Research the practice of key logging in current literature. Describe what it is and explain why some people defend the practice while some others do not. Finally, give your own opinion and defend it. Cite your sources.

Step 1:

Keyloggers are used in everything from Microsoft products to the computers and servers used by your workplace. In rare circumstances, your partner may have installed a keylogger on your laptop or phone to support their accusations of adultery. Worse-case scenarios have demonstrated that hackers may infect trustworthy websites, programmes, and even USB devices with keylogger malware.

Step 2:

logging, or "Keylogging," is the technique of secretly recording input signals from a keyboard into a computer while the computer user is unaware of it. Keylogging can be carried out using a variety of techniques, including software and hardware. These techniques include low-level rootkits, operating system-level API-based programmes, hardware devices connected in-line with keyboard connections, and analysis of electromagnetic signals emitted by a target keyboard from up to 20 metres (66 feet) away.

Keylogging features are frequently included in different types of botnet malware (like the Zeus Trojan) with the intention of capturing users' personal or financial information.

Step 3:

Protect against Key loggers are a type of malware that threatens users today and are becoming more prevalent. Keylogger software captures each keystroke the user makes, and hackers can use this information to crack passwords and access other sensitive information. Keyloggers are unfortunately quite tough to find. This means that without your knowledge, your information may have been compromised for a long period.

Keyloggers are designed to record every keystroke you make on a keyboard, whether it be on a computer or a mobile device. These are utilised to covertly watch your computer usage as you normally would. Keyloggers are employed lawfully for things like gathering user feedback for software development, but they can also be abused by thieves to steal personal data.

Step 4:

Keyloggers can pose a major threat to users by intercepting passwords and other sensitive information typed into the keyboard, hence I do not support them. As a result, fraudsters have access to PIN codes, bank account numbers, email passwords, and login information for social media accounts.

Your information can be easily collected and used by criminals using keyloggers. Time is of the essence once they have infected you with malware through a drive-by download or another method. Before you ever become aware that your sensitive information has been compromised, they can access your accounts.

But finally Keylogging is a technique that, depending on who you ask, has both advantages and disadvantages.