, utility refers to something that is useful or designed for use. Normally, utility is not considered a pillar in information security, but consider the following scenario: you encrypt the only copy of valuable information and then accidentally delete the encryption key. The information in this scenario is available, but in a form that is not useful. To preserve utility of information, you should require mandatory backup copies of all critical information and should control the use of protective mechanisms such as cryptography. Test managers should require security walk-through tests during application development to limit unusable forms of information.

Integrity

In the context of computer systems, integrity refers to methods of ensuring that the data is real, accurate and guarded from unauthorized user modification. Data integrity is a major information security component because users must be able to trust information. Untrusted data compromises integrity. Stored data must remain unchanged within a computer system, as well as during transport. It is important to implement data integrity verification mechanisms such as checksums and data comparison.

Authenticity

Regarding computer systems, authenticity or authentication refers to a process that ensures and confirms the user's identity. The process begins when the user tries to access data or information. The user must prove access rights and identity. Commonly, usernames and passwords are used for this process. However, this type of authentication can be circumvented by hackers. A better form of authentication is biometrics, because it depends on the user's presence and biological features (retina or fingerprints). The PKI (Public Key Infrastructure) authentication method uses digital certificates to prove a user's identity. Other authentication tools can be key cards or USB tokens. The greatest authentication threat occurs with unsecured emails that seem legitimate.

Confidentiality

Defining confidentiality in terms of computer systems means allowing authorized users to access sensitive and protected information. Sensitive information and data should be disclosed to authorized users only. Confidentiality can be enforced by using a classification system. The user must obtain certain clearance level to access

specific data or information. Confidentiality can be ensured by using role-based security methods to ensure user or viewer authorization (data access levels may be assigned to a specific department) or access controls that ensure user actions remain within their roles (for example, define user to read but not write data).

Nonrepudiation
Nonrepudiation refers to a method of guaranteeing message transmission between parties using digital signature and/or encryption. Proof of authentic data and data origination can be obtained by using a data hash. While the method is not 100 percent effective (phishing and Man-in-the-Middle attacks can compromise data integrity), nonrepudiation can be achieved by using digital signatures to prove the delivery and receipt of messages.

Each of the six elements can be violated independently of the others. The elements are unique and independent and often require different security controls.

Maintaining availability of information does not necessarily maintain its utility: information may be available, but useless for its intended purpose. In order to identify threats, we can pair the six elements into three pairs, which can be used to identify threats and select proper controls:

Availability and utility → Usability and usefulness
Integrity and authenticity → Completeness and validity
Confidentiality and nonrepudiation → Secrecy and control

E-Commerce threats

E-Commerce refers to the activity of buying and selling things over the internet. Simply, it refers to the commercial transactions which are conducted online. E-commerce can be drawn on many technologies such as mobile commerce, Internet marketing, online transaction processing, electronic funds transfer, supply chain management, electronic data interchange (EDI), inventory management systems, and automated data collection systems.
E-commerce threat is occurring by using the internet for unfair means with the intention of stealing, fraud and security breach. There are various types of e-commerce threats. Some are accidental, some are purposeful, and some of them are due to human error. The most common security threats are an electronic payments system, e-cash, data misuse, credit/debit card frauds, etc.

Electronic payments system:
With the rapid development of the computer, mobile, and network technology, e-commerce has become a routine part of human life. In e-commerce, the customer

can order products at home and save time for doing other things. There is no need of visiting a store or a shop. The customer can select different stores on the Internet in a very short time and compare the products with different characteristics such as price, colour, and quality.

The electronic payment systems have a very important role in e-commerce. E-commerce organizations use electronic payment systems that refer to paperless monetary transactions. It revolutionized the business processing by reducing paperwork, transaction costs, and labour cost. E-commerce processing is user-friendly and less time consuming than manual processing. Electronic commerce helps a business organization expand its market reach expansion. There is a certain risk with the electronic payments system.

E-Commerce security best practices

E-commerce security safeguards online transactions and digital interactions between customers, businesses, and vendors. E-commerce security is becoming increasingly important as more consumers shop online, making it necessary for businesses to protect their customers' data while protecting their own e-commerce business from cybercriminals.

