Unit 1: Introduction to Cyber Security

(a) One Mark (Definitions / One-liners)

1. **Define cyberspace**
   → Cyberspace is the virtual environment created by interconnected computer networks, internet, and digital communication systems.

2. **What is World Wide Web (WWW)?**
   → The WWW is a system of interlinked hypertext documents and resources, accessible via the internet using browsers.

3. **Give one issue/challenge of cyber security**
   → Data breaches and identity theft.

4. **Define Internet Society**
   → Internet Society (ISOC) is a global organization that promotes open development, evolution, and use of the Internet for the benefit of all people.

5. **What is cyber security?**
   → Cyber security is the practice of protecting computer systems, networks, and digital data from unauthorized access, attacks, or damage.

🔹 (b) Two Marks Questions – Unit 1

1. Explain architecture of cyberspace

The architecture of cyberspace can be explained through **four main layers**:

- **Physical Layer** → Consists of all hardware components like computers, servers, routers, cables, satellites, and other physical infrastructure that form the backbone of the internet.
- **Logical Layer** → Refers to the software and protocols (TCP/IP, DNS, IP addressing) that enable communication between devices in the network.
- **Information Layer** → Contains data, content, websites, applications, and services that flow across the internet.
- **User Layer** → Involves the end-users (people, organizations, governments) who interact with cyberspace for communication, transactions, and social activities.

👉 Together, these layers ensure smooth functioning of the global cyberspace.

---

2. Difference between Internet and WWW

- **Internet**: The internet is a global network of interconnected computers and devices that communicate through standard protocols (like TCP/IP). It is the underlying infrastructure that allows data transfer, email, and file sharing.
- **World Wide Web (WWW)**: The WWW is a service that runs on the internet. It is a collection of web pages and websites connected by hyperlinks, accessible using browsers (e.g., Chrome, Firefox).

👉 In short: The internet is the “roads and highways,” while the WWW is the “vehicles and shops” running on it.

---

3. Two objectives of cyber security

1. **Confidentiality, Integrity, and Availability (CIA)** → Cyber security ensures that sensitive data is kept confidential, remains accurate without tampering, and is available to authorized users whenever needed.

2. **Protection from cyber threats** → It helps protect computer systems, networks, and data against various cyber threats like hacking, malware, phishing, ransomware, and financial frauds.

👉 Thus, the main goal is to **safeguard information assets and build trust in digital systems**.

Unit 1 (Five Marks QA)

---

1. Issues and Challenges of Cyber Security

Introduction:
Cyber security faces numerous challenges due to the rapid growth of internet users, emerging technologies, and sophisticated attacks. These issues make it difficult for individuals, organizations, and governments to ensure complete security.

Main Issues and Challenges:

1. **Increasing Cyber Crimes** → Hacking, phishing, identity theft, ransomware, and frauds are growing at an alarming rate. Criminals exploit vulnerabilities for financial or personal gains.

2. **Data Privacy Issues** → Sensitive data such as banking details, Aadhaar numbers, or company secrets are at constant risk of being leaked or misused.

3. **Advanced Persistent Threats (APT)** → These are highly sophisticated, long-term targeted attacks where hackers stay undetected inside systems for months or years, stealing critical data.

4. **Zero-day Vulnerabilities** → Software often has unknown security flaws that are exploited by hackers before companies release patches.

5. **Lack of Awareness & Skilled Professionals** → Many users fall for scams due to low cyber awareness, and there is a global shortage of skilled cyber security experts.

6. **Legal and Jurisdiction Challenges** → Cyber crimes often cross national boundaries, making investigation and enforcement complex due to different cyber laws in different countries.

Conclusion:
Cyber security challenges are increasing with digitalization. To address them, we need stronger laws, better awareness, skilled manpower, and advanced security technologies.

---

2. Concept and Importance of Cyber Security

Introduction:
Cyber security refers to the practice of protecting systems, networks, programs, and data from cyber attacks. It involves the use of technologies, processes, and policies to ensure safe digital operations.

Concept of Cyber Security:

- Cyber security is built around the principle of **CIA Triad**:
    - **Confidentiality** → Data should be accessed only by authorized users.
    - **Integrity** → Data should not be altered or destroyed by unauthorized people.
    - **Availability** → Data and systems should always remain available for use when needed.

- It also covers areas like network security, information security, application security, and cloud security.

Importance of Cyber Security:

1. **Prevents Unauthorized Access** → Stops hackers, malware, and intruders from stealing or damaging information.
2. **Ensures Safe Online Transactions** → Protects financial transactions, e-commerce platforms, and banking systems.
3. **Protects Sensitive Data** → Safeguards government, corporate, and personal data against leaks and misuse.
4. **Supports Business and E-Governance** → Builds trust in online services, ensuring digital growth and development.
5. **National Security** → Protects critical infrastructure like defense systems, power grids, airports, and hospitals from cyber terrorism.

