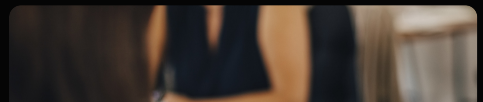
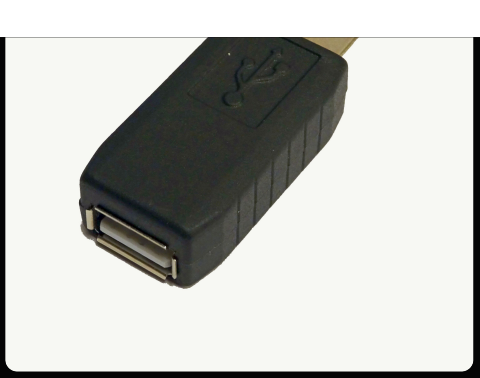
Keylogger Capturing Cybersecurity

With 90% of data breaches caused by human error, it's important to understand the threat of keyloggers. Learn how they work and how to protect your digital life.

by Raghu Varma
Last edited less than a minute ago

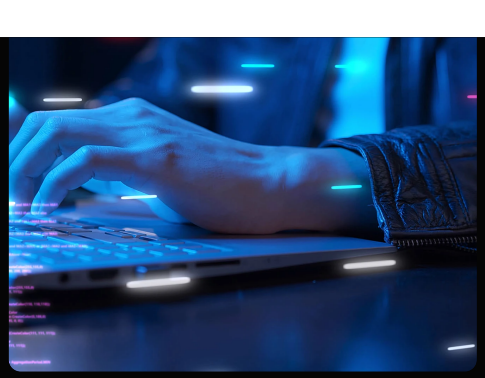
Introduction to Keyloggers





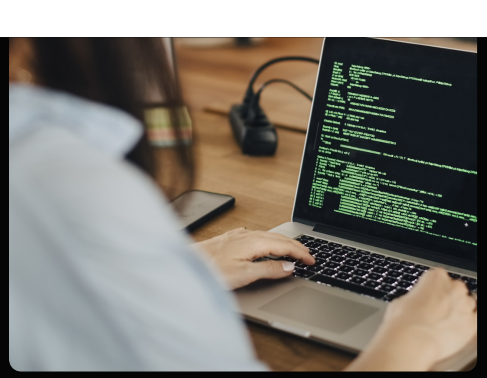
Definition

A software or hardware device that records every keystroke made on a computer.



History

Keyloggers were initially designed for legitimate purposes like monitoring employee productivity, but were later used by malicious actors for nefarious reasons.



How they Work

A keylogger can either be hardware or software. It records every keystroke made on a computer and sends the data to a third-party server.

Types of Keyloggers

Hardware	Physical devices attached to the computer to intercept keystrokes.

Software	Malware installed on the computer often through social engineering or hacking.
Wireless	Connects to a wireless keyboard and sends data to a receiver.
Acoustic	Records the sound of keystrokes and can later decipher which keys were pressed.

How Keyloggers are Used in Cyber Attacks

1

Steal Personal Information

2

Spying

Keyloggers can be installed on computers to spy on

3

Ransomware

Keyloggers can be used to launch ransomware attacks,

Criminals use keyloggers to steal sensitive information like passwords, credit card numbers, and social security numbers.	individuals and monitor their online activities.	encrypting a user's data and forcing them to pay a ransom to regain access.

Detection and Prevention Techniques

Firewalls

Firewalls provide a first level of defense and can detect and block suspicious traffic.

Antivirus

Antivirus programs can detect and remove keyloggers from infected computers.

Virtual Keyboard

Typing sensitive information using a virtual keyboard can prevent keyloggers from capturing key presses.

Password Managers

Password Managers encrypt and protect user's login credentials and can detect malicious activity.

Real-Life Examples of Keylogger Attacks

Wi-Fi Pineapple

Attackers use a tool called the Wi-Fi Pineapple to intercept Wi-Fi traffic and launch keylogger attacks.

Advanced Persistent Threats

Attackers use APTs to infiltrate a victim's computer and remain undetected for an extended period of time.

Ajax Security Team

This group of hackers used keyloggers to steal usernames and passwords, ultimately resulting in the theft of over $1 billion dollars.

Conclusion and Key Takeaways

1 Be Vigilant

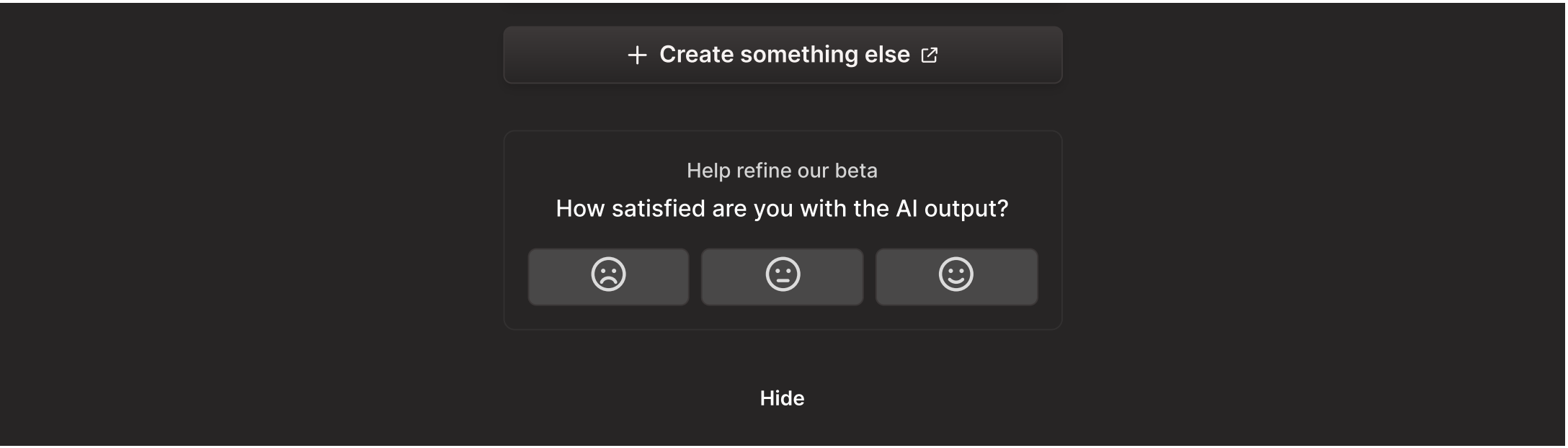
Practice safe online habits, like using strong passwords and updating software regularly.

2 Use Multiple Protection Techniques

No single technique can protect against all keylogger attacks, so use a combination of techniques to protect your digital life.

3 Stay Informed

Technology is constantly evolving, so it's important to stay informed about new threats and protection


+ Create something else
Help refine our beta
How satisfied are you with the AI output?
Hide