UNIT 1: Introduction to Cyber Security

1. Define Cyber Security.

Cyber Security refers to the practice of protecting computers, networks, programs, and data from unauthorized access, attacks, damage, or theft. It involves technologies, processes, and controls designed to safeguard digital systems.

---

2. Explain the Importance of Cyber Security.

Cyber Security is important because it protects sensitive information, ensures privacy, prevents financial losses, safeguards business reputation, and maintains national security. With increasing digital transactions, security is essential.

---

3. What is the Scope of Cyber Security?

The scope includes network security, information security, application security, cloud security, endpoint security, cyber law, ethical hacking, digital forensics, and cyber crime investigation.

---

4. Explain Cyber Security in Commerce and Business.

In commerce and business, cyber security protects online transactions, customer data, financial records, intellectual property, and business communications. It ensures safe digital payments and prevents fraud.

---

5. What is a Cyber Threat Landscape?

Cyber Threat Landscape refers to the overall environment of cyber threats, including hackers, malware, phishing attacks, ransomware, insider threats, and emerging vulnerabilities affecting organizations and individuals.

---

6. What are the Types of Cyber Threats?

Types of cyber threats include Malware, Phishing, Ransomware, Denial of Service (DoS), Man-in-the-Middle attacks, SQL Injection, Zero-day attacks, and Insider threats.

---

7. Explain the Characteristics of Cyber Security.

The main characteristics are Confidentiality (protecting data from unauthorized access), Integrity (ensuring data accuracy), Availability (ensuring access to data when needed), Authentication, and

Non-repudiation.

---

8. What are the Advantages of Cyber Security?

Advantages include protection of sensitive data, prevention of cyber attacks, improved customer trust, business continuity, compliance with laws, and reduced financial losses.

---

9. What are the Disadvantages of Cyber Security?

Disadvantages include high implementation cost, need for regular updates, complexity in management, possible system slowdowns, and requirement of skilled professionals.

---

10. Give an Overview of Digital Commerce and Its Vulnerabilities.

Digital commerce involves buying and selling goods and services through electronic platforms such as websites and mobile applications. Vulnerabilities include data breaches, payment fraud, identity theft, hacking, weak passwords, and unsecured networks.

UNIT 2: Introduction to Cyber Security in Financial System and Banking

1. What is Cyber Security in Financial Systems?

Cyber Security in financial systems refers to the protection of financial institutions, digital payment platforms, financial data, and transaction systems from cyber attacks, unauthorized access, and fraud.

---

2. Give an Overview of Cyber Security in Financial Systems.

Financial systems include banks, stock markets, insurance companies, and digital payment services. Cyber security in these systems ensures safe transactions, data confidentiality, system integrity, and uninterrupted financial services.

---

3. Explain the Importance of Cyber Security in Financial Systems.

It prevents financial fraud, protects customer data, maintains trust in banking institutions, ensures regulatory compliance, and safeguards national economic stability.

---

4. What are the Characteristics of Cyber Security in Financial Systems?

Key characteristics include Confidentiality, Integrity, Availability, Strong Authentication, Encryption, Continuous Monitoring, and Regulatory Compliance.

---

5. What is the Meaning of Cyber Security in Banking?

Cyber security in banking means protecting banking networks, online banking services, ATMs, mobile banking applications, and customer accounts from cyber threats and attacks.

---

6. Explain the Importance of Cyber Security in Banking.

It protects customer deposits, prevents identity theft, avoids financial loss, secures digital banking platforms, and maintains public confidence in the banking system.

---

7. What are the Common Cyber Attacks in Banks?

Common cyber attacks include Phishing, Malware attacks, Ransomware, ATM skimming, Insider threats, Distributed Denial of Service (DDoS), and Man-in-the-Middle attacks.

8. What are the Vulnerabilities in Banking Systems?

Vulnerabilities include weak passwords, outdated software, unsecured networks, poor access controls, lack of employee awareness, and third-party service risks.

---

9. Explain Cyber Security Measures in Banking.

Cyber security measures include firewalls, intrusion detection systems, encryption, multi-factor authentication, regular security audits, employee training, strong password policies, backup systems, and compliance with regulatory guidelines.

