SPYWARE

Spyware is a type of malicious software ([malware](https://www.techtarget.com/searchsecurity/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](https://www.techtarget.com/searchsecurity/tip/10-common-types-of-malware-attacks-and-how-to-prevent-them). 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](https://www.techtarget.com/searchsecurity/definition/cyberstalking). 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](https://www.techtarget.com/whatis/definition/anti-spyware-software) 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.

Modern spyware also targets businesses, aiming to access proprietary information, trade secrets and employee credentials, making it a significant corporate security threat.

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.

At its most damaging, spyware tracks web browsing history, passwords and other private information, such as email addresses, credit card numbers, personal identification numbers or banking records. All this information can be gathered and used for identity theft or sold to third parties. Information can be collected using keyloggers and screen captures.

Advanced spyware often employs techniques such as encrypting stolen data before transmission, obfuscating its presence to avoid detection by antivirus software and modifying system files to disable security programs.

How do spyware infections occur?

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

Downloading materials from unknown sources.

Accepting pop-up advertisements.

Opening email attachments from unknown senders.

Clicking on phishing links embedded in emails or ads.

Using outdated software, which often contains vulnerabilities that spyware exploits.

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 an HTML email message -- phishing links or physical devices.

Even legitimate websites can become a threat if compromised by hackers who insert malicious scripts into ads or downloadable content.