Keystroke logging

From Wikipedia, the free encyclopedia

  (Redirected from [Keylogger](https://en.wikipedia.org/w/index.php?title=Keylogger&redirect=no))

[Jump to navigation](https://en.wikipedia.org/wiki/Keystroke_logging#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Keystroke_logging#searchInput)

|  |
| --- |
| This article is part of a series on |
| [**Information security**](https://en.wikipedia.org/wiki/Information_security) |
| **Related security categories** |
| * [Automotive security](https://en.wikipedia.org/wiki/Automotive_security) * [Cybercrime](https://en.wikipedia.org/wiki/Cybercrime)   + [Cybersex trafficking](https://en.wikipedia.org/wiki/Cybersex_trafficking)   + [Computer fraud](https://en.wikipedia.org/wiki/Computer_fraud) * [Cyberwarfare](https://en.wikipedia.org/wiki/Cyberwarfare) * [Internet security](https://en.wikipedia.org/wiki/Internet_security) * [Mobile security](https://en.wikipedia.org/wiki/Mobile_security) * [Network security](https://en.wikipedia.org/wiki/Network_security) |
| **Threats** |
| * [Advanced persistent threat](https://en.wikipedia.org/wiki/Advanced_persistent_threat) * [Backdoors](https://en.wikipedia.org/wiki/Backdoor_(computing)) * [Bootkits](https://en.wikipedia.org/wiki/Bootkit) * [Computer crime](https://en.wikipedia.org/wiki/Computer_crime) * [Viruses](https://en.wikipedia.org/wiki/Computer_virus) * [Denial of service](https://en.wikipedia.org/wiki/Denial_of_service) * [Eavesdropping](https://en.wikipedia.org/wiki/Eavesdropping) * [Exploits](https://en.wikipedia.org/wiki/Exploit_(computer_security)) * [Keyloggers](https://en.wikipedia.org/wiki/Keylogger) * [Logic bombs](https://en.wikipedia.org/wiki/Logic_bomb) * [Malware](https://en.wikipedia.org/wiki/Malware) * [Payloads](https://en.wikipedia.org/wiki/Payload_(computing)) * [Phishing](https://en.wikipedia.org/wiki/Phishing) * [Ransomware](https://en.wikipedia.org/wiki/Ransomware) * [Rootkits](https://en.wikipedia.org/wiki/Rootkit) * [Screen scrapers](https://en.wikipedia.org/wiki/Screen_scrape) * [Spyware](https://en.wikipedia.org/wiki/Spyware) * [Trojans](https://en.wikipedia.org/wiki/Trojan_horse_(computing)) * [Vulnerabilities](https://en.wikipedia.org/wiki/Vulnerability_(computing)) * [Web shells](https://en.wikipedia.org/wiki/Web_shell) * [Web application security](https://en.wikipedia.org/wiki/Web_application_security) * [Worms](https://en.wikipedia.org/wiki/Computer_worm) |
| **Defenses** |
| * [Computer access control](https://en.wikipedia.org/wiki/Computer_access_control) * [Application security](https://en.wikipedia.org/wiki/Application_security)   + [Antivirus software](https://en.wikipedia.org/wiki/Antivirus_software)   + [Secure coding](https://en.wikipedia.org/wiki/Secure_coding)   + [Secure by default](https://en.wikipedia.org/wiki/Secure_by_default)   + [Secure by design](https://en.wikipedia.org/wiki/Secure_by_design)   + [Secure operating systems](https://en.wikipedia.org/wiki/Security-focused_operating_system) * [Authentication](https://en.wikipedia.org/wiki/Authentication)   + [Multi-factor authentication](https://en.wikipedia.org/wiki/Multi-factor_authentication) * [Authorization](https://en.wikipedia.org/wiki/Authorization) * [Data-centric security](https://en.wikipedia.org/wiki/Data-centric_security) * [Encryption](https://en.wikipedia.org/wiki/Encryption) * [Firewall](https://en.wikipedia.org/wiki/Firewall_(computing)) * [Intrusion detection system](https://en.wikipedia.org/wiki/Intrusion_detection_system) * [Mobile secure gateway](https://en.wikipedia.org/wiki/Mobile_secure_gateway) * [Runtime application self-protection (RASP)](https://en.wikipedia.org/wiki/Runtime_application_self-protection) |
| * [v](https://en.wikipedia.org/wiki/Template:Information_security) * [t](https://en.wikipedia.org/wiki/Template_talk:Information_security) * [e](https://en.wikipedia.org/w/index.php?title=Template:Information_security&action=edit) |

**Keystroke logging**, often referred to as **keylogging** or **keyboard capturing**, is the action of recording (logging) the keys struck on a [keyboard](https://en.wikipedia.org/wiki/Keyboard_(computing)), typically covertly, so that person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program. A **keystroke recorder** or **keylogger** can be either [software](https://en.wikipedia.org/wiki/Software) or [hardware](https://en.wikipedia.org/wiki/Computer_hardware).

While the programs themselves are legal,[[1]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-1) with many of them being designed to allow employers to oversee the use of their computers, keyloggers are most often used for stealing [passwords](https://en.wikipedia.org/wiki/Password) and other [confidential information](https://en.wikipedia.org/wiki/Confidential_information).[[2]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-2)[[3]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-3)

Keylogging can also be used to study [human-computer interaction](https://en.wikipedia.org/wiki/Human%E2%80%93computer_interaction). Numerous keylogging methods exist: they range from hardware and software-based approaches to [acoustic](https://en.wikipedia.org/wiki/Acoustics) analysis.

