# KEYLOGGERS- CYBERSECURITY

A keylogger is a type of software or hardware device that is used to monitor and record the keystrokes typed on a computer or mobile device keyboard. While keyloggers can have legitimate purposes such as monitoring employee activity, parental control, or debugging software, they are often associated with malicious intent in the context of cybersecurity.

Here are some key points about keyloggers in cybersecurity:

Types of Keyloggers: Keyloggers can be classified into two main types: software-based and hardware-based. Software-based keyloggers are typically installed on a computer or device like any other software, often without the user's knowledge. Hardware-based keyloggers are physical devices that are physically attached to the computer or device and intercept keystrokes as they are entered.

Malicious Use: In cybersecurity, keyloggers are frequently used as a tool by attackers to steal sensitive information such as usernames, passwords, credit card numbers, and other personal or financial data. Once installed on a victim's computer, keyloggers can silently capture every keystroke typed by the user and transmit this information to the attacker.

Delivery Methods: Keyloggers can be delivered to a victim's computer through various methods, including phishing emails, malicious attachments, infected websites, or through physical access to the device. They may also be bundled with other malware such as viruses, trojans, or spyware.

Detection and Prevention: Detecting keyloggers can be challenging, as they often operate silently in the background without the user's knowledge. However, there are several methods for detecting and preventing keyloggers, including the use of antivirus software, intrusion detection systems, behavior monitoring tools, and practicing good security hygiene such as keeping software updated and being cautious of suspicious emails or websites.

Legal and Ethical Considerations: The use of keyloggers raises various legal and ethical considerations, especially in cases where they are used without the consent of the user. In many jurisdictions, the unauthorized use of keyloggers to monitor someone's computer activity is illegal and may constitute a violation of privacy laws.

Overall, keyloggers represent a significant threat to cybersecurity and can be used by attackers to steal sensitive information and compromise the security of individuals and organizations. It's essential for users to remain vigilant and take proactive measures to protect themselves against this type of threat

A.Maria Immaculate

# KEYLOGGERS- CYBERSECURITY

CSE-III years