**TEXT**

**WHAT IS SPYWARE?**



Spyware is a type of malicious software -- or [malware](https://searchsecurity.techtarget.com/definition/malware) -- that is installed on a computing device without the end user's knowledge. It invades the device, steals sensitive information and internet usage data, and relays it to advertisers, data firms or external users.

Any software can be classified as spyware if it is downloaded without the user's authorization. Spyware is controversial because, even when it is installed for relatively innocuous reasons, it can violate the end user's privacy and has the potential to be abused.

Spyware is one of the most common threats to internet users. Once installed, it monitors internet activity, tracks login credentials and spies on sensitive information. The primary goal of spyware is usually to obtain credit card numbers, banking information and passwords.

But spyware can also be used to track a person's location, as is the case with stalkerware. Often installed secretly on mobile phones by jealous spouses, ex-partners and even concerned parents, this type of spyware can track the physical location of the victim, intercept their emails and texts, eavesdrop on their phone calls and record conversations, and access personal data, such as photos and videos.

Spyware can be difficult to detect; often, the first indication a user has that a computing device has been infected with spyware is a noticeable reduction in processor or network connection speeds and -- in the case of mobile devices -- data usage and battery life. Antispyware tools can be used to prevent or remove spyware. They can either provide real-time protection by scanning network data and blocking malicious data, or they can execute scans to detect and remove spyware already on a system.

**TEXT**

**HOW DOES SPYWARE WORK?**



Spyware can make its way onto a device without the end user's knowledge via an app install package, file attachment or malicious website. In its least damaging form, spyware exists as an application that starts up as soon as the device is turned on and continues to run in the background. Its presence will steal random access memory and processor power and could generate infinite pop-up ads, effectively slowing down the web browser until it becomes unusable.

Spyware may also reset the browser's homepage to open to an ad every time or redirect web searches and control the provided results, making the search engine useless. Additionally, spyware can change the computer's [dynamic link libraries](https://searchwindowsserver.techtarget.com/definition/dynamic-link-library-DLL), which are used to connect to the internet, resulting in connectivity failures that can be hard to diagnose.

At its most damaging, spyware will track web browsing history, passwords and other private information, such as email addresses, credit card numbers, personal identification numbers or banking records. All of this information can be gathered and used for [identity theft](https://searchsecurity.techtarget.com/definition/identity-theft) or sold to third parties. Information can be collected using keyloggers and screen captures.

Spyware can also secretly make changes to a device's [firewall](https://searchsecurity.techtarget.com/definition/firewall) settings, reconfiguring the security settings to allow in even more malware. Some forms of spyware can even identify when the device is trying to remove it from the Windows registry and will intercept all attempts to do so.

**TEXT**

**HOW DO SPYWARE INFECTIONS OCCUR?**



Spyware infections can affect any personal computer, Mac, iOS or Android device. Some of the most common ways for computers to become infected include the following:

* pirating media such as games, videos and music by downloading and distributing copyrighted digital content without permission;
* downloading materials from unknown sources;
* accepting pop-up advertisements; and
* opening email attachments from unknown senders.

Spyware is most commonly distributed by getting potential victims to click on a link. The link can be in an email, pop-up window or ad. Malicious code can also be embedded on legitimate websites as an advertisement. Other ways for spyware to infect a machine include via drive-by download -- where spyware is downloaded just by visiting a website or viewing a HyperText Markup Language email message -- phishing links or physical devices.

**TEXT**

**TYPES OF SPYWARE**



Spyware is not just one type of program. It is an entire category of malware that includes adware, keyboard loggers, Trojans and mobile information-stealing programs.

**Adware.** Malicious [adware](https://searchsecurity.techtarget.com/definition/adware) is often bundled with free software, shareware programs and utilities downloaded from the internet or surreptitiously installed onto a user's device when the user visits an infected website. Many internet users were first introduced to spyware in 1999 when a popular freeware game called *Elf Bowling* came bundled with tracking software. Adware is often flagged by [antimalware programs](https://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques) as to whether the program in question is malicious or not.