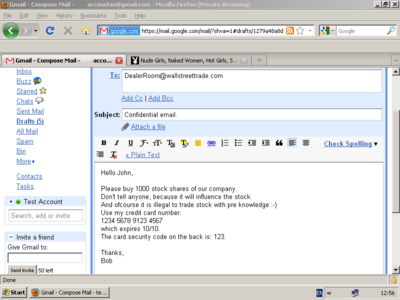


**Contents**

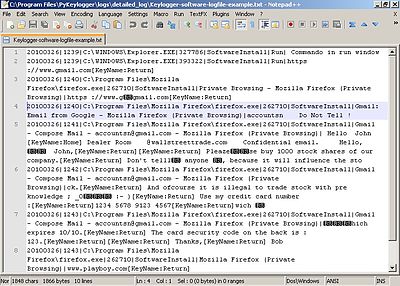
* [1Application](https://en.wikipedia.org/wiki/Keystroke_logging#Application)
  + [1.1Software-based keyloggers](https://en.wikipedia.org/wiki/Keystroke_logging#Software-based_keyloggers)
    - [1.1.1Keystroke logging in writing process research](https://en.wikipedia.org/wiki/Keystroke_logging#Keystroke_logging_in_writing_process_research)
    - [1.1.2Related features](https://en.wikipedia.org/wiki/Keystroke_logging#Related_features)
  + [1.2Hardware-based keyloggers](https://en.wikipedia.org/wiki/Keystroke_logging#Hardware-based_keyloggers)
* [2History](https://en.wikipedia.org/wiki/Keystroke_logging#History)
* [3Cracking](https://en.wikipedia.org/wiki/Keystroke_logging#Cracking)
  + [3.1Trojans](https://en.wikipedia.org/wiki/Keystroke_logging#Trojans)
  + [3.2Use by police](https://en.wikipedia.org/wiki/Keystroke_logging#Use_by_police)
* [4Countermeasures](https://en.wikipedia.org/wiki/Keystroke_logging#Countermeasures)
  + [4.1Anti-keyloggers](https://en.wikipedia.org/wiki/Keystroke_logging#Anti-keyloggers)
  + [4.2Live CD/USB](https://en.wikipedia.org/wiki/Keystroke_logging#Live_CD/USB)
  + [4.3Anti-spyware / Anti-virus programs](https://en.wikipedia.org/wiki/Keystroke_logging#Anti-spyware_/_Anti-virus_programs)
  + [4.4Network monitors](https://en.wikipedia.org/wiki/Keystroke_logging#Network_monitors)
  + [4.5Automatic form filler programs](https://en.wikipedia.org/wiki/Keystroke_logging#Automatic_form_filler_programs)
  + [4.6One-time passwords (OTP)](https://en.wikipedia.org/wiki/Keystroke_logging#One-time_passwords_(OTP))
  + [4.7Security tokens](https://en.wikipedia.org/wiki/Keystroke_logging#Security_tokens)
  + [4.8On-screen keyboards](https://en.wikipedia.org/wiki/Keystroke_logging#On-screen_keyboards)
  + [4.9Keystroke interference software](https://en.wikipedia.org/wiki/Keystroke_logging#Keystroke_interference_software)
  + [4.10Speech recognition](https://en.wikipedia.org/wiki/Keystroke_logging#Speech_recognition)
  + [4.11Handwriting recognition and mouse gestures](https://en.wikipedia.org/wiki/Keystroke_logging#Handwriting_recognition_and_mouse_gestures)
  + [4.12Macro expanders/recorders](https://en.wikipedia.org/wiki/Keystroke_logging#Macro_expanders/recorders)
  + [4.13Deceptive typing](https://en.wikipedia.org/wiki/Keystroke_logging#Deceptive_typing)
* [5See also](https://en.wikipedia.org/wiki/Keystroke_logging#See_also)
* [6References](https://en.wikipedia.org/wiki/Keystroke_logging#References)
* [7External links](https://en.wikipedia.org/wiki/Keystroke_logging#External_links)

Application[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=1)]

**Software-based keyloggers**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=2)]

[](https://en.wikipedia.org/wiki/File:Keylogger-screen-capture-example.png)

A keylogger example of a screen capture, which holds potentially confidential and private information. The image below holds the corresponding keylogger text result.

[](https://en.wikipedia.org/wiki/File:Keylogger-software-logfile-example.jpg)

A [logfile](https://en.wikipedia.org/wiki/Logfile) from a software-based keylogger, based on the screen capture above.

Software-based keyloggers are computer programs designed to work on the target computer's [software](https://en.wikipedia.org/wiki/Software).[[4]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-4) Keyloggers are used in [IT](https://en.wikipedia.org/wiki/Information_technology) organizations to troubleshoot technical problems with computers and business networks. Families and business people use keyloggers legally to monitor network usage without their users' direct knowledge. Even [Microsoft](https://en.wikipedia.org/wiki/Microsoft) publicly admitted that [Windows 10](https://en.wikipedia.org/wiki/Windows_10) operation system has a built-in keylogger in its final version “to improve typing and writing services”.[[5]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-5) However, malicious individuals can use keyloggers on public computers to steal passwords or credit card information. Most keyloggers are not stopped by [HTTPS](https://en.wikipedia.org/wiki/HTTP_Secure) encryption because that only protects [data in transit](https://en.wikipedia.org/wiki/Data_in_transit) between computers, thus the threat being from the user's computer.

From a technical perspective, there are several categories:

* **Hypervisor-based**: The keylogger can theoretically reside in a [malware](https://en.wikipedia.org/wiki/Malware) [hypervisor](https://en.wikipedia.org/wiki/Hypervisor) running underneath the operating system, which thus remains untouched. It effectively becomes a [virtual machine](https://en.wikipedia.org/wiki/Virtual_machine). [Blue Pill](https://en.wikipedia.org/wiki/Blue_Pill_(software)) is a conceptual example.
* [**Kernel**](https://en.wikipedia.org/wiki/Kernel_(computing))**-based**: A program on the machine obtains [root access](https://en.wikipedia.org/wiki/Superuser) to hide in the OS and intercepts keystrokes that pass through the kernel. This method is difficult both to write and to combat. Such keyloggers reside at the [kernel level](https://en.wikipedia.org/wiki/Ring_(computer_security)), which makes them difficult to detect, especially for user-mode applications that don't have root access. They are frequently implemented as [rootkits](https://en.wikipedia.org/wiki/Rootkit) that subvert the operating system kernel to gain unauthorized access to the hardware. This makes them very powerful. A keylogger using this method can act as a keyboard [device driver](https://en.wikipedia.org/wiki/Device_driver), for example, and thus gain access to any information typed on the keyboard as it goes to the operating system.
* **API-based**: These keyloggers [hook](https://en.wikipedia.org/wiki/Hooking) keyboard [APIs](https://en.wikipedia.org/wiki/Application_programming_interface) inside a running application. The keylogger registers keystroke events as if it was a normal piece of the application instead of malware. The keylogger receives an event each time the user presses or releases a key. The keylogger simply records it.
  + Windows APIs such as GetAsyncKeyState(), GetForegroundWindow(), etc. are used to poll the state of the keyboard or to subscribe to keyboard events.[[6]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-6) A more recent example simply polls the [BIOS](https://en.wikipedia.org/wiki/BIOS) for pre-boot authentication [PINs](https://en.wikipedia.org/wiki/Personal_identification_number) that have not been cleared from memory.[[7]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-7)
* **Form grabbing based**: [Form grabbing](https://en.wikipedia.org/wiki/Form_grabbing)-based keyloggers log [web form](https://en.wikipedia.org/wiki/Form_(web)) submissions by recording the web browsing on submit events. This happens when the user completes a form and submits it, usually by clicking a button or hitting enter. This type of keylogger records forms data before it is passed over the Internet.
* **Javascript-based:** A malicious script tag is injected into a targeted web page, and listens for key events such as onKeyUp(). Scripts can be injected via a variety of methods, including [cross-site scripting](https://en.wikipedia.org/wiki/Cross-site_scripting), [man-in-the-browser](https://en.wikipedia.org/wiki/Man-in-the-browser), [man-in-the-middle](https://en.wikipedia.org/wiki/Man-in-the-middle_attack), or a compromise of the remote web site.[[8]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-8)
* **Memory-injection-based**: Memory Injection ([MitB](https://en.wikipedia.org/wiki/Man-in-the-browser))-based keyloggers perform their logging function by altering the memory tables associated with the browser and other system functions. By patching the memory tables or injecting directly into memory, this technique can be used by malware authors to bypass Windows UAC (User Account Control). The [Zeus](https://en.wikipedia.org/wiki/Zeus_(malware)) and [SpyEye](https://en.wikipedia.org/wiki/SpyEye_trojan) trojans use this method exclusively.[[9]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-9) Non-Windows systems have protection mechanisms that allow access to locally recorded data from a remote location.[[*clarification needed*](https://en.wikipedia.org/wiki/Wikipedia:Please_clarify)] Remote communication may be achieved when one of these methods is used:
  + Data is uploaded to a website, database or an [FTP](https://en.wikipedia.org/wiki/File_Transfer_Protocol) server.
  + Data is periodically emailed to a pre-defined [email address](https://en.wikipedia.org/wiki/Email_address).
  + Data is [wirelessly](https://en.wikipedia.org/wiki/Wireless) transmitted employing an attached hardware system.
  + The software enables a remote login to the local machine from the Internet or the local network, for data logs stored on the target machine.

