5 METHODS TO PREVENT KEYLOGGING ATTACKS

**Method no. 1 - Use a 2-Step Verification**

Using 2-Step verification helps prevent keylogging attacks. It requires entering a pin code sent to a mobile phone via text to verify identity. It prevents hackers from accessing your account even if he is able to steal your username and password through a keylogger.

If you want to secure your account from unauthorized access, enable a 2-Step verification. When someone tries to access your account without your permission, you’ll get notified immediately. That’s the primary step on how to prevent keylogging attacks.

**Method no. 2 - Install Software Updates**

Installing Software updates patches vulnerabilities on the computer. Thus, prevents exploit kits from injecting keyloggers. It addresses the existing issues on the computer that hackers can exploit. It also installs new features on the application, making them more efficient.

Also, remember to install the latest updates for your browsers too. Hackers also exploit outdated plug-ins and add-ons. If you want to keep your computer security tight, install software updates. Installing software updates is another effective method for how to prevent keylogging attacks.

**Method no. 3 - Use Key Encryption Software**

Key encryption software encrypt the keys you press on the keyboard to prevent keyloggers from capturing the exact keys. They conceal the keystrokes as they reach the application. So keylogger will only be able to log the characters used to encrypt the sensitive information. If you want to add another layer of security against keyloggers, use key encryption software.

**Method no. 4 - Avoid Downloading Crack Software**

Refusing to download crack software also prevents keyloggers from infecting the computer. Crack software is often infected with malware. They are free, but they could be unsafe for your computer. You may inadvertently install a keylogger disguised as computer software.

If you want to keep your computer malware free, avoid downloading crack software. Download trusted applications only. That’s another good way on how to prevent keylogging attacks.

**Method no. 5 - Install Anti Malware Program**

Anti Malware software protects you from varieties of malware such as keyloggers, [ransomware](https://enterprise.comodo.com/ransomware-attacks.php), [rootkit](https://enterprise.comodo.com/rootkit-definition/), and [trojan](https://enterprise.comodo.com/example-of-a-trojan-horse.php). It scans the files that enter the computer, thus detects and prevents fake software. It also regularly scans the computer for malware to keep the hard drive malware free.

Anti malware software also protects your keyboard from direct access. So it prevents any malicious software from gaining direct access to it.

Those are some effective methods on how to prevent keylogging attacks.

What if you want to know if there’s a keylogger lurking on your computer, how can you tell? Below are some ways on how to detect keyloggers on the computer.

**How to Detect Keyloggers Step no. 1 - Task Manager**

The Task Manager enables you to see the active applications on the computer. Press Ctrl+Alt+Del to open Task Manager. In the list of applications, check if there’s any suspicious file, if a keylogger is active, it should be visible in Task Manager. Disable the malicious application.

**How to Detect Keyloggers Step no. 2 - Programs and Features**

In Programs and Features, you will see the list of applications you installed on the computer. If an application appears suspicious with an unverified publisher, you can Google it. If it is unnecessary, uninstall it. It could have been installed without your knowledge.

**How to Detect Keyloggers Step no. 3 - Full Malware Scan**

If you want to ensure your protection from keyloggers, do a full malware scan on the PC. Look for a reputable anti malware software. It will scan the computer for malware. The threats detected will be displayed when the malware scanning process is finished. Just click remove and exit. That’s how to detect keyloggers fast and easy.

**Conclusion**

To prevent keyloggers from stealing your personal information, you need to take preventive measures and add an extra layer of security. Keylogger is easy to detect, but once it infects your computer, it can cause unauthorized transactions. Data-stealing malware attacks are prevalent today. Don’t leave your computer vulnerable.

Do you own a business network and want to protect your endpoint devices from malicious keyloggers? Click here to learn more about [endpoint protection](https://enterprise.comodo.com/blog/what-is-endpoint-security/).