[Cookies](https://searchsoftwarequality.techtarget.com/definition/cookie) that track and record users' personally identifiable information (PII) and internet browsing habits are one of the most common types of adware. An advertiser might use tracking cookies to track what webpages a user visits in order to target advertising in a contextual marketing campaign. For example, an advertiser could track a user's browser history and downloads with the intent to display pop-up or banner advertisements to lure the user into making a purchase. Because data collected by spyware is often sold to third parties, regulations such as the [General Data Protection Regulation](https://whatis.techtarget.com/definition/General-Data-Protection-Regulation-GDPR) have been enacted to protect the PII of website visitors.

**Keyboard loggers.** [Keyloggers](https://searchsecurity.techtarget.com/definition/keylogger) are a type of system monitor that cybercriminals often use to steal PII, login credentials and sensitive enterprise data. Employers may also use keyloggers to observe employees' computer activities; parents to supervise their children's internet usage; device owners to track possible unauthorized activity on their devices; or law enforcement agencies to analyze incidents involving computer use.

Hardware keyloggers resemble a Universal Serial Bus flash drive and serve as a physical connector between the computer keyboard and the computer, while software keylogging programs do not require physical access to the user's computer for installation. Software keyloggers can be downloaded on purpose by someone who wants to monitor activity on a particular computer, or they can be downloaded unwittingly and executed as part of a [rootkit](https://searchsecurity.techtarget.com/definition/rootkit) or remote access Trojan.

**Trojans.** Trojans are typically malware programs that are disguised as legitimate software. A victim of a Trojan could unknowingly install a file posing as an official program, enabling the Trojan to access the computer. The Trojan can then delete files, encrypt files for ransom or enable other malicious actors to have access to the user's information.

**Mobile spyware.** Mobile spyware is dangerous because it can be transferred through Short Message Service or Multimedia Messaging Service text messages and typically does not require user interaction to execute commands. When a smartphone or tablet gets infected with mobile spyware that is sideloaded with a third-party app, the phone's camera and microphone can be used to spy on nearby activity, record phone calls, and log browsing activity and keystrokes. The device owner's location can also be monitored through the Global Positioning System (GPS) or the mobile computing device's [accelerometer](https://whatis.techtarget.com/definition/accelerometer).

**TEXT**

**HOW DO YOU PREVENT SPYWARE?**



Maintaining strict cybersecurity practices is the best way to prevent spyware. Some best practices include the following:

* only downloading software from trusted sources;
* reading all disclosures when installing software;
* avoiding interactions with pop-up ads;
* staying current with updates and patches for browser, operating system (OS) and application software;
* not opening email attachments or clicking on links from unknown senders;
* using only trusted antivirus software and reputable spyware tools; and
* enabling two-factor authentication ([2FA](https://searchsecurity.techtarget.com/definition/two-factor-authentication)) whenever possible.

To further reduce the probability of infection, network administrators should practice the [principle of least privilege](https://searchsecurity.techtarget.com/definition/principle-of-least-privilege-POLP) and require remote workers to access network resources over a virtual private network that runs a security scan before granting access privileges.

Using a pop-up blocker or ad blocker also helps avoid spyware. Mozilla Firefox and Google Chrome have built-in pop-up blockers, and ad blockers can be added as a browser extension.

Mobile users should avoid downloading applications from outside their respective app stores and avoid jailbreaking their phones, if possible. Since both make it easier for spyware to infect mobile devices.

IPhone users can enable 2FA at no charge to protect all the data on their smartphones and prevent mobile spyware attacks. 2FA can also be used in a variety of other common services, including PayPal, Google, Dropbox and Microsoft 365, as well as in social networking sites, such as Instagram, Snapchat, Facebook and Twitter. Most major banks have also started implementing 2FA in their websites and mobile apps. Some services have even increased their authentication process to three-factor and [four-factor authentication](https://searchsecurity.techtarget.com/definition/four-factor-authentication-4FA).