**Keystroke logging in writing process research**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=3)]

Keystroke logging is now an established research method for the study of writing processes.[[10]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-10)[[11]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-11) Different programs have been developed to collect online process data of writing activities,[[12]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-AAA-12) including [Inputlog](https://en.wikipedia.org/wiki/Inputlog), Scriptlog, and Translog.

Keystroke logging is legitimately used as a suitable research instrument in several writing contexts. These include studies on cognitive writing processes, which include

* descriptions of writing strategies; the writing development of children (with and without writing difficulties),
* spelling,
* first and second language writing, and
* specialist skill areas such as translation and subtitling.

Keystroke logging can be used to research writing, specifically. It can also be integrated into educational domains for second language learning, programming skills, and typing skills.

**Related features**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=4)]

Software keyloggers may be augmented with features that capture user information without relying on keyboard key presses as the sole input. Some of these features include:

* Clipboard logging. Anything that has been copied to the [clipboard](https://en.wikipedia.org/wiki/Clipboard_(software)) can be captured by the program.
* Screen logging. [Screenshots](https://en.wikipedia.org/wiki/Screenshot) are taken to capture graphics-based information. Applications with screen logging abilities may take screenshots of the whole screen, of just one application, or even just around the mouse cursor. They may take these screenshots periodically or in response to user behaviors (for example, when a user clicks the mouse). A practical application that is used by some keyloggers with this screen logging ability, is to take small screenshots around where a mouse has just clicked; thus defeating web-based keyboards (for example, the web-based screen keyboards that are often used by banks), and any web-based on-screen keyboard without screenshot protection.
* Programmatically capturing the text in a [control](https://en.wikipedia.org/wiki/GUI_widget). The [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows) [API](https://en.wikipedia.org/wiki/Application_programming_interface) allows programs to request the text 'value' in some controls. This means that some passwords may be captured, even if they are hidden behind password masks (usually asterisks).[[13]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-13)
* The recording of every program/folder/window opened including a screenshot of every website visited.
* The recording of [search engines queries](https://en.wikipedia.org/wiki/Web_search_query), [instant messenger](https://en.wikipedia.org/wiki/Instant_messenger) conversations, FTP downloads and other Internet-based activities (including the bandwidth used).

**Hardware-based keyloggers**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=5)]

[](https://en.wikipedia.org/wiki/File:USB_Hardware_Keylogger.jpg)

A hardware-based keylogger.

[](https://en.wikipedia.org/wiki/File:Usb-logger.jpg)

A connected hardware-based keylogger.

*Main article:*[*Hardware keylogger*](https://en.wikipedia.org/wiki/Hardware_keylogger)

Hardware-based keyloggers do not depend upon any software being installed as they exist at a hardware level in a computer system.

* Firmware-based: [BIOS](https://en.wikipedia.org/wiki/BIOS)-level [firmware](https://en.wikipedia.org/wiki/Firmware) that handles keyboard events can be modified to record these events as they are processed. Physical and/or [root-level access](https://en.wikipedia.org/wiki/Superuser) is required to the machine, and the software loaded into the BIOS needs to be created for the specific hardware that it will be running on.[[14]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-14)
* Keyboard hardware: Hardware keyloggers are used for keystroke logging utilizing a hardware circuit that is attached somewhere in between the [computer keyboard](https://en.wikipedia.org/wiki/Computer_keyboard) and the computer, typically inline with the keyboard's cable connector. There are also [USB](https://en.wikipedia.org/wiki/Universal_Serial_Bus) connectors based Hardware keyloggers as well as ones for Laptop computers (the Mini-PCI card plugs into the expansion slot of a laptop). More stealthy implementations can be installed or built into standard keyboards so that no device is visible on the external cable. Both types log all keyboard activity to their [internal memory](https://en.wikipedia.org/wiki/Primary_storage), which can be subsequently accessed, for example, by typing in a secret key sequence. A hardware keylogger has an advantage over a software solution: it is not dependent on being installed on the target computer's operating system and therefore will not interfere with any program running on the target machine or be detected by any [software](https://en.wikipedia.org/wiki/Anti-spyware_software). However, its physical presence may be detected if, for example, it is installed outside the case as an inline device between the computer and the keyboard. Some of these implementations can be controlled and monitored remotely using a wireless communication standard.[[15]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-15)
* Wireless keyboard and mouse sniffers: These passive sniffers collect packets of data being transferred from a wireless keyboard and its receiver. As encryption may be used to secure the wireless communications between the two devices, this may need to be cracked beforehand if the transmissions are to be read. In some cases, this enables an attacker to type arbitrary commands into a victim's computer.[[16]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-16)
* Keyboard overlays: Criminals have been known to use keyboard overlays on [ATMs](https://en.wikipedia.org/wiki/Automated_teller_machine) to capture people's PINs. Each keypress is registered by the keyboard of the ATM as well as the criminal's keypad that is placed over it. The device is designed to look like an integrated part of the machine so that bank customers are unaware of its presence.[[17]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-17)
* Acoustic keyloggers: [Acoustic cryptanalysis](https://en.wikipedia.org/wiki/Acoustic_cryptanalysis) can be used to monitor the sound created by someone typing on a computer. Each key on the keyboard makes a subtly different acoustic signature when struck. It is then possible to identify which keystroke signature relates to which keyboard character via [statistical methods](https://en.wikipedia.org/wiki/Statistics) such as [frequency analysis](https://en.wikipedia.org/wiki/Frequency_analysis). The repetition frequency of similar acoustic keystroke signatures, the timings between different keyboard strokes and other context information such as the probable language in which the user is writing are used in this analysis to map sounds to letters.[[18]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-18) A fairly long recording (1000 or more keystrokes) is required so that a big enough [sample](https://en.wikipedia.org/wiki/Sample_(statistics)) is collected.[[19]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-19)
* Electromagnetic emissions: It is possible to capture the [electromagnetic emissions](https://en.wikipedia.org/wiki/Electromagnetic_radiation) of a wired keyboard from up to 20 metres (66 ft) away, without being physically wired to it.[[20]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-20) In 2009, Swiss researchers tested 11 different [USB](https://en.wikipedia.org/wiki/Universal_Serial_Bus), [PS/2](https://en.wikipedia.org/wiki/IBM_Personal_System/2) and laptop keyboards in a semi-[anechoic chamber](https://en.wikipedia.org/wiki/Anechoic_chamber) and found them all vulnerable, primarily because of the prohibitive cost of adding [shielding](https://en.wikipedia.org/wiki/Electromagnetic_shielding) during manufacture.[[21]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-21) The researchers used a wide-band [receiver](https://en.wikipedia.org/wiki/Receiver_(radio)) to tune into the specific frequency of the emissions radiated from the keyboards.
* Optical surveillance: Optical surveillance, while not a keylogger in the classical sense, is nonetheless an approach that can be used to capture passwords or PINs. A strategically placed camera, such as a hidden [surveillance camera](https://en.wikipedia.org/wiki/Surveillance_camera) at an [ATM](https://en.wikipedia.org/wiki/Automated_teller_machine), can allow a criminal to watch a PIN or password being entered.[[22]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-22)[[23]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-23)
* Physical evidence: For a keypad that is used only to enter a security code, the keys which are in actual use will have evidence of use from many fingerprints. A passcode of four digits, if the four digits in question are known, is reduced from 10,000 possibilities to just 24 possibilities (104 versus 4! ([factorial](https://en.wikipedia.org/wiki/Factorial) of 4)). These could then be used on separate occasions for a manual "brute force attack".
* Smartphone sensors: Researchers have demonstrated that it is possible to capture the keystrokes of nearby computer keyboards using only the commodity [accelerometer](https://en.wikipedia.org/wiki/Accelerometer) found in smartphones.[[24]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-24) The attack is made possible by placing a smartphone near a keyboard on the same desk. The smartphone's accelerometer can then detect the vibrations created by typing on the keyboard and then translate this raw accelerometer signal into readable sentences with as much as 80 percent accuracy. The technique involves working through probability by detecting pairs of keystrokes, rather than individual keys. It models "keyboard events" in pairs and then works out whether the pair of keys pressed is on the left or the right side of the keyboard and whether they are close together or far apart on the QWERTY keyboard. Once it has worked this out, it compares the results to a preloaded dictionary where each word has been broken down in the same way.[[25]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-25) Similar techniques have also been shown to be effective at capturing keystrokes on touchscreen keyboards[[26]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-26)[[27]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-27)[[28]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-28) while in some cases, in combination with [gyroscope](https://en.wikipedia.org/wiki/Gyroscope)[[29]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-29)[[30]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-30) or with the ambient-light sensor.[[31]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-31)
* Body keyloggers: Body keyloggers tracks and analyze body movements to determine which keys were stroke. The attacker needs to be familiar with the keys layout of the tracked keyboard to correlate between body movements and keys position. Tracking audible signals of the user' interface (e.g. a sound the device produce to informs the user that a keystroke was logged) may reduce the complexity of the body keylogging algorithms, as it marks the moment at which a key was pressed.[[32]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-32)