Prepared By: Prof. Harsh Joshi

With the number of cyberattacks increasing every year, organizations must be diligent in implementing security protocols to maintain the trust of their customers. Cybersecurity measures such as encryption, authentication, and authorization can help protect customer data and company assets from malicious actors. Authentication is one of the most important aspects of e-commerce security as it requires both buyer and seller to be legitimate and provides proof of identity. Encryption is also a key element as it protects the data transmitted over the network.

Common E-commerce Security Threats

With the growth of e-commerce comes a heightened level of risk regarding data security. Businesses must be aware of the common threats in the digital space and how to best protect their customer data.

Data Security

Data security is one of the most important aspects of e-commerce safety and security. Data security includes protecting customer data from hackers, malware, and denial of service (DoS) attacks.

1. **Hacking**

Hacking is a type of cyberattack that involves gaining unauthorized access to a computer system or network. Hackers can use this access to steal customer data, modify or delete files, or take control of the system. Businesses should take steps to protect their systems from hacks, including implementing strong passwords and two-factor authentication, using a secure connection, and regularly patching software.

2. **Malware**

Malware is software that is intended to harm or disable computer systems. Malware commonly includes viruses, ransomware, and spyware. Businesses should use anti-malware software and scan their systems on a regular basis to protect themselves from malware.

3. **Denial of Service (DoS) Attacks**

DoS attacks are a type of cyberattack that seeks to make a computer system or network unavailable for use by flooding it with traffic or requests. DoS attacks can cause significant disruptions to an e-commerce store, including slowing down or crashing the website, preventing customers from accessing the site, and preventing orders from processing.

Payment Security

Payment security is critical for any e-commerce business, as customers trust their sensitive financial information to your website. Payment security threats come in many forms, including phishing, skimming, and credit card fraud.

1. **Credit Card Fraud**

Credit card fraud is one of the most common forms of payment security threat. Credit card fraudsters use stolen credit card numbers to make unauthorized purchases. It's important to ensure your website is PCI-compliant to prevent credit card fraud. This will include using SSL encryption, tokenization, and other security measures.

2. **Phishing**

Phishing is a common tactic cybercriminals use to access sensitive information. Phishing involves sending out emails that appear from a legitimate source but are malicious. The emails often contain a malicious link or attachment that installs malware onto the user's computer.

3. **Skimming**

Skimming is another payment security threat when a malicious actor places a device on a payment terminal or ATM to capture credit card information. Skimmers are becoming increasingly sophisticated; some can even be used remotely via Bluetooth. To protect against skimming, it's important to ensure that any payment terminals and ATMs have up-to-date security protocols.

Network Security

Network security is one of the most essential parts of any e-commerce security strategy. It's important to ensure that your network is up-to-date with the latest security protocols and that you're using a secure network architecture. It's also

important to regularly monitor your network to ensure its security. This can be done through network scanning and intrusion detection systems.

1. **Unauthorized Access**

Unauthorized access is a major security threat in the e-commerce world. This can be done through malicious software, phishing attacks, and other malicious activities. It's important to ensure that all of your systems are secured and that you're using strong authentication methods to prevent unauthorized access.

2. **Insecure Network Infrastructure**

Insecure network infrastructure is another common security threat. It's important to make sure that your network is regularly updated and maintained in order to prevent any cyber-attacks. Additionally, you should make sure that your network is protected from the inside out, with firewalls, VPNs, and other security measures.

3. **Poor Password Management**

Poor password management is another common security threat in e-commerce. It's crucial to ensure that all of your passwords are strong and that they're regularly changed. Additionally, you should also ensure that all of your staff members have unique passwords and that they're not shared with anyone else.

Digital Payments

Introduction:

A digital payment, sometimes called an electronic payment, is the transfer of value from one payment account to another using a digital device or channel.

Components of digital payment and stake holders:

Digital payments have become a key part of the digital economy, offering faster, more flexible payment options than ever before. Some components of digital payments include:

- **Contactless payments**

Allow users to make payments without physical contact with currency or a payment point.

- **Mobile wallets**

Store payment information in apps so customers don't need to provide it repeatedly.

- **Peer-to-peer (P2P) payments**

Connect customers directly to a merchant's bank account through payment gateways like PayPal.

- **Banking cards**

A widely used digital payment system in India that offers security and convenience, and can also be used to make other types of digital payments.