---

10. Why is Continuous Monitoring Important in Banking Cyber Security?

Continuous monitoring helps detect suspicious activities early, prevents major breaches, ensures real-time threat response, and maintains secure banking operations.

UNIT 3: Fundamentals of Networking and Security

1. What are the Basics of Networking?

Networking refers to the connection of two or more computers to share data and resources. It allows communication between devices using hardware (routers, switches) and software protocols.

---

2. Define LAN, WAN, and Internet.

LAN (Local Area Network) connects computers within a small area like a home or office. WAN (Wide Area Network) connects networks across large geographical areas. The Internet is a global network connecting millions of networks worldwide.

---

3. What is IP Addressing?

An IP (Internet Protocol) address is a unique numerical label assigned to each device connected to a network. It helps in identifying and locating devices for communication.

---

4. Explain Types of Networks: Wired and Wireless.

Wired networks use physical cables like Ethernet for data transmission. Wireless networks use radio waves such as Wi-Fi or Bluetooth to connect devices without cables.

---

5. What is a Firewall?

A firewall is a security system that monitors and controls incoming and outgoing network traffic based on predefined security rules to prevent unauthorized access.

---

6. What is a VPN?

VPN (Virtual Private Network) creates a secure and encrypted connection over the internet, protecting data from hackers and ensuring privacy.

---

7. What is Antivirus Software?

Antivirus software detects, prevents, and removes malicious software such as viruses, worms, and trojans from computer systems.

---

8. Explain Password Security and Best Practices.

Strong passwords should be long, unique, and include a mix of letters, numbers, and symbols. Avoid sharing passwords, enable multi-factor authentication, and change passwords regularly.

---

9. How Can Cyber Threats Be Prevented?

Cyber threats can be prevented through regular software updates, firewalls, antivirus software, employee training, strong authentication, secure backups, and safe browsing practices.

---

10. How to Protect Payment Gateways and Transactions?

Payment gateways can be protected using SSL encryption, tokenization, secure authentication, regular security audits, compliance with security standards, and monitoring for fraudulent activities.

UNIT 4: Risk Management and Compliance

1. Cyber Risk Assessment and Risk Mitigation in Financial Systems

Cyber risk assessment in financial systems refers to the systematic process of identifying, analyzing, and evaluating cyber threats that may affect financial institutions such as banks, insurance companies, NBFCs, and fintech organizations. Financial systems are highly attractive targets for cybercriminals due to the sensitive customer data, digital payment systems, and large-scale monetary transactions involved. The process of cyber risk assessment includes asset identification, threat identification, vulnerability assessment, risk analysis, and risk evaluation. Asset identification involves recognizing critical systems like core banking solutions, payment gateways, databases, and customer information systems. Threat identification includes malware attacks, phishing, ransomware, insider threats, Distributed Denial of Service (DDoS), and data breaches. Risk mitigation strategies include implementation of firewalls, intrusion detection systems (IDS), multi-factor authentication (MFA), encryption techniques, network segmentation, and regular security patch updates. Financial institutions must also adopt strong access control policies, conduct regular employee training programs, and perform penetration testing to ensure system resilience. Effective cyber risk management ensures confidentiality, integrity, and availability (CIA triad) of financial data.

2. Compliance Standards: ISO 27001, NIST, RBI Cyber Security Framework

Compliance standards provide structured guidelines for managing cybersecurity risks in financial institutions. ISO 27001 is an international standard for Information Security Management Systems (ISMS). It provides a systematic approach to managing sensitive company information through risk assessment, risk treatment, and continuous improvement. The NIST Cybersecurity Framework provides guidelines based on five core functions: Identify, Protect, Detect, Respond, and Recover. It helps financial institutions improve cybersecurity posture and manage risk efficiently. The RBI Cyber Security Framework mandates Indian banks and financial institutions to establish robust cybersecurity policies, incident response mechanisms, security operations centers (SOC), cyber crisis management plans, and board-level oversight. It emphasizes continuous monitoring, cyber audits, and reporting of security incidents to regulatory authorities. Compliance with these standards ensures legal adherence, strengthens customer trust, and enhances organizational security maturity.

