What is keylogging and how do you prevent it?

As the [rate of cybercrime steadily increases](https://thehill.com/policy/cybersecurity/519704-european-union-police-agency-warns-of-increase-in-cybercrime-due-to), the need for protection from alternative threats is crucial. Whilst malware and ransomware can have obvious and immediate effects on a computer or network, spyware such as keyloggers are harder to spot and cause damage to your data in more clandestine ways.

# What is Keystroke logging?

Keystroke loggers or [Keyloggers](https://www.kaspersky.co.za/resource-center/definitions/keylogger) are pieces of software or hardware designed to record, log and ultimately share the keystrokes made on a computer. The most basic keystrokes that can be logged are the button presses made on a keyboard; as keyloggers advance, however, the recorded keystrokes likely to be stored are growing to include text that has been copied and pasted, screenshots, microphone and camera usage, and even call history and GPS locations on mobile devices.

This duplicitous monitoring of user activity is such an effective way of enacting harm on a user because they are totally unaware that they are being watched and are likely to let their guard down. The logs of a user’s activity on a computer are incredibly valuable - internet search history, information entered into an application or a website, usernames and passwords can either be sold or used to gain illegal access to a system. ~~As Google claims that R~~oughly [15,000 login credentials are stolen each week due to keylogging](https://money.cnn.com/2017/11/09/technology/google-hackers-research/index.html), meaning that the dangers of such spyware have never been greater.

Whilst keylogging poses a threat to your data security and safety, it can also be used legally and securely within businesses. [Corporate keylogging](https://www.observeit.com/blog/advanced-corporate-keylogging-primer/) is the common practice of hardware and software manufacturers disclosing that they are tracking your activity for ‘usage analytics’. This can be used to improve the design of a product, determine bugs in code or locate unusual user behaviour (like an employee accessing restricted files).

# How does keylogging work?

Keyloggers can exist as [software installed on a computer](https://www.csoonline.com/article/3326304/what-is-a-keylogger-how-attackers-can-monitor-everything-you-type.html) (most commonly), hardware components installed in a computer or as an external device.

**Software keyloggers** disguise themselves as legitimate programs installed on your device and run continuously in the background. The logs of keystrokes may be updated in real-time or in intervals and are saved onto the machine’s hard drive. Then, the keylogs are transmitted to the source of the keylogger to be analysed. The algorithms used in software keyloggers analyse the type of key pressed, how long it was pressed for, when it was pressed and how frequently - this, in turn, allows cybercriminals to determine which combination of characters typed may be a username, password, PIN or email address.

As software keyloggers are installed directly on devices, they are impervious to the protection and security provided by secure remote-work solutions, such as Citrix, VMware and the likes. Although cloud applications and services may be well-encrypted and can reliably keep your data safe, keyloggers avoid those protective features because they ‘steal’ data before it is entered into other software. The threat of keylogging remains the same whether the software used on an endpoint device is secure or not - if anti-keylogging measures are not implemented on the device, no amount of cloud security can prevent a keylogger from harvesting your data.

**Hardware keyloggers** are more dangerous as they cannot be detected through antivirus software. If the keylogger is installed as an electrical component within a keyboard or the cabling of a network, the only way to detect them is through physical inspections. External hardware keyloggers may take the form of a USB drive (which records keystrokes and would be physically removed to retrieve the logs), or a camera installed to film keystrokes (often found above ATMs).

# Spotting a keylogger

Software keyloggers are the greatest form of digital eavesdropping and are incredibly hard to spot. Spyware like keyloggers are known as persistent threats as they can remain undetected in a system for an extended period of time and may only cause direct harm to data weeks, months or years after it was first installed on the system.

The stealth-like nature of keyloggers enables the malicious software to disguise itself from antivirus by claiming to be a safe piece of software or application. As a recent example, the popular social media app [TikTok was caught surreptitiously copying the contents of users’ clipboards](https://nypost.com/2020/06/26/tiktok-caught-spying-on-users-thanks-to-ios-14-feature/) at regular intervals. Whilst the app claimed that this form of keylogging was not intended maliciously, the nature of this privacy invasion, coupled with TikTok’s Chinese ownership has led to its [potential prohibition in the United States](https://www.theverge.com/2020/7/31/21349841/trump-tiktok-bytedance-sell-ownership-china-us-order-ban).

Unlike other viruses which attack instantly, keyloggers require continuous computer resources to copy user keystrokes - this can affect your computer’s performance by slowing down other programs or causing glitches when typing. Unfortunately, this is becoming less common as keyloggers have adapted to embed themselves at the kernel level, deep within a device.

If you believe your device may be infected with a keylogger, the following steps may help to confirm your suspicions:

1. Monitor the processes running on your device when no other applications are open. By using the Task Manager on Windows (Ctrl+Shift+Esc) or the Activity Manager on Mac (Command+Space+“Activity Monitor”) you can track which processes are currently running on your computer. Many normal operating system processes will be running but these may be unrecognisable to you - search the internet for the names of any suspect processes to see if they are malicious.
2. Try to locate a keystroke log by laying a trap. In a new document, type a long and arbitrary combination of letters and numbers which would not appear anywhere else on your computer and save the file. Then, after an hour or two (to allow the keylogger to update its logs) use the search feature on your computer to search for that exact combination of letters and numbers. If more files than just the original document are returned as search results, you would have just found a keylog.
3. Inspect recently modified files. In the Windows File Explorer search bar, select Date Modified > Yesterday from the Search Tools tab to see all files which were modified yesterday. On Mac, press Command+F within Finder and select “Last Modified” from the search conditions to see all recently edited files. Inspect the search results to find any dubious documents which may contain logs of your recent activity.

# Protection against keyloggers

1. Make sure your antivirus is up-to-date; this provides the best defence from keyloggers entering your system.
2. Read the terms, agreements and permission requests of any software or app you are installing to make sure you know what private data they are recording.
3. Make use of virtual/ on-screen keyboards when typing sensitive information as logging clicks on a screen is much harder than recording key presses.
4. Don’t leave your devices unattended as this provides opportunities for criminals to install unwanted hardware and software.
5. Make use of two-factor authentication to maximise your security if one of your devices becomes compromised.

# Our solution to keylogger protection

At Redite, we recommend the SentryBay [Armored Client](https://redite.co/armoredclient) data-security toolset to protect against all cyber threats, including keylogging. A key element of the Armored Client package is the [anti-keylogger defence](https://www.sentrybay.com/news/article/sentrybay-launches-anti-keylogging-solution-for-mobile-devices) which stops keyloggers, even at the kernel level - this includes protection against screen capture, encryption of all keypresses, a secure virtual keyboard and scans of your system to detect and protect against any harmful keylogging behaviour.

Glossary:

Spyware → malicious software that gathers personal information on a digital device and uses that data to enact harm.

Kernel → can be considered the fundamental core of all devices with operating systems. It has complete control of all memory, processes and hardware installed.

Notes:

If you want a video to accompany, I thought [this one](https://www.youtube.com/watch?v=L8169DHNeQ0) was okay.