Prepared By: Prof. Harsh Joshi

- **Unified Payments Interface (UPI)**

An interface developed by the National Payments Corporation of India (NPCI) to facilitate real-time inter-bank transactions.

- **Bharat Bill Payment System (BBPS)**

An integrated payment platform that simplifies digital payments and protects users' privacy.

Modes of Digital Payments:

1. Banking Cards:
Debit and credit cards are popular digital payment options in India. Visa debit cards are also a type of card that can be used for digital payments.

2. Unified Payment Interface (UPI):
Unified Payments Interface (UPI) is a system that powers multiple bank accounts into a single mobile application, merging several banking features, seamless fund routing & merchant payments into one hood. It also caters to the “Peer to Peer” (P2P) collect request which can be scheduled and paid as per requirement and convenience.

3. e-Wallets:
Also known as digital wallets, these virtual wallets can be linked to a debit card, credit card, or savings account for mobile payments. Popular mobile wallets in India include Paytm and PhonePe.

4. Unstructured Supplementary Service Data (USSD):

*99# is a USSD based digital payment and banking service. Customers can avail this service by dialing *99#, a “Common number across all Telecom Service Providers (TSPs)” on their mobile phone and transact through an interactive menu displayed on the mobile screen. *99# service is currently offered by almost all leading banks & all GSM service providers and can be accessed in 13 different languages including Hindi & English.
Key services offered under *99# service include:

- Interbank account to account fund transfer
- Balance enquiry
- Mini statement besides host of other services

5. Aadhar enabled payments:

Aadhaar Enabled Payment System (AePS) is a bank led model which allows online interoperable financial inclusion transaction at Point of sale (MicroATM) through the

Business correspondent of any bank using the Aadhaar authentication. AePS allows you to do six types of transactions, the inputs required for a customer to do a transaction Bank Name, Aadhaar Number, Fingerprint captured during enrolment. Banking Services Offered by AePS

- Cash Deposit
- Cash Withdrawal
- Balance Enquiry
- Mini Statement
- Aadhaar to Aadhaar Fund Transfer
- Authentication
- BHIM Aadhaar Pay

Digital payments frauds and preventive measures:

Digital payment fraud is a persistent concern, but armed with awareness and preventive measures, we can navigate this digital landscape more securely. Let's delve into some common types of fraud and practical steps to safeguard against them:

1. **Phishing Attacks**:
    - **What is it?** Phishing involves tricking individuals into revealing sensitive information (like passwords or credit card details) by posing as a trustworthy entity (often via email).
    - **Preventive Measures**:
        - Educate yourself and your team about phishing tactics.
        - Verify the sender's identity before clicking on any links or sharing information.
        - Practice safe browsing habits—don't click on suspicious links or download attachments from unknown sources.
2. **Skimming**:
    - **What is it?** Skimming occurs when criminals tamper with point-of-sale (POS) terminals or ATMs to steal card information.
    - **Preventive Measures**:
        - Regularly inspect POS terminals and ATMs for signs of tampering.
        - Cover your PIN while entering it at ATMs or POS terminals.
3. **Identity Theft**:
    - **What is it?** Identity theft involves stealing personal information (such as Social Security numbers or Aadhaar details) to commit fraud.
    - **Preventive Measures**:
        - Use secure payment methods.
        - Keep your antivirus software updated.
        - Encrypt transactions and sensitive emails.

Prepared By: Prof. Harsh Joshi

        - Change passwords regularly.
4. **Chargeback Fraud**:
    - **What is it?** Fraudsters make a purchase, receive the goods or services, and then dispute the charge with their bank, resulting in a chargeback.
    - **Preventive Measures**:
        - Maintain clear records of transactions.
        - Provide excellent customer service to reduce disputes.
5. **Business Email Compromise (BEC)**:
    - **What is it?** Cybercriminals impersonate company executives or vendors to deceive employees into transferring funds.
    - **Preventive Measures**:
        - Implement multi-factor authentication (MFA) for email accounts.
        - Verify payment requests through a separate communication channel.
6. **Card-Not-Present (CNP) Fraud**:
    - **What is it?** CNP fraud occurs in online transactions where the physical card isn't present.
    - **Preventive Measures**:
        - Use secure payment gateways.
        - Monitor transactions for any anomalies.