3. Business Continuity Planning (BCP) for Financial Institutions

Business Continuity Planning (BCP) refers to the preparation of financial institutions to continue critical operations during and after a cyberattack, natural disaster, or system failure. BCP involves Business Impact Analysis (BIA), identifying critical processes, setting Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), and establishing disaster recovery sites. Financial institutions must maintain backup data centers, cloud-based redundancy systems, data backup policies, and emergency communication protocols. Regular mock drills and testing of disaster recovery plans are essential to ensure effectiveness. A strong BCP minimizes financial losses, protects customer interests, and ensures regulatory compliance.

4. Cybersecurity Audits and Reporting

Cybersecurity audits are systematic evaluations of an organization's information systems, security policies, and controls to ensure compliance with regulatory standards and internal policies. Audits may be internal or external. They assess risk management practices, incident response capabilities, access control systems, network security architecture, and data protection measures. Financial institutions are required to submit regular cybersecurity reports to regulatory bodies. These reports include incident summaries, vulnerability assessments, compliance status, and risk mitigation measures. Continuous monitoring, third-party risk assessment, and independent security audits enhance transparency and accountability. Proper documentation and reporting help maintain stakeholder confidence and regulatory trust. In conclusion, risk management and compliance form the backbone of cybersecurity governance in financial systems. Proper assessment, adherence to standards, continuity planning, and regular audits ensure resilience against evolving cyber threats.

UNIT 5: Digital Payment Systems Theft

1. Digital Payment Systems: UPI, NEFT, RTGS, SWIFT

Digital payment systems enable electronic transfer of funds securely and efficiently. UPI (Unified Payments Interface) is an instant real-time payment system that allows fund transfers between bank accounts through mobile applications. It operates 24/7 and supports peer-to-peer as well as merchant transactions. NEFT (National Electronic Funds Transfer) is a nationwide payment system that facilitates one-to-one funds transfer. It operates in half-hourly batches and is commonly used for retail banking transactions. RTGS (Real Time Gross Settlement) is used for high-value transactions. Transfers are processed individually and in real time, ensuring immediate settlement. SWIFT (Society for Worldwide Interbank Financial Telecommunication) is a global messaging network used by financial institutions to securely transmit information and instructions for international money transfers.

2. Vulnerabilities in Payment Systems and Fraud Prevention

Despite their efficiency, digital payment systems are vulnerable to cyber threats. Common vulnerabilities include phishing attacks, malware infections, social engineering, SIM swap fraud, man-in-the-middle attacks, data breaches, and unauthorized access to banking credentials. Fraud prevention strategies include encryption of transaction data, secure coding practices, transaction monitoring systems, anomaly detection using AI, strong customer authentication, regular system updates, and security awareness programs. Banks also implement transaction limits, OTP verification, device binding, and real-time fraud detection systems to reduce financial losses.

3. Two-Factor Authentication (2FA) and Biometric Security

Two-Factor Authentication (2FA) enhances security by requiring users to provide two different forms of identification before accessing accounts or authorizing transactions. The three main authentication factors include: 1. Something you know (password, PIN) 2. Something you have (OTP sent to mobile, hardware token) 3. Something you are (biometric verification) Biometric security includes fingerprint recognition, facial recognition, iris scanning, and voice recognition. These technologies reduce dependency on passwords and strengthen digital payment security. 2FA and biometric systems significantly reduce unauthorized access and protect users from digital payment theft.

4. Compliance Standards: PCI-DSS for Payment Card Security

PCI-DSS (Payment Card Industry Data Security Standard) is a global security standard designed to protect cardholder data. It applies to all organizations that store, process, or transmit credit and debit card information. PCI-DSS requirements include: - Building and maintaining secure networks - Protecting cardholder data through encryption - Implementing strong access control measures - Regular monitoring and testing of networks - Maintaining an information security policy Compliance with PCI-DSS reduces the risk of card fraud, data theft, and financial loss. Financial institutions and merchants must undergo regular security audits to maintain compliance. In conclusion, digital payment systems have transformed financial transactions, but they also present cybersecurity challenges. Strong authentication methods, fraud prevention mechanisms, and compliance with global security standards are essential to prevent digital payment theft and ensure financial safety.