Security Concerns with Key Logger

A **Key Logger** (or keystroke logger) is a type of software program or hardware used to track and record what someone types on their keyboard. It records every keystroke you type and creates a log file containing information of all the keys you typed

It is used for both legal like Data Monitoring and Troubleshooting etc. as well as illegal purposes like Authentication thefts (deciphering the passwords and other information entered using keyboard) and collection of Sensitive information.

Threats and vulnerabilities related to Key Logging

- **Financial Frauds**

  Using Key Logger cyberattackers can decipher your passwords and other sensitive credentials like OTP or account numbers and can cause huge financial frauds

- **Identity Theft**

  The cyberattacker can access victim's personal information using keylogger and misuse it to act in the victim's name, hence become a false source of information and sending false messages to receiver in the name of victim.

- **Exposure of Personal Sensitive Information**

  The Cyber Attacker can stalk victim's personal information and misuse against victim.

- **Data Ransom**

  Ransomware is malware that employs encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases, or applications. A ransom like cash is then demanded to provide access.

Cybercriminals may be able to record and use everything you type. No matter how secure you believe your devices are, a Key Logger hack represents a major threat to your cyber security because they are difficult to detect and cyberattackers can weaponize some of your common virtual activities without your knowledge. A lot of information can be gathered from what you enter on your devices via your emails, text messages, login credentials, and web browsing. Hence the security against Key Logger mainly focuses on prevention of keylogging attack than recovering after the attack.

Measures of Prevention against Key Logging

- **Enable Two-Factor Authentication**

  It is one of the most effective forms of virus, malware, and Key Logger prevention. this solution adds an extra log-in step such as a fingerprint or temporary PIN sent to your phone, helping verify that the person logging into your account is really you. Hence if any cybercriminal try to access the information, he cannot sign in remotely.

- **Don’t download unknown files**

  The second best way is not downloading any unknown file as it can contain any Key Logger software or any file that calls for a Key Logger program to run backend.

- **Install Antivirus Software**

  Installing Antivirus Software that includes protection against spywares and Key logging malwares can be considered as the most effective way for protection against Key Loggers

- **Using Voice to Text Software**

  Using Voice to Text Software can decrease the chances of Key logging as Key Logger specifically focuses on the physical keyboard

- **Do a Program Inventory Check**

  We can check for any Key Logger program running in our pc by opening Task Manager disabling the program which you find malicious or unnecessary as it can be a Key Logger running backend.