RBI guidelines on digital payments and customer protection in unauthorized banking transactions

- **Notify the bank**

Customers should notify their bank of unauthorized electronic banking transactions as soon as possible. The bank must resolve complaints within 90 days of receiving them. Customers should get an acknowledgment from the bank when they notify it.

- **Report within 30 days**

Customers who claim an unauthorized debit transaction must report it to the bank within 30 days to be eligible for compensation.

- **Bear the loss**

Customers are liable for any losses due to unauthorized transactions if they were negligent, such as by sharing their password, PIN, or OTP. The customer will bear the entire loss until they report the transaction to the bank.

- **Limited liability**

If a customer reports a fraudulent transaction within 3 days, they may have zero liability. If they report it between 3 and 7 days after the transaction, they may have limited liability of up to INR 25,000, whichever is lower. If they don't report the transaction within 7 days, the bank may not refund any amount.

Prepared By: Prof. Harsh Joshi

- **Bank's discretion**

The bank may decide to waive customer liability even if the customer was negligent. The bank is also responsible for proving customer liability.

The RBI also has guidelines to help customers make safe digital transactions, such as:

- Not clicking on suspicious links in emails or texts
- Not entering personal or financial information on Google forms, advertisements, or suspicious links
- Verifying the authenticity of anyone trying to access personal or financial information
- Using a token issued by the bank instead of a debit or credit card number for online transactions.

Relevant provisions of Payment Settlement Act, 2007

The Payment and Settlement Systems Act, 2007 (PSS Act) gives the Reserve Bank of India (RBI) the power to regulate payment and settlement systems in India. The act covers a range of topics, including:

- **Authorizations**

The RBI can issue authorizations to people who want to start or continue operating a payment system. The RBI must process applications as soon as possible and aim to make a decision within six months. If the RBI decides to refuse an application, it must give the applicant a written notice with reasons.

- **Standards**

The RBI can set standards and requirements for payment system operators to follow.

- **Penalties**

The RBI can impose fines and penalties on operators who don't comply with the act or the RBI's guidelines. For example, under section 26, someone who violates section 4 or doesn't follow the terms of their authorization could face up to 10 years in prison or a fine. Other offenses that could lead to criminal prosecution include:

    - Operating a payment system without authorization
    - Failing to provide documents, returns information, or statements
    - Giving false information or statements
    - Disclosing prohibited information
    - Not following the RBI's directions

- **Other powers**

The RBI also has the power to:

    - Call for documents, returns, or other information
    - Inspect and enter certain areas
    - Ensure that information is kept confidential

Prepared By: Prof. Harsh Joshi

- Carry out audits and inspections
- Issue general directions

Unit-5

Digital Devices Security, Tools and Technologies for Cyber Security

End Point device and Mobile Phone security

Endpoint security protects devices like mobile phones, laptops, and desktops from cybersecurity threats. These threats can include phishing, ransomware, and device vulnerabilities. Endpoint security can help organizations reduce the attack surface, detect and prevent threats in real time, and automate responses to security events.

Here are some ways endpoint security can protect mobile devices:

- Application control: Allows administrators to monitor installed applications, block access to certain apps, or prompt users to uninstall an app.
- Encryption: Prevents data loss.
- Detection and response: Can identify and block more advanced security threats.
- Endpoint monitoring: Can help organizations gain greater visibility of devices and systems across their networks.
- Other types of endpoint protection solutions include: Endpoint Protection Platform (EPP), Mobile Threat Defense (MTD), and Advanced Threat Protection (ATP).

Password Policy:

A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly.

A strong password policy in cybersecurity can help protect your accounts from unauthorized access. Here are some recommendations for strong passwords:

- **Length:** At least 16 characters long, but longer is better.
- **Complexity:** A mix of uppercase and lowercase letters, numbers, and symbols. You can also use a passphrase of 5–7 random words.
- **Uniqueness:** Use a different password for each account, and don't reuse passwords for other services like banking or email.
- **Avoidability:** Don't use personal information like names, birthdates, or phone numbers that are easy to guess.
- **Changes:** Change your password regularly, or if you suspect it's been compromised.

Prepared By: Prof. Harsh Joshi

Security Patch Management:
Patch management is the process of applying updates to software, drivers, and firmware to protect against vulnerabilities. Effective patch management also helps ensure the best operating performance of systems, boosting productivity.

