**KEYLOGGER**

1. **What is Keystroke Logging and Keyloggers?**

* Keyloggers are built for the act of keystroke logging — creating records of everything you type on a computer or mobile keyboard. These are used to quietly monitor your computer activity while you use your devices as normal. Keyloggers are used for legitimate purposes like feedback for software development but can be misused by criminals to steal your data.



|  |
| --- |
| Flag: fake flag hehe. |

1. **Keystroke Logging Definition**

* The concept of a keylogger breaks down into two definitions:
  + Keystroke logging: Record-keeping for every key pressed on your keyboard.
  + Keylogger tools: Devices or programs used to log your keystrokes.
* You’ll find use of keyloggers in everything from Microsoft products to your own employer’s computers and servers. In some cases, your spouse may have put a keylogger on your phone or laptop to confirm their suspicions of infidelity. Worse cases have shown criminals to implant legitimate websites, apps, and even USB drives with keylogger malware. Whether for malicious intent or for legitimate uses, you should be aware how keyloggers are affecting you. First, we’ll further define keystroke logging before diving into how keyloggers work. Then you’ll be able to better understand how to secure yourself from unwanted eyes.

1. **What does a Keylogger Do?**

* Keylogger tools can either be hardware or software meant to automate the process of keystroke logging. These tools record the data sent by every keystroke into a text file to be retrieved at a later time. Some tools can record everything on your copy-cut-paste clipboard, calls, GPS data, and even microphone or camera footage. Keyloggers are a surveillance tool with legitimate uses for personal or professional IT monitoring. Some of these uses enter an ethically questionable grey area. However, other keylogger uses are explicitly criminal.
* Regardless of the use, keyloggers are often used without the user’s fully aware consent and keyloggers are used under the assumption that users should behave as normal.

1. **Types of Keyloggers**

* Keylogger tools are mostly constructed for the same purpose. But they’ve got important distinctions in terms of the methods they use and their form factor. Here are the two forms of keyloggers
  + Software keyloggers easyf1@g: \_Im@gIn3\_IS\_r3a1}
  + Hardware keyloggers
  1. Software Keyloggers
* Software keyloggers are computer programs that install onto your device’s hard drive. Common keylogger software types may include:
* API-based keyloggers directly eavesdrop between the signals sent from each keypress to the program you’re typing into. Application programming interfaces (APIs) allow software developers and hardware manufacturers to speak the same “language” and integrate with each other. API keyloggers quietly intercept keyboard APIs, logging each keystroke in a system file. “Form grabbing”-based keyloggers eavesdrop all text entered into website forms once you send it to the server. Data is recorded locally before it is transmitted online to the web server. Kernel-based keyloggers work their way into the system’s core for admin-level permissions. These loggers can bypass and get unrestricted access to everything entered in your system.
  1. Hardware keyloggers
* Hardware are physical components built-in or connected to your device. Some hardware methods may be able to track keystrokes without even being connected to your device. For brevity, we’ll include the keyloggers you are most likely to fend against: Keyboard hardware keyloggers can be placed in line with your keyboard’s connection cable or built into the keyboard itself. This is the most direct form of interception of your typing signals. Hidden camera keyloggers may be placed in public spaces like libraries to visually track keystrokes. USB disk-loaded keyloggers can be a physical Trojan horse that delivers the keystroke logger malware once connected to your device.