1. Introduction to Cyber Security

1.1 Defining Cyberspace

Cyberspace is a virtual environment created by the global network of interconnected computers and devices. It includes the internet, telecommunication systems, and the infrastructure that supports them.

- Key Feature: It is not a physical space but relies on real-world hardware like servers, cables, and satellites.
- Example: When you send an email, it travels through cyberspace via data packets across servers and undersea cables.

1.2 Overview of Computer and Web Technology

The backbone of cyberspace includes:

1. Computer Systems: Desktops, servers, and mobile devices.
2. Web Technology: Tools that enable websites and applications (e.g., HTML, HTTP, and DNS).

Key Highlight: DNS (Domain Name System) is like the phonebook of the internet, translating domain names into IP addresses.

1.3 Architecture of Cyberspace

- Physical Layer: Undersea cables, satellites, routers, and data centers.
- Logical Layer: Protocols like TCP/IP that handle communication between devices.
- Application Layer: Web browsers and applications that users interact with.

1.4 Communication and Web Technology

- Data Flow:
  Data on the internet is broken into smaller packets, which travel independently and reassemble at the destination.
- Example: Sending a file through email involves TCP breaking it into packets.

Key Highlight: TCP/IP ensures reliability, while UDP prioritizes speed (e.g., in video streaming).

1.5 Regulation of Cyberspace

Cyberspace is governed by international treaties and national regulations.

- Examples:
- GDPR (General Data Protection Regulation) protects user data in Europe.
- India's IT Act 2000 governs cybersecurity laws and penalties.

Challenge: Lack of a global consensus leads to jurisdictional conflicts, such as cross-border cybercrimes.

1.6 Concept of Cyber Security

Cybersecurity is the practice of protecting systems, networks, and data from attacks.

- Pillars of Cybersecurity:

1. Confidentiality: Ensuring only authorized users access data.
2. Integrity: Maintaining data accuracy.
3. Availability: Ensuring systems are accessible when needed.

1.7 Challenges of Cyber Security

1. Increasing Sophistication of Attacks: Zero-day vulnerabilities.
2. Human Error: A major cause of breaches (e.g., weak passwords).
3. Evolving Technology: IoT devices add more vulnerabilities.

2. Cyber Crime and Cyber Law

2.1 Classification of Cyber Crimes

Cybercrimes are categorized based on their targets:

1. Crimes Targeting Computers and Devices

- Example: DDoS (Distributed Denial-of-Service) attacks overwhelm servers.
- Impact: Disrupts online services like banking and e-commerce.

2. Crimes Against Individuals

- Cyberbullying: Harassment on social platforms.
- Identity Theft: Using stolen personal information to commit fraud.

Highlight: In India, cyberstalking is addressed under Section 354D of the IPC.

3. Financial Frauds

- Phishing: Deceptive emails tricking users into sharing sensitive data.
- Case Study: The 2016 Bangladesh Bank heist, where hackers used fraudulent SWIFT messages to steal $81 million.

4. Social Engineering Attacks

- Methods:

1. Pretexting: Creating a fabricated scenario to extract data.
2. Baiting: Using a lure, such as a free USB drive, containing malware.

2.2 Modus Operandi of Cybercriminals

- Phases of an Attack:

1. Reconnaissance: Gathering information about the target.
2. Exploitation: Deploying the attack (e.g., malware).
3. Exfiltration: Stealing or destroying data.

Key Insight: Cybercriminals often operate from countries with weak cyber laws to avoid prosecution.

2.3 Reporting and Mitigation

1. Reporting Channels in India:
- Cybercrime.gov.in: A portal to report cybercrimes.
- CERT-In: Tracks and resolves security incidents.
2. Mitigation Strategies:
- Regularly updating software to patch vulnerabilities.
- Implementing multi-factor authentication (MFA).

2.4 Legal Framework: Cyber Law

- IT Act 2000: India's primary legislation for regulating cyberspace.
- Section 43: Protects against unauthorized data access.
- Section 66: Penalizes hacking.
- Section 67: Regulates obscene content.

Highlight: The 2008 amendment strengthened provisions against cyber terrorism.

2.5 Case Studies

1. WannaCry Ransomware Attack (2017)
- Nature: Exploited a Windows vulnerability (EternalBlue).
- Impact: Affected 150 countries, causing $4 billion in damages.
2. Aadhaar Data Leak (2018)
- Issue: Mismanagement of sensitive personal data in India's Aadhaar database.

Key Insight: Highlight the importance of secure infrastructure for critical systems.

Additional Key Points

Emerging Threats

1. AI-Generated Phishing: Hyper-realistic scams using AI tools.
2. Quantum Computing Threats: Potential to break modern cryptographic systems.

Best Practices for Cyber Security

- Use strong, unique passwords and change them regularly.
- Avoid clicking on suspicious links or downloading unknown attachments.
- Educate users on social engineering techniques.