History[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=6)]

In the mid-1970s, the [Soviet Union](https://en.wikipedia.org/wiki/Soviet_Union) developed and deployed a hardware keylogger targeting [typewriters](https://en.wikipedia.org/wiki/Typewriter). Termed the "selectric bug", it measured the movements of the print head of IBM Selectric typewriters via subtle influences on the regional magnetic field caused by the rotation and movements of the print head.[[33]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-33) An early keylogger was written by [Perry Kivolowitz](https://en.wikipedia.org/wiki/Perry_Kivolowitz) and posted to the Usenet newsgroup net.unix-wizards, net.sources on November 17, 1983.[[34]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-34) The posting seems to be a motivating factor in restricting access to /dev/kmem on [Unix](https://en.wikipedia.org/wiki/Unix) systems. The [user-mode](https://en.wikipedia.org/wiki/User-mode) program operated by locating and dumping character lists (clients) as they were assembled in the Unix kernel.

In the 1970s, spies installed keystroke loggers in the US Embassy and Consulate buildings in [Moscow](https://en.wikipedia.org/wiki/Moscow).[[35]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-35)[[36]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-ingersoll-36) They installed the bugs in [Selectric](https://en.wikipedia.org/wiki/Selectric) II and Selectric III electric typewriters.[[37]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-gunman-37)

Soviet embassies used manual typewriters, rather than electric typewriters, for [classified information](https://en.wikipedia.org/wiki/Classified_information)—apparently because they are immune to such bugs.[[37]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-gunman-37) As of 2013, Russian special services still use typewriters.[[36]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-ingersoll-36)[[38]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-38)[[39]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-39)

Cracking[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=7)]

Writing simple software applications for keylogging can be trivial, and like any nefarious computer program, can be distributed as a [trojan horse](https://en.wikipedia.org/wiki/Trojan_horse_(computing)) or as part of a [virus](https://en.wikipedia.org/wiki/Computer_virus). What is not trivial for an attacker, however, is installing a covert keystroke logger without getting caught and downloading data that has been logged without being traced. An attacker that manually connects to a host machine to download logged keystrokes risks being traced. A trojan that sends keylogged data to a fixed e-mail address or [IP address](https://en.wikipedia.org/wiki/IP_address) risks exposing the attacker.

**Trojans**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=8)]

Researchers[[*who?*](https://en.wikipedia.org/wiki/Wikipedia:Manual_of_Style/Words_to_watch#Unsupported_attributions)] devised several methods for solving this problem.[[*clarification needed*](https://en.wikipedia.org/wiki/Wikipedia:Please_clarify)] They presented a deniable password snatching attack in which the keystroke logging trojan is installed using a virus or [worm](https://en.wikipedia.org/wiki/Computer_worm).[[40]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-auto-40)[[41]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-41) An attacker who is caught with the virus or worm can claim to be a victim. The [cryptotrojan](https://en.wikipedia.org/wiki/Cryptotrojan) asymmetrically encrypts the pilfered login/password pairs using the [public key](https://en.wikipedia.org/wiki/Public_key) of the trojan author and covertly broadcasts the resulting [ciphertext](https://en.wikipedia.org/wiki/Ciphertext). They mentioned that the ciphertext can be [steganographically](https://en.wikipedia.org/wiki/Steganography) encoded and posted to a public bulletin board such as [Usenet](https://en.wikipedia.org/wiki/Usenet).[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

**Use by police**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=9)]

In 2000, the [FBI](https://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation) used FlashCrest iSpy to obtain the [PGP](https://en.wikipedia.org/wiki/Pretty_Good_Privacy) [passphrase](https://en.wikipedia.org/wiki/Passphrase) of [Nicodemo Scarfo, Jr.](https://en.wikipedia.org/wiki/Nicodemo_Scarfo,_Jr.), son of mob boss [Nicodemo Scarfo](https://en.wikipedia.org/wiki/Nicodemo_Scarfo).[[42]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-42) Also in 2000, the FBI lured two suspected Russian cybercriminals to the US in an elaborate ruse, and captured their usernames and passwords with a keylogger that was covertly installed on a machine that they used to access their computers in [Russia](https://en.wikipedia.org/wiki/Russia). The FBI then used these credentials to hack into the suspects' computers in Russia to obtain evidence to prosecute them.[[43]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-43)

Countermeasures[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=10)]

The effectiveness of countermeasures varies because keyloggers use a variety of techniques to capture data and the countermeasure needs to be effective against the particular data capture technique. In the case of Windows 10 keylogging from Microsoft it is enough to change some privacy settings on your computer.[[44]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-44) For example, an on-screen keyboard will be effective against hardware keyloggers, transparency will defeat some—but not all—screen loggers and an [anti-spyware](https://en.wikipedia.org/wiki/Anti-spyware) application that can only disable hook-based keyloggers will be ineffective against kernel-based keyloggers.

