Spyware and Stalkerware:
Computer Surveillance & Safety for Survivors

What is Spyware and Stalkerware?

Spyware and stalkerware refer to tools - apps, software programs, and devices - that let an unauthorized person (such as an abuser) secretly monitor and record information about your computer. The term "stalkerware" is a more recent term that draws attention to the invasive, intrusive, and dangerous misuse of these tools.

Spyware can keep track of almost everything you do on your computer, including every keystroke typed, website visited, online chat or instant message sent or received, and documents opened. Some spyware can also allow the person who installed it to turn on the webcam or microphone, take screenshots, make the computer talk or make other noises, or shut down or restart the computer. The abusive person can view your computer activities or control your computer remotely, generally via a website dashboard or accompanying app.

Most computer spyware can be installed remotely, usually by sending an email or message with an attached file or link. The spyware automatically installs when you click on the link or open the attachment. Some spyware products can be sent through an instant message, computer game, or other ploys to entice you or your children to open the attachment or click on a link. Once installed, it runs in stealth mode without any notification or identifying activity and is difficult to detect or remove.

While most spyware is installed as software, there are also hardware-based spyware devices called keystroke loggers. These keylogging devices may appear to be a normal computer part; for example, it can be a special keyboard with keystroke logging capabilities or a small device that connects the keyboard to the computer. Once the keylogger is plugged into the computer, it records every key typed, which can include passwords, personal identification numbers (PIN), and websites visited. Some hardware devices allow for remote spying while others

require the abuser to have access to the hardware to access information on the computer activity.

How Do I Find Out if Spyware Is on My Computer?

Detecting spyware on your computer can be very difficult. In most cases, a computer with spyware installed will not have noticeable changes in the way it operates (i.e., your computer won't necessarily slow down or freeze up). Even without these things happening, however, you might suspect that your activity is being monitored because of the abuser's suspicious behavior. Trust your instincts and look for patterns. If the abusive person knows too much about your computer activity or knows things that you've only done on your computer or phone, it's possible that spyware may be on your device.

If a hardware device has been installed, you might see an additional component between the computer and the keyboard cord, or you might suddenly have a new keyboard or mouse. On laptops, a hardware device may not be as noticeable since it would be installed inside the laptop, through the access panel.

Responding to Spyware

Safety first. Before acting to find or remove spyware, it is important to consider safety and the possibility of collecting evidence. Since many abusers use spyware as a way to monitor and control survivors, they may escalate their harassing and abusive behavior if they suspect that the survivor is removing the spyware and cutting off their access. Before removing the spyware, think through your safety as you consider ways to protect yourself, and talk with an advocate about safety planning. If you need an advocate, please reach out to the National Domestic Violence Hotline.

Gather evidence. Law enforcement or a computer forensics expert may be able to assist you if you want to preserve evidence needed for a criminal investigation or civil legal action. Forensic tools may be the only way to determine for sure if spyware is on a computer. Read more about Spyware Evidence.

Remove spyware. Spyware on a computer can be very difficult to remove once it's installed. You can consider wiping the computer and rebuilding the computer starting with reinstalling the operating system, although this will not guarantee complete removal. Another option is to replace the hard drive of the computer or get a new computer. Be careful not to copy files or documents from the infected computer onto the new computer, which could reinstall spyware hidden in the files. Use online cloud services to store documents from the infected computer.

Use devices that aren't being monitored. If you suspect that spyware is on your device, remember that all activity, including online chat, emails, and web searches, can be revealed to the abuser. If you can, use a safer computer or device – one the person has not had physical or remote access to –when you look for help or information. This may be a computer at a public library, community center, or a friend's device.

Update accounts. Since spyware would have given the abusive person access to your login information, consider resetting your passwords on a different device and no longer accessing certain accounts from the computer you are concerned is being monitored. Also consider changing passwords to sensitive accounts such as online banks, social media accounts, etc. Read more about Password Safety.

Preventing Spyware

Consider access. Be suspicious if someone abusive wants to install a new keyboard, cord, or software or updates or "fixes" the computer or phone — particularly if this coincides with increased monitoring or stalking. Beware of gifts from an abuser to you or your children, such as new phones, computers, keyboards, or games.

Create separate user or guest accounts. You can create guest accounts or a user account that have settings that do not allow software or apps to be installed without the administrator's login. This can prevent accidentally installing spyware or other malware if you or someone else using your computer clicks a link or opens a file.

Use anti-virus and anti-spyware protection. Install anti-virus and anti-spyware programs, make sure it is up-to-date and set it to scan your computer regularly. These programs can help prevent spyware from being installed, but they work best before your computer has been compromised. In addition, before browsing online or clicking on links, run your anti-virus/anti-spyware software for further protection. (Note that these programs will only protect you from spyware software or programs but not hardware devices, such as a keystroke logging keyboard or device.)

Not Spyware?

There are many other methods someone can access information on your computer without installing spyware. If the abusive person has physical access to the computer, they may not need to install spyware, which is mostly for remote monitoring.

Abusive individuals may also be logging into accounts such as email or social media to learn about what you are doing. These accounts can be accessed from another device if the abusive person knows the username or email and password.

Sometimes, the explanation for an abusive person knowing too much about what you're doing could be as simple as friends or family members sharing information about you. Looking for patterns of what the person knows, and where that information might have come from, can help you to narrow down the possibilities. An advocate can help you figure out what may be happening, and plan next steps.