Types of Patches

- Security Patches. Security patches are critical updates designed to address vulnerabilities that could be exploited by malicious actors. ...
- Service Packs. ...
- Hotfixes. ...
- Point Releases. ...
- Program Temporary Fix (PTF) ...
- OS Patching. ...
- Security Tools Updates.

Data backup:
Data backup is the process of making copies of your data and storing them in a secure location to protect against data loss. Data loss can happen in many ways, including:

- Hardware or software failure
- Data corruption
- Malicious attacks like viruses or malware
- Accidental deletion
- Power failure
- Human errors

Backups can help companies restore data quickly and accurately when unexpected circumstances arise. They can also help ensure the confidentiality, integrity, and availability (CIA) of critical data.
Here are some options for storing data backups:

- **Removable Devices:** These include USB flash drives, CDs, DVDs, and Blu-Ray disks. They're simple and practical, but they don't offer much storage space.
- **External Hard Drives:** These are easy to use and contain plenty of storage space, but they can break over time and can be lost or stolen.
- **Cloud Storage Containers:** These are another option for storing backups.

You can also encrypt your data to make it more secure. For example, most office software allows you to encrypt individual files with a password. Windows Pro and Enterprise editions also include a whole drive encryption feature called BitLocker.

Prepared By: Prof. Harsh Joshi

Downloading and management of third-party software:

Third Party Risk Management (TPRM) is the process of managing risks with third parties that are integrated into your business IT infrastructure and an essential cybersecurity practice for businesses today.

What is Third Party Risk Management (TPRM)?

Third party risk management (TPRM) is the process an organization implements to manage risks that are a result of business relationships with third parties that are integrated into their IT environment and infrastructure. These risks can be operational, cybersecurity, regulatory, financial and reputational. According to a survey from Cyber Risk Alliance, the average organization uses 88 IT third parties (including software and service providers, partners, external contractors, agencies, suppliers and vendors), and larger organizations can rely on nearly twice as many (175) third parties.

The Most Common Third-Party Cyber Risks

Risk management technology can help your organization both consolidate vendor information and conduct an ongoing third party risk assessment of all your vendors to help identify risk factors and evaluate each vendor's inherent risk. Often, the technology determines the risk according to risk scores. After identifying the risk level that each vendor poses, a risk reduction strategy can be put into place according to your organization's risk tolerance. This is the heart of third party risk management.

Third party risks include:

- **Cybersecurity risk**. A data breach, phishing, DDoS, social engineering or ransomware attack from a third party can cost your organization in time and resources, halt or disrupt operations and significantly impact its reputation.
- **Operational risk.** If a third party provides a critical component of your system and is disrupted due to a natural disaster, political conflict or cybersecurity attack, it also poses a critical risk to your business continuity.
- **Financial risk.** If a supply chain is poorly managed, it can result in financial risk to a third party as they are unable to properly evaluate which products they offer are in high demand and which are not.
- **Strategic risk.** Market changes, new acquisitions or mergers, and changing expectations of customers can make it difficult for all parties in the supply chain to align on business strategy.
- **Compliance risk.** Compliance requirements depend on the industry (e.g. HIPAA and PCI DSS), your company's location, and your customer's location (e.g. GDPA, CCPA, EBA).

Prepared By: Prof. Harsh Joshi

- **Geopolitical risk.** For example, political tensions can make it difficult to continue a business relationship with a supplier or vendor. Political instability can motivate companies to look for a vendor in another location.

Device Security Policy:

A device security policy is a set of guidelines and best practices that outline how to protect mobile devices, laptops, PCs, and Internet of Things (IoT) devices from cyberthreats and unauthorized access. It can also define how to protect the data stored on these devices.

Device security policies can include:

- Encryption: Encoding data to keep it hidden from unauthorized parties. This can help protect data in transit and at rest, and ensure sensitive data remains private.
- Authentication: Strong authentication for users and their devices.
- Network access: Restricted network access.

Other types of cyber security policies include:

- Access control policy (ACP)
- Acceptable use of data systems policy
- Account management policy
- E-commerce policy
- Hardware and electronic media disposal policy
- Security incident management policy
- Information technology purchasing policy
- Web policy
- Log management policy

Significance of host firewall and Anti-virus:

Firewalls and antiviruses are both crucial to cybersecurity, but they serve different purposes. Firewalls control network traffic, while antiviruses protect devices from specific threats.