Also, keylogger program authors may be able to update the code to adapt to countermeasures that may have proven to be effective against them.

**Anti-keyloggers**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=11)]

*Main article:*[*Anti-keylogger*](https://en.wikipedia.org/wiki/Anti-keylogger)

An [anti-keylogger](https://en.wikipedia.org/wiki/Anti-keylogger) is a piece of [software](https://en.wikipedia.org/wiki/Software) specifically designed to detect keyloggers on a computer, typically comparing all files in the computer against a database of keyloggers looking for similarities which might signal the presence of a hidden keylogger. As anti-keyloggers have been designed specifically to detect keyloggers, they have the potential to be more effective than conventional antivirus software; some antivirus software do not consider keyloggers to be malware, as under some circumstances a keylogger can be considered a legitimate piece of software.[[45]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-45)

**Live CD/USB**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=12)]

Rebooting the computer using a [Live CD](https://en.wikipedia.org/wiki/Live_CD) or write-protected [Live USB](https://en.wikipedia.org/wiki/Live_USB) is a possible countermeasure against software keyloggers if the CD is clean of malware and the operating system contained on it is secured and fully patched so that it cannot be infected as soon as it is started. Booting a different operating system does not impact the use of a hardware or BIOS based keylogger.

**Anti-spyware / Anti-virus programs**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=13)]

Many [anti-spyware](https://en.wikipedia.org/wiki/Anti-spyware) applications can detect some software based keyloggers and quarantine, disable or cleanse them. However, because many keylogging programs are legitimate pieces of software under some circumstances, anti-spyware often neglects to label keylogging programs as spyware or a virus. These applications can detect software-based keyloggers based on patterns in [executable code](https://en.wikipedia.org/wiki/Subroutine), [heuristics](https://en.wikipedia.org/wiki/Heuristics) and keylogger behaviors (such as the use of [hooks](https://en.wikipedia.org/wiki/Hooking) and certain [APIs](https://en.wikipedia.org/wiki/Application_programming_interface)).

No software-based anti-spyware application can be 100% effective against all keyloggers.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] Also, software-based anti-spyware cannot defeat non-software keyloggers (for example, hardware keyloggers attached to keyboards will always receive keystrokes before any software-based anti-spyware application).

However, the particular technique that the anti-spyware application uses will influence its potential effectiveness against software keyloggers. As a general rule, anti-spyware applications with [higher privileges](https://en.wikipedia.org/wiki/Ring_(computer_security)) will defeat keyloggers with lower privileges. For example, a hook-based anti-spyware application cannot defeat a kernel-based keylogger (as the keylogger will receive the keystroke messages before the anti-spyware application), but it could potentially defeat hook- and API-based keyloggers.

**Network monitors**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=14)]

[Network monitors](https://en.wikipedia.org/wiki/Network_monitoring) (also known as reverse-firewalls) can be used to alert the user whenever an application attempts to make a network connection. This gives the user the chance to prevent the keylogger from "[phoning home](https://en.wikipedia.org/wiki/Phoning_home)" with his or her typed information.

**Automatic form filler programs**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=15)]

*Main article:*[*Form filler*](https://en.wikipedia.org/wiki/Form_filler)

Automatic form-filling programs may prevent keylogging by removing the requirement for a user to type personal details and passwords using the keyboard. [Form fillers](https://en.wikipedia.org/wiki/Form_filler) are primarily designed for [web browsers](https://en.wikipedia.org/wiki/Web_browser) to fill in checkout pages and log users into their accounts. Once the user's account and [credit card](https://en.wikipedia.org/wiki/Credit_card) information has been entered into the program, it will be automatically entered into forms without ever using the keyboard or [clipboard](https://en.wikipedia.org/wiki/Clipboard_(software)), thereby reducing the possibility that private data is being recorded. However, someone with physical access to the machine may still be able to install software that can intercept this information elsewhere in the operating system or while in transit on the network. ([Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security) (TLS) reduces the risk that data in transit may be intercepted by [network sniffers](https://en.wikipedia.org/wiki/Packet_analyzer) and [proxy tools](https://en.wikipedia.org/wiki/Proxy_server).)

**One-time passwords (OTP)**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=16)]

Using [one-time passwords](https://en.wikipedia.org/wiki/One-time_password) may be keylogger-safe, as each password is invalidated as soon as it is used. This solution may be useful for someone using a public computer. However, an attacker who has remote control over such a computer can simply wait for the victim to enter his/her credentials before performing unauthorized transactions on their behalf while their session is active.

**Security tokens**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=17)]

Use of [smart cards](https://en.wikipedia.org/wiki/Smart_card) or other [security tokens](https://en.wikipedia.org/wiki/Security_token) may improve security against [replay attacks](https://en.wikipedia.org/wiki/Replay_attack) in the face of a successful keylogging attack, as accessing protected information would require both the (hardware) security token *as well as* the appropriate password/passphrase. Knowing the keystrokes, mouse actions, display, clipboard, etc. used on one computer will not subsequently help an attacker gain access to the protected resource. Some security tokens work as a type of hardware-assisted one-time password system, and others implement a cryptographic [challenge-response authentication](https://en.wikipedia.org/wiki/Challenge-response_authentication), which can improve security in a manner conceptually similar to one time passwords. [Smartcard readers](https://en.wikipedia.org/wiki/Card_reader) and their associated keypads for [PIN](https://en.wikipedia.org/wiki/Personal_identification_number) entry may be vulnerable to keystroke logging through a so-called [supply chain attack](https://en.wikipedia.org/wiki/Supply_chain_attack)[[46]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-46) where an attacker substitutes the card reader/PIN entry hardware for one which records the user's PIN.

