

**Course-BCA Part II**

**Paper XVI (Internet and Web Technology)**

**Topic- Cyber Security-Spyware**

**Prepared by- A. N. Pandey, Coordinator, School of Computer Science & IT**

### **Cyber Security-Spyware**



Spyware is software that is installed on a computing device without the end user's knowledge. Any software can be classified as spyware if it is downloaded without the user's authorization.

Spyware is typically delivered through infected websites, free mobile or desktop apps and email attachments. Once installed, spyware runs silently in the background, collecting the information it was designed to gather.

Types of spyware include the following:

**Keyloggers** – can monitor and record each keystroke typed on a keyboard.

**Password stealers** – will capture stored passwords.

**Banking Trojans** – can steal payment data, credentials and funds from victims' bank accounts.

**Infostealers** – are designed to capture and record browser history, cookies and information in targeted files.

**Browser hijackers** – can modify web browser settings without the user’s permission and redirect the user to websites the user had not intended to visit.

**Commercial spyware** – is often marketed as “parental control” or “employee monitoring” software.

Spyware can be difficult to detect; often, the first indication that a user has been infected with spyware is a noticeable reduction in network connection speeds, battery life or bank account balance.

To prevent spyware from being installed, users should create strong passwords, only download software from trusted sources, read all clickwrap agreements when installing software and regularly update all operating systems, web browsers and software apps — especially anti-virus applications.

---