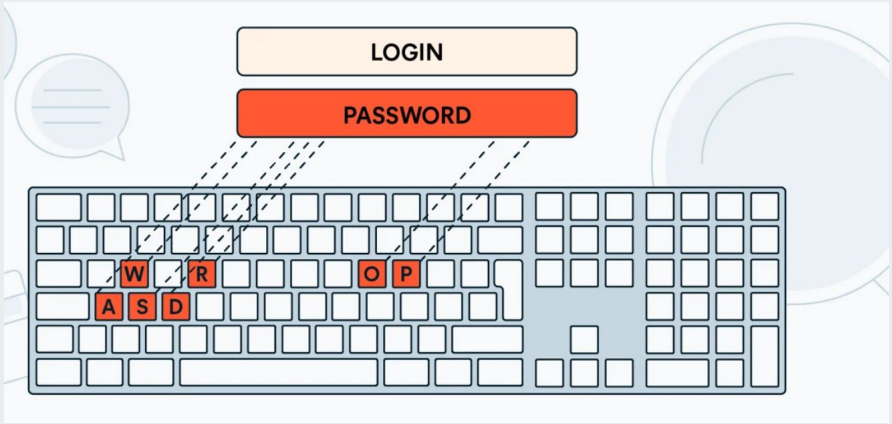
What We Will Cover:

1. What is a keylogger? brief history of keylogger!
2. Types of keyloggers
3. Is a keylogger a virus?
4. How to detect a keylogger on your PC
5. How to prevent keyloggers
6. Example

keylogger :

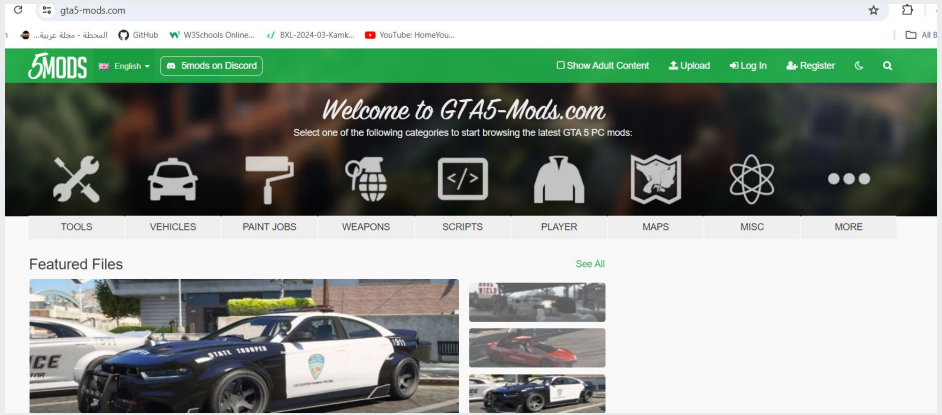
A keylogger is a software or device that logs every keystroke made on a computer. It records letters typed passwords entered and websites visited without the users awareness. The intention is to track and collect all typed information without the users consent.



History of Keylogger:

In the mid-1970s, the Soviet Union created a hardware keylogger called the "selectric bug." This device targeted IBM Selectric typewriters. It worked by detecting small changes in the magnetic field caused by the movements of the typewriter's print head as it typed.

In 2015, a mod for Grand Theft Auto V was uploaded to GTA5-mods.com, unbeknownst to users and site owners, it contained a hidden keylogger called Fade.exe. Players noticed odd game behavior, investigated, and found a mysterious C# compiler running in the background. Fade.exe was found to track and send user activities online.



Types of Keyloggers

Hardware keyloggers are physical devices that record every keystroke. Cybercriminals can disguise them in the computer cabling or in a USB adapter, making it hard for the victim to detect. However, because you need physical access to the device to install a hardware keylogger, it isn't as commonly used in cyberattacks.

Software keyloggers don’t require physical access to a device. Instead, users download software keyloggers onto the device. A user might download a software keylogger intentionally or inadvertently along with malware.

Some software keyloggers can capture additional information without any keyboard key presses. Like-

-Screen Logging – Randomly timed screenshots of your computer screen are logged.
-Activity Tracking – Recording of folders, programs and windows opened and possibly screenshots of each.

How Keyloggers Work

-Web Page Scripts: Malicious code inserted into web pages downloads the keylogger when you click an infected link or visit a malicious site.

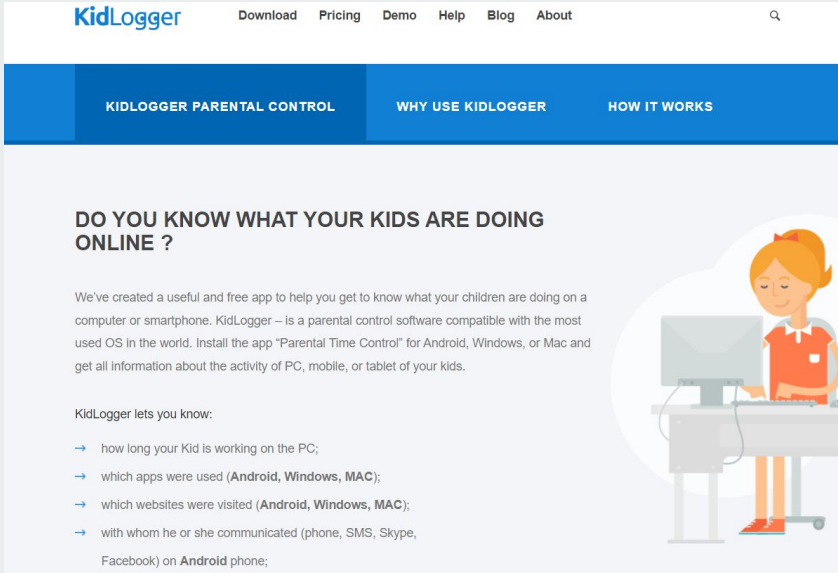
-Phishing: Fraudulent emails that look legitimate contain infected links or malicious attachments. Clicking these results in the keylogger being downloaded.

-Social Engineering: Tactics like phishing trick victims into revealing confidential information or opening attachments that download malware, including keyloggers.

-Unidentified Software: Keyloggers can be embedded in software downloaded from the internet, installing alongside the desired software without the user's knowledge.

Legal Uses of Keyloggers

- Parental Monitoring of Children's Screen Time
- Employee Productivity Tracking by Companies



Detecting Keyloggers

There are three primary warning signs that can help you detect keyloggers:

-A slow browser
-A lag in mouse movements and keystrokes
-A disappearing cursor

Removing Keyloggers

-Use the Task Manager on PCs or the Activity Monitor on Macs. The Task Manager and the Activity Monitor are utility programs that show which applications and background processes are currently running. Review what's running and end any applications or processes that are suspicious.

-Inspect programs and features. Review which programs are installed on your device. If you don't recognize one, research it online and uninstall it if necessary.

-Scan your device using antivirus software. This software constantly scans for malware on your devices, removing it automatically.

Tools to Prevent Keylogging

-Use a firewall.
-Use a password manager and update passwords frequently.
-Update your system frequently.
-Use antivirus software.

Thank you!