**On-screen keyboards**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=18)]

Most on-screen keyboards (such as the on-screen keyboard that comes with [Windows XP](https://en.wikipedia.org/wiki/Windows_XP)) send normal keyboard event messages to the external target program to type text. Software key loggers can log these typed characters sent from one program to another.[[47]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-47) Additionally, keylogging software can take screenshots of what is displayed on the screen (periodically, and/or upon each mouse click), which means that although certainly a useful security measure, an on-screen keyboard will not protect from all keyloggers.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

**Keystroke interference software**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=19)]

Keystroke interference software is also available.[[48]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-48) These programs attempt to trick keyloggers by introducing random keystrokes, although this simply results in the keylogger recording more information than it needs to. An attacker has the task of extracting the keystrokes of interest—the security of this mechanism, specifically how well it stands up to [cryptanalysis](https://en.wikipedia.org/wiki/Cryptanalysis), is unclear.

**Speech recognition**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=20)]

Similar to on-screen keyboards, [speech-to-text conversion](https://en.wikipedia.org/wiki/Speech_recognition) software can also be used against keyloggers, since there are no typing or mouse movements involved. The weakest point of using voice-recognition software may be how the software sends the recognized text to target software after the recognition took place.

**Handwriting recognition and mouse gestures**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=21)]

Also, many [PDAs](https://en.wikipedia.org/wiki/Personal_digital_assistant) and lately [tablet PCs](https://en.wikipedia.org/wiki/Tablet_computer) can already convert pen (also called stylus) movements on their [touchscreens](https://en.wikipedia.org/wiki/Touchscreen) to computer understandable text successfully. [Mouse gestures](https://en.wikipedia.org/wiki/Mouse_gestures) use this principle by using mouse movements instead of a stylus. Mouse gesture programs convert these strokes to user-definable actions, such as typing text. Similarly, [graphics tablets](https://en.wikipedia.org/wiki/Graphics_tablet) and [light pens](https://en.wikipedia.org/wiki/Light_pen) can be used to input these gestures, however, these are less common every day.

The same potential weakness of speech recognition applies to this technique as well.

**Macro expanders/recorders**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=22)]

With the help of many programs, a seemingly meaningless text can be expanded to a meaningful text and most of the time context-sensitively, e.g. "en.wikipedia.org" can be expanded when a web browser window has the focus. The biggest weakness of this technique is that these programs send their keystrokes directly to the target program. However, this can be overcome by using [the 'alternating' technique described below](https://en.wikipedia.org/wiki/Keystroke_logging#_Nontechnological_methods), i.e. sending mouse clicks to non-responsive areas of the target program, sending meaningless keys, sending another mouse click to the target area (e.g. password field) and switching back-and-forth.

**Deceptive typing**[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=23)]

Alternating between typing the login credentials and typing characters somewhere else in the focus window[[49]](https://en.wikipedia.org/wiki/Keystroke_logging#cite_note-49) can cause a keylogger to record more information than they need to, but this could be easily filtered out by an attacker. Similarly, a user can move their cursor using the mouse while typing, causing the logged keystrokes to be in the wrong order e.g., by typing a password beginning with the last letter and then using the mouse to move the cursor for each subsequent letter. Lastly, someone can also use [context menus](https://en.wikipedia.org/wiki/Context_menu) to remove, [cut, copy, and paste](https://en.wikipedia.org/wiki/Cut,_copy,_and_paste) parts of the typed text without using the keyboard. An attacker who can capture only parts of a password will have a larger [key space](https://en.wikipedia.org/wiki/Key_space_(cryptography)) to attack if he chose to execute a [brute-force attack](https://en.wikipedia.org/wiki/Brute-force_attack).

Another very similar technique uses the fact that any selected text portion is replaced by the next key typed. e.g., if the password is "secret", one could type "s", then some dummy keys "asdf". Then, these dummies could be selected with the mouse, and the next character from the password "e" is typed, which replaces the dummies "asdf".

These techniques assume incorrectly that keystroke logging software cannot directly monitor the clipboard, the selected text in a form, or take a screenshot every time a keystroke or mouse click occurs. They may, however, be effective against some hardware keyloggers.

See also[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=24)]

* [Anti-keylogger](https://en.wikipedia.org/wiki/Anti-keylogger)
* [Black-bag cryptanalysis](https://en.wikipedia.org/wiki/Black-bag_cryptanalysis)
* [Computer surveillance](https://en.wikipedia.org/wiki/Computer_surveillance)
* [Digital footprint](https://en.wikipedia.org/wiki/Digital_footprint)
* [Hardware keylogger](https://en.wikipedia.org/wiki/Hardware_keylogger)
* [Reverse connection](https://en.wikipedia.org/wiki/Reverse_connection)
* [Session replay](https://en.wikipedia.org/wiki/Session_replay)
* [Spyware](https://en.wikipedia.org/wiki/Spyware)
* [Trojan horse](https://en.wikipedia.org/wiki/Trojan_horse_(computing))
* [Virtual keyboard](https://en.wikipedia.org/wiki/Virtual_keyboard)
* [Web tracking](https://en.wikipedia.org/wiki/Web_tracking)

References[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=25)]

