# CYBER THREATS VIRUS, MALWARE, PHISHING, RANSOMWARE SEC (SEMESTER-1)

By

Santosh Kumar Lal

Dept. of Commerce

Sariya College, Suriya

# 🦠 VIRUS

A **computer virus** is a malicious program that attaches itself to a legitimate file or program and spreads when the host file is executed.

**Key Characteristics**

- Requires **user action** to spread (e.g., opening a file)
- Self-replicating
- Attaches to executable files or documents
- Can corrupt or delete data

**Types of Viruses**

- **File Infector Virus** – attaches to executable files
- **Boot Sector Virus** – infects boot records
- **Macro Virus** – spreads through documents (Word, Excel)
- **Polymorphic Virus** – changes its code to evade detection

**Effects**

- Data corruption or deletion
- Slows down system performance
- Causes system crashes

**Prevention**

- Install antivirus software
- Avoid downloading from unknown sources
- Regular system updates
- Scan external devices

# EFFECTS, PREVENTION

# 🐛 MALWARE

**Malware** (malicious software) is a broad term for any software designed to harm, exploit, or gain unauthorized access to systems.

**Types of Malware**

- **Virus** (subset of malware)
- **Worm** – spreads automatically without user action
- **Trojan Horse** – disguised as legitimate software
- **Spyware** – monitors user activity
- **Adware** – displays unwanted ads

**Key Characteristics**

- Designed for **damage, spying, or control**
- Can spread via internet, email, or infected devices
- May run silently in the background

**Effects**

- Theft of personal data
- Unauthorized system access
- System slowdown
- Financial loss

**Prevention**

- Use trusted software sources
- Enable firewalls
- Keep OS and apps updated
- Use anti-malware tools

# EFFECTS, PREVENTION

**Phishing** is a cyber attack where attackers impersonate trusted entities to trick users into revealing sensitive information like passwords, OTPs, or bank details.

**Common Methods**

- Fake emails
- Fraudulent websites
- SMS scams (**Smishing**)
- Voice calls (**Vishing**)

**Characteristics**

- Urgent or threatening messages
- Fake links resembling real websites
- Requests for confidential information

# 🎣 PHISHING

**Examples**

- Email pretending to be from a bank
- Fake login page of social media
- “You won a prize” scams

**Effects**

- Identity theft
- Financial fraud
- Account hacking

**Prevention**

- Check email sender carefully
- Avoid clicking unknown links
- Use two-factor authentication (2FA)
- Verify URLs before entering credentials

# EXAMPLES, EFFECTS, PREVENTION

# 💰 RANSOMWARE

**Definition**

**Ransomware** is a type of malware that encrypts a user's data and demands payment (ransom) to restore access.

**How It Works**

1. Infects system (via email, download, etc.)
2. Encrypts files
3. Displays ransom message
4. Demands payment (often in cryptocurrency like Bitcoin)

**Types**

- **Crypto Ransomware** – encrypts files
- **Locker Ransomware** – locks entire system

**Characteristics**

- Strong encryption
- Payment deadlines
- Threat of data loss

# TYPES, CHARACTERISTICS

# EFFECTS, PREVENTION

**Effects**

- Loss of important data
- Financial damage
- Business disruption

**Prevention**

- Regular data backups
- Avoid suspicious attachments
- Keep software updated
- Use security software

# SUMMARY TABLE

| Threat | Nature | Spread Method | Main Damage |
|---|---|---|---|
| Virus | Self-replicating code | User action required | File corruption |
| Malware | Broad category | Multiple methods | Data theft, control |
| Phishing | Social engineering | Emails, SMS, calls | Credential theft |
| Ransomware | Malware type | Download, phishing | Data encryption, extortion |

Cyber threats are increasing rapidly with technological growth. Understanding their **types, characteristics, and prevention methods** is essential for protecting personal and organizational data. Users must stay aware, cautious, and adopt strong cybersecurity practices.

# CONCLUSION