- **Firewalls**

Act as gatekeepers, filtering data packets based on rules to allow or block traffic. They monitor network activity and protect against unauthorized access, malicious traffic, and intrusion. Host-based firewalls run on individual devices to detect and stop viruses and other malicious scripts.

- **Antiviruses**

Detect and remove malware, viruses, and other malicious software from devices. They scan removable devices, block pop-ups and spam from malicious

websites, and restrict website access to prevent unauthorized networks. Antiviruses also use heuristics to identify and eliminate malware.

Management of host firewall and Anti-virus:

1. Block all access by default. When configuring a firewall, it's important to start by blocking access to the network from all traffic. ...
2. Regularly audit firewall rules and policies. ...
3. Keep the firewall up-to-date. ...
4. Keep track of authorized users. ...
5. Document all firewall changes.

Wi-Fi security:

Wi-Fi security is the protection of devices and networks connected in a wireless environment. Without Wi-Fi security, a networking device such as a wireless access point or a router can be accessed by anyone using a computer or mobile device within range of the router's wireless signal.

Protect your Wi-Fi network:

Media Access Control (MAC) addresses:
Another basic approach to Wi-Fi security is to use MAC addresses, which restrict access to a Wi-Fi network. (A MAC address is a unique code or number used to identify individual devices on a network.) While this tactic provides a higher measure of security than an open network, it is still susceptible to attack by adversaries using "spoofed" or modified addresses.

Encryption:
A more common method of protecting Wi-Fi networks and devices is the use of security protocols that utilize encryption. Encryption in digital communications encodes data and then decodes it only for authorized recipients.
There are several types of encryption standards in use today, including Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). See the section "Types of wireless security protocols" on this page for more details about these and other standards related to Wi-Fi security.
Most newer network devices, such as access points and Wi-Fi routers, feature built-in wireless-security encryption protocols that provide Wi-Fi protection.

Virtual private networks (VPNs):
VPNs are another source of Wi-Fi network security. They allow users to create secure, identity-protected tunnels between unprotected Wi-Fi networks and the internet.
A VPN can encrypt a user's internet connection. It also can conceal a user's IP address by using a virtual IP address it assigns to the user's traffic as it passes through the VPN server.

Security software:
There are many types of consumer and enterprise software that also can provide Wi-Fi security. Some Wi-Fi protection software is bundled with related products, such as antivirus software. For more information about Wi-Fi security software, see the next question.

Types of wireless security protocols:

There are four main wireless-security protocols. These protocols were developed by the Wi-Fi Alliance, an organization that promotes wireless technologies and interoperability. The group introduced three of the protocols, described below, in the late 1990s. Since then, the protocols have been improved with stronger encryption. The fourth protocol was released in 2018.

WEP:
The first wireless security protocol was WEP (Wired Equivalent Privacy). It was the standard method of providing wireless network security from the late 1990s until 2004. WEP was hard to configure, and it used only basic (64-/128-bit) encryption. WEP is no longer considered secure and should be replaced by a newer protocol such as WPA2, described below.

WPA:
WPA (Wi-Fi Protected Access) was developed in 2003. It delivers stronger (128-/256-bit) encryption than WEP by using a security protocol known as Temporal Key Integrity Protocol (TKIP). Along with WPA2, WPA is the most common protocol in use today. But unlike WPA2, it is compatible with older software.

WPA2:
WPA2, a later version of WPA, was developed in 2004. It's easier to configure and provides even greater network security than WPA by using a security protocol known as the Advanced Encryption Standard (AES). Versions of the WPA2 protocol are available for individual users and enterprises.

Prepared By: Prof. Harsh Joshi

WPA3:
A new generation of WPA, known as WPA3, is designed to deliver simpler configuration and even stronger (192-/256-/384-bit) encryption and security than any of its predecessors. It is also meant to work across the latest Wi-Fi 6 networks.

Configuration of basic security policy and permissions:

1. Log in to DeviceManager
2. Select Settings > Permission Settings > Security Policies
3. In the Basic Service Settings area, click Permission Settings
4. Configure the user name, password, login, and account audit policies
5. Click Save to confirm the configuration
6. Click Close in the Execution Results dialog box

Prepared By: Prof. Harsh Joshi