Conclusion:
Cyber security is essential in today's digital world as it builds **trust, safety, and resilience** in cyberspace for individuals, businesses, and governments.

---

3. Role of Internet Infrastructure in Data Transfer and Governance

Introduction:
The internet infrastructure is the foundation that enables communication, information sharing, and governance in cyberspace. Without it, global connectivity and digital services would not exist.

Components of Internet Infrastructure:

1. **Routers and Switches** → Direct data packets across networks.
2. **Servers and Data Centers** → Store and deliver applications, websites, and services.
3. **Domain Name System (DNS)** → Translates domain names into IP addresses to locate websites.
4. **Fiber-Optic Cables & Satellites** → Provide high-speed data transmission across the globe.

Role in Data Transfer:

- Ensures **fast, reliable, and secure transfer** of digital information.
- Provides **protocols** like TCP/IP, HTTP, and HTTPS to standardize communication.
- Enables real-time services such as **video conferencing, cloud computing, and online banking**.

Role in Governance:

- Helps in **e-Governance** (online tax filing, Aadhaar, e-voting).
- Supports **digital identity systems** for secure citizen verification.
- Facilitates **global communication** between governments, businesses, and citizens.
- Strengthens **transparency, efficiency, and accountability** in governance through digital platforms.

Conclusion:
Internet infrastructure is the **backbone of digital communication and governance**. Its continuous improvement ensures secure, accessible, and efficient online services for society and government operations.

✅ Unit 2: Cyber Crime and Cyber Law

(a) One Mark (Definitions / One-liners)

1. **Define cyber crime**
   → Cyber crime is any illegal activity carried out using computers, networks, or the internet.

2. **Example of financial fraud**
   → Online banking fraud / Credit card phishing.

3. **What is a zero-day attack?**
   → A cyber attack that exploits unknown software vulnerabilities before they are patched.

4. **Expand IT Act 2000**
   → Information Technology Act, 2000.

5. **What is cyber forensics?**
   → Cyber forensics is the process of collecting, analyzing, and preserving digital evidence to investigate cyber crimes.

🔹 Unit 2 – Two Marks QA

---

1. Two Common Cyber Crimes

Cyber crimes are illegal activities carried out using computers or the internet. Two common types are:

1. **Phishing**
   - Phishing is a cyber crime where attackers send fake emails, messages, or create fraudulent websites that look genuine (like bank or government portals).
   - The aim is to trick victims into revealing sensitive information such as usernames, passwords, ATM PINs, or credit card details.
   - Example: Receiving an email that looks like it is from your bank asking you to “update your account details” through a fake link.
2. **Ransomware Attack**
   - In this attack, malware is installed on a victim’s system which encrypts all files and locks the system.
   - The attacker then demands a ransom (usually in cryptocurrency) in exchange for providing the decryption key.
   - Example: The **WannaCry attack (2017)** that affected thousands of computers worldwide, including hospital systems.

👉 Both phishing and ransomware are major threats because they directly affect financial security and personal data.

---

2. Social Engineering Attack

- Social engineering is a cyber crime technique where **human psychology** is exploited rather than using technical hacking methods.
- Attackers manipulate or trick people into giving away confidential information like passwords, bank details, or OTPs.
- Common forms include:
  1. **Phishing Calls/Emails** – Fake bank calls asking for OTP.
  2. **Pretexting** – Pretending to be an official authority to gain trust.
  3. **Baiting** – Offering free downloads, pen drives, or links that contain malware.
-
- Example: A caller pretending to be from a bank’s customer service and convincing the victim to share their OTP, leading to financial fraud.

- 👉 Social engineering works because people trust others easily, making awareness and caution the best defense.

---

3. Reporting of Cyber Crimes

- **Why report?** Reporting cyber crimes is important to prevent further damage, recover losses, and help authorities track criminals.
- **How to report?**
    1. Victims can lodge a complaint at their **nearest police station** (all police stations in India must accept cyber complaints).
    2. Specialized **Cyber Crime Cells** exist in most cities to handle such cases.
    3. The Government of India has launched the **National Cyber Crime Reporting Portal (cybercrime.gov.in)** where victims can file complaints online.

- **Example:** If someone is a victim of online financial fraud, they should immediately report to the cyber crime helpline **1930** or file an online complaint to block fraudulent transactions.

👉 Timely reporting ensures quick action, prevents other victims from being targeted, and supports law enforcement in strengthening cyber security.

