Cyber Law and Ethics 2k25 - Exam Answers (MAKAUT)

Group B (Short Answer)

1. SQL Injection & Prevention

SQL injection is a code injection technique where attackers insert malicious SQL statements into input fields to access or manipulate the database. Prevention methods include using prepared statements, input validation, and stored procedures.

2. Phishing/Vishing Techniques

Phishing is a fraudulent attempt to obtain sensitive data via email or fake websites, while vishing uses voice calls. Spear phishing targets individuals, and whaling targets executives. Prevention includes awareness training, email filters, and two-factor authentication.

3. Virus vs. Worm

A virus attaches to files and spreads when the file is executed. A worm is self-replicating and spreads through networks without user action. Antivirus software and regular updates help prevent them.

4. Software Piracy & Prevention

Software piracy is the unauthorized copying or distribution of software. It raises ethical concerns like loss of developer revenue. Prevention methods include license keys, digital rights management (DRM), and legal enforcement.

5. Identity Theft (ID Theft) Techniques

Identity theft involves stealing personal information to commit fraud. Techniques include phishing, dumpster diving, and skimming. Prevention includes monitoring financial accounts, strong passwords, and secure networks.

6. Cyberlaw & IT Act 2000

The IT Act 2000 establishes legal recognition for electronic transactions and cybercrimes in India. Amendments in 2008 added provisions for data protection, privacy, and penalties for cyber offenses.

7. Ethical Hacking (White-hat vs. Black-hat)

White-hat hackers test systems legally to find vulnerabilities. Black-hat hackers exploit systems for illegal gain. Ethical hacking helps improve security by identifying and fixing weaknesses.

8. Bluetooth/Mobile Device Vulnerabilities

Bluetooth and mobile vulnerabilities include Bluejacking, Bluesnarfing, and mobile malware. Prevention involves turning off Bluetooth when not in use, updating software, and using security apps.

Group C (Long Answer)

1. DDoS/DoS Attacks & Tools

DoS attacks overload a system with traffic from a single source; DDoS uses multiple sources (botnets). Tools like LOIC and HOIC are common. Prevention includes firewalls, intrusion detection systems, and rate limiting.

2. IT Act 2000 & Amendments

The IT Act 2000 sets a framework for electronic governance, digital signatures, and cybercrime penalties. The 2008 amendment expanded provisions to cover identity theft, data breaches, and introduced intermediary liabilities.

3. Botnet & Social Engineering

A botnet is a network of compromised devices controlled remotely. Social engineering manipulates people to reveal confidential info. Prevention includes anti-malware, employee training, and monitoring network traffic.

4. Cybercrime Types & Phases

Cybercrimes include hacking, phishing, cyberstalking, and ransomware. Phases are reconnaissance, attack execution, and covering tracks. Organizations prevent them through audits, intrusion detection, and regular updates.

5. Credit Card Fraud Prevention

Credit card fraud includes cloning, phishing, and unauthorized use. Prevention methods: EMV chip cards, transaction monitoring, and two-factor authentication.

6. Mobile Security & Attacks

Mobile threats include viruses, spyware, and data theft. Prevention: app permissions control, regular updates, using VPNs, and installing trusted security apps.

7. Trojan Horse vs. Backdoors

A Trojan horse is malware disguised as legitimate software. Backdoors are hidden access points into systems. Prevention includes anti-malware tools, system hardening, and code audits.

8. SQL Injection Prevention

SQL injection attacks exploit unvalidated input to run unauthorized queries. Prevention includes parameterized queries, input sanitation, and minimal database privileges.

Top 5 Most Repeated Topics (Key Points)

1. Cyber Attacks & Techniques

Includes phishing, DDoS, malware, SQL injection. Defenses: firewalls, encryption, user training.

2. Legal Frameworks (IT Act 2000)

Objectives: regulate digital transactions, prevent cybercrime. Amendments: added provisions for privacy, identity theft, and intermediary responsibility.

3. Identity Theft & Fraud

Involves stealing PII for fraudulent activities. Prevention: strong passwords, secure networks, regular monitoring.

4. Mobile & Wireless Security

Threats: mobile malware, Bluetooth attacks. Defenses: VPNs, app permission control, updates.

5. Ethical Issues & Prevention

Includes software piracy, ethical hacking. Best practices: following legal standards, using licensed software, conducting regular security audits.

Good luck on your exam!