**TEXT**

**HOW DO YOU REMOVE SPYWARE?**



In order to remove spyware, device owners must first identify that the spyware exists in their system. There are several symptoms to look for that can signify the presence of an attack. Indicators include the following:

* The device runs slower than normal.
* The device consistently crashes.
* Pop-up ads appear whether the user is online or offline.
* The device starts running out of hard drive (HD) space.

If users determine that spyware has infected the system, they should perform the following steps:

1. Disconnect the internet connection.
2. Check the device's programs list to see if the unwanted software is listed. If it is, choose to remove it from the device. After uninstalling the program, reboot the entire system.
3. If the above step does not work, run a scan of the system using a reputable antivirus software. The scan should find suspicious programs and ask the user to either clean, quarantine or delete the software.
4. The user can also download a virus removal tool or antispyware tool and allow it to run through the system.

If none of the above steps work, then the user will have to access the device's HD in [safe mode](https://whatis.techtarget.com/definition/safe-mode). However, this requires a tool that enables the user to access the spyware folders and manually delete them. While this sounds complicated, the process should only take a few minutes.

Spyware on mobile devices can also be scanned for using security programs. Mobile device owners can also back their data up and then reset the device to its factory settings.

**TEXT**

**ANTISPYWARE TOOLS**



Some antispyware tools only perform when the scan is manually started, while others are continuously running and monitoring computer activity to ensure spyware cannot record the user's information. Users should be cautious when downloading antispyware tools and only download tools from reputable sites. Product reviews can also help users determine which tools are safest.

Some antispyware tools include the following:

* **Malwarebytes** is an antimalware and spyware tool that can remove spyware from Windows, macOS, Chrome OS, Android and iOS. [Malwarebytes](https://searchsecurity.techtarget.com/definition/Malwarebytes-software) can scan through registry files, running programs, HDs and individual files. Once a spyware program is detected, a user can quarantine and delete it. However, users cannot set up automatic scanning schedules.
* **Trend Micro HouseCall** is another antispyware tool that does not require user installation, so it uses minimal processor and memory resources and disk space. However, like Malwarebytes, users cannot set automatic scans.
* **Windows Defender** is a Microsoft antimalware product that is included in the Windows 10 OS under Windows Defender Security Center. The software is a lightweight antimalware tool that protects against threats such as spyware, adware and viruses. Windows Defender includes features such as protection against phishing sites, real-time threat detection and parental controls. Windows Defender users can set automatic quick and full scans, as well as set alerts for low, medium, high and severe priority items.

**TEXT**

**WHAT ARE COMMON EXAMPLES OF SPYWARE?**

Well-known examples of spyware include the following:

* **CoolWebSearch**uses security vulnerabilities found in Internet Explorer to take control, change settings and send browsing information to spyware authors.
* **DarkHotel** is a targeted [spear phishing](https://searchsecurity.techtarget.com/definition/spear-phishing) spyware that selectively attacks business hotel visitors through the hotel's Wi-Fi network.
* **Emotet** was one of the most prevalent threats in the 2010s. It acted as a Trojan that stole banking credentials from its victims.
* **Gator**is commonly found in file sharing software. It monitors a victim's web browsing habits to present the user with better-targeted ads.
* **TIBS Dialer** disconnects the user's computer from local phone lines and connects it to a toll number designed for accessing pornographic websites.
* **Zlob** downloads itself onto a computer to record keystrokes and search a user's browsing history.

In addition, smartphone spy apps enable different people to track the phone user's activity. While most of these tools were created with the intent of letting parents monitor their child's phone use, their abilities have been grossly abused. These apps act as mobile spyware and enable external users to access the phone's microphone and camera to view their surroundings, listen in on phone calls and access the phone's GPS location, passwords and mobile apps. Some well-known spy apps include Spyera, FlexiSPY and TheOneSpy.