* 1. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-1) [Use of legal software products for computer monitoring](https://www.keylogger.org/keylogger.html#h_8), keylogger.org
  2. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-2) [*"Keylogger"*](http://oxforddictionaries.com/definition/english/keylogger)*. Oxford dictionaries.*
  3. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-3) [Keyloggers: How they work and how to detect them (Part 1)](https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/), *Secure List*, "Today, keyloggers are mainly used to steal user data relating to various online payment systems, and virus writers are constantly writing new keylogger Trojans for this very purpose."
  4. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-4) [*"What is a Keylogger?"*](http://www.pctools.com/security-news/what-is-a-keylogger/)*. PC Tools.*
  5. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-5) *Caleb Chen (2017-03-20).*[*"Microsoft Windows 10 has a keylogger enabled by default – here's how to disable it"*](https://www.privateinternetaccess.com/blog/2017/03/microsoft-windows-10-keylogger-enabled-default-heres-disable/)*.*
  6. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-6) [*"The Evolution of Malicious IRC Bots"*](http://www.symantec.com/avcenter/reference/the.evolution.of.malicious.irc.bots.pdf)*(PDF).*[*Symantec*](https://en.wikipedia.org/wiki/NortonLifeLock)*. 2005-11-26: 23–24. Retrieved 2011-03-25.*
  7. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-7) *Jonathan Brossard (2008-09-03).*[*"Bypassing pre-boot authentication passwords by instrumenting the BIOS keyboard buffer (practical low level attacks against x86 pre-boot authentication software)"*](https://web.archive.org/web/20080913072014/http:/www.ivizsecurity.com/research/preboot/preboot_whitepaper.pdf)*(PDF).*[*Iviz Technosolutions*](http://www.ivizsecurity.com/)*. Archived from*[*the original*](http://www.ivizsecurity.com/research/preboot/preboot_whitepaper.pdf)*(PDF) on 2008-09-13. Retrieved 2008-09-23.* External link in |publisher= ([help](https://en.wikipedia.org/wiki/Help:CS1_errors#param_has_ext_link))
  8. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-8) [*"Web-Based Keylogger Used to Steal Credit Card Data from Popular Sites"*](https://threatpost.com/web-based-keylogger-used-to-steal-credit-card-data-from-popular-sites/121141/)*. Threatpost | The first stop for security news. 2016-10-06. Retrieved 2017-01-24.*
  9. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-9) [*"SpyEye Targets Opera, Google Chrome Users"*](https://krebsonsecurity.com/2011/04/spyeye-targets-opera-google-chrome-users/)*. Krebs on Security. Retrieved 26 April 2011.*
  10. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-10) K.P.H. Sullivan & E. Lindgren (Eds., 2006), Studies in Writing: Vol. 18. Computer Key-Stroke Logging and Writing: Methods and Applications. Oxford: Elsevier.
  11. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-11) V. W. Berninger (Ed., 2012), Past, present, and future contributions of cognitive writing research to cognitive psychology. New York/Sussex: Taylor & Francis. [ISBN](https://en.wikipedia.org/wiki/ISBN_(identifier)) [9781848729636](https://en.wikipedia.org/wiki/Special:BookSources/9781848729636)
  12. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-AAA_12-0) *Vincentas (11 July 2013).*[*"Keystroke Logging in SpyWareLoop.com"*](https://web.archive.org/web/20131207133350/http:/www.spywareloop.com/news/keystroke-logging)*. Spyware Loop. Archived from*[*the original*](http://www.spywareloop.com/news/keystroke-logging)*on 7 December 2013. Retrieved 27 July 2013.*
  13. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-13) *Microsoft.*[*"EM\_GETLINE Message()"*](http://msdn.microsoft.com/en-us/library/bb761584(VS.85).aspx)*.*[*Microsoft*](https://en.wikipedia.org/wiki/Microsoft)*. Retrieved 2009-07-15.*
  14. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-14) [*"Apple keyboard hack"*](https://web.archive.org/web/20090826150015/http:/www.digitalsociety.org/2009/08/apple-keyboards-hacked-and-possessed)*. Digital Society. Archived from*[*the original*](http://www.digitalsociety.org/2009/08/apple-keyboards-hacked-and-possessed/)*on 26 August 2009. Retrieved 9 June 2011.*
  15. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-15) [*"Keylogger Removal"*](https://web.archive.org/web/20110429181147/http:/spyreveal.com/keyloggerremoval)*. SpyReveal Anti Keylogger. Archived from*[*the original*](http://spyreveal.com/keyloggerremoval)*on 29 April 2011. Retrieved 25 April 2011.*
  16. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-16) [*"Keylogger Removal"*](https://www.bastille.net/technical-details)*. SpyReveal Anti Keylogger. Retrieved 26 February 2016.*
  17. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-17) *Jeremy Kirk (2008-12-16).*[*"Tampered Credit Card Terminals"*](http://www.pcworld.com/article/155525/.html?tk=rss_news)*.*[*IDG*](https://en.wikipedia.org/wiki/International_Data_Group)*News Service. Retrieved 2009-04-19.*
  18. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-18) *Andrew Kelly (2010-09-10).*[*"Cracking Passwords using Keyboard Acoustics and Language Modeling"*](http://www.inf.ed.ac.uk/publications/thesis/online/IM100855.pdf)*(PDF).*
  19. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-19) *Sarah Young (14 September 2005).*[*"Researchers recover typed text using audio recording of keystrokes"*](http://www.berkeley.edu/news/media/releases/2005/09/14_key.shtml)*. UC Berkeley NewsCenter.*
  20. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-20) *Knight, Will.*[*"A Year Ago: Cypherpunks publish proof of Tempest | ZDNet"*](https://www.zdnet.com/article/a-year-ago-cypherpunks-publish-proof-of-tempest/)*. ZDNet.*
  21. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-21) *Martin Vuagnoux and Sylvain Pasini (2009-06-01). Vuagnoux, Martin; Pasini, Sylvain (eds.).*[*"Compromising Electromagnetic Emanations of Wired and Wireless Keyboards"*](http://infoscience.epfl.ch/record/140523?ln=en)*. Proceedings of the 18Th Usenix Security Symposium.*
  22. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-22) [*"ATM camera"*](http://www.snopes.com/fraud/atm/atmcamera.asp)*.*[*snopes.com*](http://snopes.com/)*. Retrieved 2009-04-19.* External link in |publisher= ([help](https://en.wikipedia.org/wiki/Help:CS1_errors#param_has_ext_link))
  23. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-23) *Maggi, Federico; Volpatto, Alberto; Gasparini, Simone; Boracchi, Giacomo; Zanero, Stefano (2011).*[*A fast eavesdropping attack against touchscreens*](http://www.syssec-project.eu/m/page-media/3/iclearshot-ias11.pdf)*(PDF). 7th International Conference on Information Assurance and Security. IEEE.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1109/ISIAS.2011.6122840*](https://doi.org/10.1109%2FISIAS.2011.6122840)*.*
  24. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-24) *Marquardt, Philip; Verma, Arunabh; Carter, Henry; Traynor, Patrick (2011). (sp)iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers. Proceedings of the 18th ACM conference on Computer and communications security. ACM. pp. 561–562.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1145/2046707.2046771*](https://doi.org/10.1145%2F2046707.2046771)*.*
  25. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-25) [*"iPhone Accelerometer Could Spy on Computer Keystrokes"*](https://www.wired.com/2011/10/iphone-keylogger-spying/)*. Wired. 19 October 2011. Retrieved August 25, 2014.*
  26. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-26) *Owusu, Emmanuel; Han, Jun; Das, Sauvik; Perrig, Adrian; Zhang, Joy (2012). ACCessory: password inference using accelerometers on smartphones. Proceedings of the Thirteenth Workshop on Mobile Computing Systems and Applications. ACM.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1145/2162081.2162095*](https://doi.org/10.1145%2F2162081.2162095)*.*
  27. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-27) *Aviv, Adam J.; Sapp, Benjamin; Blaze, Matt; Smith, Jonathan M. (2012). Practicality of accelerometer side channels on smartphones. Proceedings of the 28th Annual Computer Security Applications Conference. ACM.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1145/2420950.2420957*](https://doi.org/10.1145%2F2420950.2420957)*.*