🔹 Unit 2 – FIVE Marks

---

1. Classification of Cyber Crimes with Examples

Cyber crime refers to any illegal activity carried out using computers, networks, or the internet. These crimes can target individuals, property, organizations, society, or even governments. The classification is as follows:

1. **Cyber Crimes against Individuals**
    - Target private persons with the intention to harass, defraud, or steal information.
    - **Examples**: Identity theft (stealing personal data like Aadhaar or credit card details), cyber stalking (sending repeated threatening emails or messages), phishing (fake bank emails).
2. **Cyber Crimes against Property**
    - Aim to damage or steal digital property such as intellectual property, data, or software.
    - **Examples**: Hacking into computer systems to steal files, piracy of movies/software, virus or malware attacks that delete or alter files.
3. **Cyber Crimes against Organizations**
    - Focused on companies or institutions, usually for financial gain or to disrupt services.
    - **Examples**: Ransomware attacks demanding payment, insider attacks by disgruntled employees, denial-of-service (DoS) attacks on company servers.
4. **Cyber Crimes against Society**
    - Affect large groups of people or disrupt social harmony.
    - **Examples**: Circulating fake news, hate speech, spreading child pornography, online gambling, and cyber terrorism activities.
5. **Cyber Crimes against Government**
    - These are highly dangerous crimes that target sensitive government systems or national security.
    - **Examples**: Cyber espionage (stealing defense secrets), hacking official websites, disrupting defense communication networks.

👉 **Conclusion**: Cyber crimes are wide-ranging and can harm individuals, organizations, and nations. Preventive measures, awareness, and strict cyber laws are necessary to control them.

---

2. Cyber Crimes against Women and Children

The rise of digital platforms has unfortunately given criminals new methods to target vulnerable groups, especially women and children.

1. **Cyber Crimes against Women**
    - **Cyber Stalking**: Persistent online harassment through emails, social media, or messages.
    - **Morphing of Images**: Editing women's photos without permission and posting them in obscene ways.
    - **Online Harassment & Defamation**: Spreading false or vulgar information to damage reputation.
    - **Blackmailing & Sextortion**: Threatening to release private information or pictures unless money is paid.
2. **Cyber Crimes against Children**
    - **Cyber Bullying**: Children are insulted, abused, or threatened online, leading to depression or anxiety.
    - **Online Gaming Frauds**: Criminals trick children through gaming apps to reveal personal details or make payments.
    - **Child Pornography**: Creation, sharing, or viewing obscene content involving minors.
    - **Fake Social Media Accounts**: Criminals pretend to be children's friends to exploit them.

👉 **Conclusion**: Such crimes not only break the law but also cause serious **psychological and emotional harm**. Strict implementation of the IT Act, awareness programs, parental monitoring, and cyber police action are essential to protect women and children.

---

3. IT Act 2000 and its Amendments

The **Information Technology Act, 2000 (IT Act 2000)** was India's first cyber law. It was enacted to give legal recognition to electronic transactions and tackle cyber crimes.

1. **Key Provisions of IT Act 2000**
    - Recognizes **electronic records** and **digital signatures** as legally valid.
    - Provides legal framework for **e-commerce and online contracts**.
    - Defines cyber crimes such as hacking, identity theft, and online fraud.
    - Empowers **certifying authorities** to issue digital signatures.
2. **Need for Amendment**
    - With time, new types of crimes like cyber terrorism, phishing, and online harassment emerged, which were not covered by the original law.
3. **Amendments in IT Act 2008**
    - **Cyber Terrorism (Sec 66F)**: Introduced to punish acts that threaten national security through the internet.
    - **Stronger Penalties**: Enhanced punishments for identity theft, phishing, and child pornography.
    - **Corporate Responsibility**: Companies must protect sensitive customer data; negligence can lead to heavy penalties.
    - **Legal Recognition of E-Signatures**: Introduced stronger mechanisms for electronic authentication.

👉 **Conclusion**: The IT Act 2000 and its 2008 amendments are crucial in India's fight against cyber crimes. They provide a legal framework to regulate the digital world, promote e-commerce, and punish cyber criminals effectively.

---

4. Remedial and Mitigation Measures of Cyber Crime

Since cyber crime cannot be eliminated completely, the focus should be on **reducing risks** and responding effectively when crimes occur.

1. **Technical Measures**
    - Use **firewalls and antivirus software** to block malware and intrusions.
    - Apply **data encryption** to protect sensitive files.
    - Keep systems and applications **updated with patches** to fix vulnerabilities.
    - Implement strong authentication methods such as **biometric verification and OTPs**.
2. **Legal Measures**
    - Strict enforcement of cyber laws like the **IT Act 2000 and its amendments**.
    - Establish specialized **cyber courts** for faster trials.
    - Increase international cooperation, since many cyber crimes cross national borders.
3. **Organizational Measures**
    - Companies should run **cyber awareness training** programs for employees.
    - Set up **Incident Response Teams** to act quickly in case of an attack.
    - Implement **data protection policies** and regular audits.
4. **Individual Measures**
    - Use strong, unique passwords and change them regularly.
    - Avoid clicking unknown links or downloading suspicious files.
    - Limit sharing of personal data on social media.
    - Report crimes immediately to the **police, cyber crime cells, or online portals (cybercrime.gov.in)**.

👉 **Conclusion**: Cyber security is everyone's responsibility. A combination of **technical solutions, strict laws, organizational policies, and individual caution** is required to minimize the impact of cyber crimes.