3. Social Media Overview and Security

3.1 Introduction to Social Networks

Social networks are platforms where users interact, share content, and build virtual communities.

- Examples: Facebook, LinkedIn, Instagram, and Twitter.
- Key Feature: Real-time communication and global reach.

3.2 Types of Social Media

1. Social Networks: Platforms for interaction (e.g., Facebook, LinkedIn).
2. Media Sharing: For photos and videos (e.g., YouTube, Instagram).
3. Microblogging: Short content updates (e.g., Twitter).
4. Discussion Forums: Community Q&A (e.g., Reddit, Quora).

3.3 Social Media Security Challenges

1. Privacy Risks: Excessive sharing can lead to identity theft.
2. Phishing and Scams: Fraudulent messages lure users into sharing sensitive data.
3. Inappropriate Content: Harmful posts affecting mental health and societal norms.

Case Study: The Cambridge Analytica scandal highlighted the misuse of user data for political campaigns.

3.4 Best Practices for Social Media Use

- Adjust privacy settings to control who sees your posts.
- Avoid sharing sensitive information like location or financial data.
- Use strong, unique passwords and enable two-factor authentication.

3.5 Reporting Inappropriate Content

Most platforms allow users to flag and report harmful content.

- Example: Facebook allows reporting posts that violate community guidelines.

Laws in India: Section 67 of the IT Act penalizes publishing obscene or defamatory content online.

3.6 Opportunities and Challenges in Social Media

1. Opportunities:
- Brand marketing through viral content and hashtags.
- Crowd-sourcing opinions and user engagement.
2. Challenges:
- Cyberbullying, trolling, and spreading fake news.

4. E-Commerce and Digital Payments

4.1 Definition of E-Commerce

E-Commerce refers to online buying and selling of goods and services.

- Example Platforms: Amazon, Flipkart, and Shopify.
- Main Components:

1. Website/Storefront
2. Payment Gateway
3. Logistics and Delivery

4.2 E-Commerce Security Elements

- Confidentiality: Encrypt customer data (e.g., SSL/TLS).
- Authentication: Verifying user identity through OTPs or biometrics.
- Non-repudiation: Ensuring neither party can deny transactions.

4.3 E-Commerce Threats

1. Data Breaches: Theft of sensitive customer data.
- Example: The 2014 eBay breach exposed personal data of 145 million users.
2. Payment Fraud: Fake websites tricking users into payments.

4.4 Digital Payments

Digital payment systems enable cashless transactions.

- Modes of Digital Payments:

1. Banking Cards: Credit and debit cards.

2. Unified Payment Interface (UPI): Real-time bank transfer (e.g., Google Pay, PhonePe).
3. e-Wallets: Apps like Paytm store funds for easy payments.
4. USSD: Mobile payments without internet.

Common Frauds:

1. Phishing: Fake emails or links requesting bank details.
2. SIM Swap Fraud: Gaining control of user accounts through SIM card cloning.

Preventive Measures:

- Always verify URLs and apps before entering credentials.
- Report unauthorized transactions immediately to your bank.

4.5 RBI Guidelines

- Customer Protection: Banks must resolve unauthorized transaction complaints within 90 days.
- Zero Liability: If reported promptly, customers may not be held liable for losses.

5. Digital Devices Security, Tools, and Technologies for Cyber Security

5.1 End-Point and Mobile Phone Security

1. Device Security Practices:
- Regularly update your OS to patch vulnerabilities.
- Avoid using public Wi-Fi for sensitive transactions.
2. Password Policies:
- Use complex passwords with a mix of uppercase, lowercase, numbers, and special characters.
- Change passwords every 60–90 days.

Example: A weak password like "password123" can be cracked within seconds.

5.2 Data Backup and Recovery

1. Importance of Backups:
- Prevents data loss during ransomware attacks.
- Cloud services like Google Drive provide automatic backups.
2. Best Practices:
- Follow the 3-2-1 Rule: 3 copies of data, 2 local, 1 offsite.

5.3 Device Security Policies

Organizations enforce policies to safeguard devices:

- Prohibit downloading unverified software.
- Mandate the use of VPNs for remote access.

5.4 Cyber Security Tools

1. Antivirus Software: Scans and removes malicious files.
- Examples: Norton, Kaspersky.
2. Host Firewalls: Prevent unauthorized access.
- Configure firewall settings to block untrusted applications.

5.5 Wi-Fi Security

- Use WPA3 encryption for strong protection.
- Regularly change the router password.

5.6 Configuration of Basic Security Policies

1. Limit user permissions based on roles.
2. Disable auto-download for attachments in emails to avoid malware.

Real-World Example:
In 2019, a misconfigured firewall allowed hackers to breach Capital One's database, exposing sensitive customer data.

Conclusion

This section highlights the importance of proactive security measures, laws, and tools to navigate the evolving landscape of social media, e-commerce, and device protection effectively.