DegreeLive

B.Com Honours | Semester I | Calicut University

Foundations of Modern Banking

Course Code: COM1MN106 • Module 4 Notes

1. Cybersecurity in Banking: Threats and Vulnerabilities

As banking operations migrate to the cloud and mobile applications, the banking sector has become the primary target of global cybercriminals. A single data breach or system hack can result in massive financial losses, disrupt the national payment system, and destroy public trust in the financial system. This final module covers the landscape of cybersecurity in banking, common cyber threats, emerging security technologies, RBI regulatory guidelines, and the role of data analytics in risk management.

Common Cyber Threats Facing Banks

Cybercriminals target both bank servers and individual bank customers to compromise accounts:

Social Engineering & Phishing

- **Phishing:** Sending deceptive emails mimicking bank communications to steal login credentials and PINs.
- **Vishing & Smishing:** Executing scams via phone calls (voice phishing) or SMS to trick users into sharing OTPs.

System Attacks & Malware

- **Ransomware:** Malware that encrypts bank databases, holding data hostage for financial ransom.
- **Man-in-the-Middle (MITM):** Intercepting transaction data between the customer's browser and the bank's server (common on public Wi-Fi).
- **DoS/DDoS:** Overloading bank websites with traffic to crash online and mobile banking applications.

2. Cyber Security Technologies and Regulations

To defend against threats, banks implement multi-layered technological barriers and adhere to strict regulatory compliance standards:

Emerging Security Technologies

- **Multi-Factor Authentication (MFA):** Requiring multiple independent credentials for account access (e.g., password + biometric scan + mobile OTP).
- **Biometric Authentication:** Using fingerprints, facial recognition, or voice recognition for secure user verification.
- **End-to-End Encryption (E2EE):** Encrypting all transaction data in transit to prevent interception during transmission.
- **Blockchain Ledgers:** Using decentralized, immutable ledger technology to secure interbank settlements and prevent database tampering.

RBI Cybersecurity Guidelines

The Reserve Bank of India mandates strict cybersecurity compliance for all banks operating in India:

- **Cybersecurity Policy:** Banks must have a dedicated Board-approved cybersecurity policy outlining risk limits and incident response protocols.
- **SOC (Security Operations Centre):** Maintaining a 24/7 monitoring center to detect and respond to security threats in real-time.
- **Regular Audits:** Mandating periodic vulnerability assessment and penetration testing (VAPT) audits by CERT-In empaneled security firms.
- **Disaster Recovery (DR):** Establishing separate, synchronized disaster recovery data centers to ensure business continuity during primary server failure.

3. Data Analytics in Modern Banking

Modern banking leverages massive datasets to improve risk management and customize customer offerings:

Risk Management & Credit Assessment

Analyzing transaction patterns, historical repayment behaviors, utility bill records, and social indices to build accurate credit-risk models, predicting non-performing assets (NPAs).

Customer Retention & Marketing

Analyzing customer activity data to predict account churn, identify product requirements (e.g., car loans), and design highly targeted, cost-effective marketing campaigns.