  28. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-28) *Cai, Liang; Chen, Hao (2011).*[*TouchLogger: inferring keystrokes on touch screen from smartphone motion*](https://www.usenix.org/events/hotsec11/tech/final_files/Cai.pdf)*(PDF). Proceedings of the 6th USENIX conference on Hot topics in security. USENIX. Retrieved 25 August 2014.*
  29. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-29) *Xu, Zhi; Bai, Kun; Zhu, Sencun (2012). TapLogger: inferring user inputs on smartphone touchscreens using on-board motion sensors. Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks. ACM. pp. 113–124.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1145/2185448.2185465*](https://doi.org/10.1145%2F2185448.2185465)*.*
  30. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-30) *Miluzzo, Emiliano; Varshavsky, Alexander; Balakrishnan, Suhrid; Choudhury, Romit Roy (2012). Tapprints: your finger taps have fingerprints. Proceedings of the 10th international conference on Mobile systems, applications, and services. ACM. pp. 323–336.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1145/2307636.2307666*](https://doi.org/10.1145%2F2307636.2307666)*.*
  31. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-31) *Spreitzer, Raphael (2014). PIN Skimming: Exploiting the Ambient-Light Sensor in Mobile Devices. Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices. ACM. pp. 51–62.*[*arXiv*](https://en.wikipedia.org/wiki/ArXiv_(identifier))*:*[*1405.3760*](https://arxiv.org/abs/1405.3760)*.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1145/2666620.2666622*](https://doi.org/10.1145%2F2666620.2666622)*.*
  32. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-32) *Hameiri, Paz (2019).*[*"Body Keylogging"*](https://hakin9.org/product/hacking-with-raspberry-pi-4/)*. Hakin9 IT Security Magazine.****14****(7): 79–94.*
  33. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-33) [*"Selectric bug"*](http://www.cryptomuseum.com/covert/bugs/selectric/index.htm)*.*
  34. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-34) [*"The Security Digest Archives"*](http://securitydigest.org/unix/archive/006)*. Retrieved 2009-11-22.*
  35. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-35) [*"Soviet Spies Bugged World's First Electronic Typewriters"*](https://web.archive.org/web/20131220110339/http:/www.qccglobal.com/news/first-keystroke-logger.php)*. qccglobal.com. Archived from*[*the original*](http://www.qccglobal.com/news/first-keystroke-logger.php)*on 2013-12-20. Retrieved 2013-12-20.*
  36. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-ingersoll_36-0) [***b***](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-ingersoll_36-1) Geoffrey Ingersoll. ["Russia Turns To Typewriters To Protect Against Cyber Espionage"](http://www.businessinsider.com/russia-turns-to-typewriters-for-secrets-2013-7). 2013.
  37. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-gunman_37-0) [***b***](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-gunman_37-1) Sharon A. Maneki. ["Learning from the Enemy: The GUNMAN Project"](http://www.nsa.gov/about/_files/cryptologic_heritage/center_crypt_history/publications/learning_from_the_enemy_the_gunman_project.pdf) [Archived](https://web.archive.org/web/20171203032854/https:/www.nsa.gov/about/_files/cryptologic_heritage/center_crypt_history/publications/learning_from_the_enemy_the_gunman_project.pdf) 2017-12-03 at the [Wayback Machine](https://en.wikipedia.org/wiki/Wayback_Machine). 2012.
  38. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-38) *Agence France-Presse, Associated Press.*[*"Wanted: 20 electric typewriters for Russia to avoid leaks"*](http://technology.inquirer.net/27149/wanted-20-electric-typewriters-for-russia-to-avoid-leaks)*. inquirer.net.*
  39. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-39) Anna Arutunyan. ["Russian security agency to buy typewriters to avoid surveillance"](http://themoscownews.com/russia/20130711/191758523/Russian-security-agency-to-buy-typewriters-to-avoid-surveillance.html) [Archived](https://web.archive.org/web/20131221071647/http:/themoscownews.com/russia/20130711/191758523/Russian-security-agency-to-buy-typewriters-to-avoid-surveillance.html) 2013-12-21 at the [Wayback Machine](https://en.wikipedia.org/wiki/Wayback_Machine).
  40. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-auto_40-0) *Young, Adam; Yung, Moti (1997). Deniable Password Snatching: On the Possibility of Evasive Electronic Espionage. Proceedings of IEEE Symposium on Security and Privacy. pp. 224–235.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1109/SECPRI.1997.601339*](https://doi.org/10.1109%2FSECPRI.1997.601339)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-0-8186-7828-8*](https://en.wikipedia.org/wiki/Special:BookSources/978-0-8186-7828-8)*.*
  41. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-41) *Young, Adam; Yung, Moti (1996). Cryptovirology: extortion-based security threats and countermeasures. Proceedings of IEEE Symposium on Security and Privacy. pp. 129–140.*[*CiteSeerX*](https://en.wikipedia.org/wiki/CiteSeerX_(identifier))[*10.1.1.44.9122*](https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.44.9122)*.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1109/SECPRI.1996.502676*](https://doi.org/10.1109%2FSECPRI.1996.502676)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-0-8186-7417-4*](https://en.wikipedia.org/wiki/Special:BookSources/978-0-8186-7417-4)*.*
  42. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-42) *John Leyden (2000-12-06).*[*"Mafia trial to test FBI spying tactics: Keystroke logging used to spy on mob suspect using PGP"*](https://www.theregister.co.uk/2000/12/06/mafia_trial_to_test_fbi/)*. The Register. Retrieved 2009-04-19.*
  43. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-43) *John Leyden (2002-08-16).*[*"Russians accuse FBI Agent of Hacking"*](https://www.theregister.co.uk/2002/08/16/russians_accuse_fbi_agent/)*. The Register.*
  44. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-44) *Alex Stim (2015-10-28).*[*"3 methods to disable Windows 10 built-in Spy Keylogger"*](http://www.spyrix.com/3-methods-to-disable-windows-10-built-in-spy-keylogger.php)*.*
  45. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-45) [*"What is Anti Keylogger?"*](http://www.securitysupervisor.com/security-q-a/computer-security/218-what-is-anti-keylogger)*. 23 August 2018.*
  46. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-46) *Austin Modine (2008-10-10).*[*"Organized crime tampers with European card swipe devices"*](https://www.theregister.co.uk/2008/10/10/organized_crime_doctors_chip_and_pin_machines/)*. The Register. Retrieved 2009-04-18.*
  47. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-47) *Scott Dunn (2009-09-10).*[*"Prevent keyloggers from grabbing your passwords"*](http://windowssecrets.com/top-story/prevent-keyloggers-from-grabbing-your-passwords/)*. Windows Secrets. Retrieved 2014-05-10.*
  48. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-48) *Christopher Ciabarra (2009-06-10).*[*"Anti Keylogger"*](https://web.archive.org/web/20100626093658/http:/networkintercept.com/keystrokeinterference.html)*. Networkintercept.com. Archived from*[*the original*](http://networkintercept.com/keystrokeinterference.html)*on 2010-06-26.*
  49. [**^**](https://en.wikipedia.org/wiki/Keystroke_logging#cite_ref-49) *Cormac Herley and Dinei Florencio (2006-02-06).*[*"How To Login From an Internet Cafe Without Worrying About Keyloggers"*](http://cups.cs.cmu.edu/soups/2006/posters/herley-poster_abstract.pdf)*(PDF).*[*Microsoft Research*](https://en.wikipedia.org/wiki/Microsoft_Research)*. Retrieved 2008-09-23.*

External links[[edit](https://en.wikipedia.org/w/index.php?title=Keystroke_logging&action=edit&section=26)]

|  |  |
| --- | --- |
|  | Wikimedia Commons has media related to [***Keystroke logging***](https://commons.wikimedia.org/wiki/Category:Keystroke_logging). |

* [Keyloggers](https://curlie.org/Computers/Security/Products_and_Tools/Monitoring/Keyloggers/) at [Curlie](https://en.wikipedia.org/wiki/Curlie)