Who's Spying on Your Computer?
Spyware, Surveillance, and Safety for Survivors

SAFETY ALERT: Spyware has made it easier than ever before for perpetrators to stalk, track, monitor, and harass their victims. Abusers, stalkers, and other perpetrators can now use spyware to secretly monitor what you do on your computer or handheld device, like a cell phone. If you suspect you are being stalked or monitored, be aware that:

- Attempting to look for spyware on your computer or cellphone could be dangerous since the abuser could be alerted to your searches immediately.
- Use a safer computer (one that the stalker does not have remote or physical access) to perform Internet searches or send emails that you wouldn't want an abuser to intercept.

WHAT IS SPYWARE?

Spyware is a computer software program or hardware device that enables an unauthorized person (such as an abuser) to secretly monitor and gather information about your computer use.

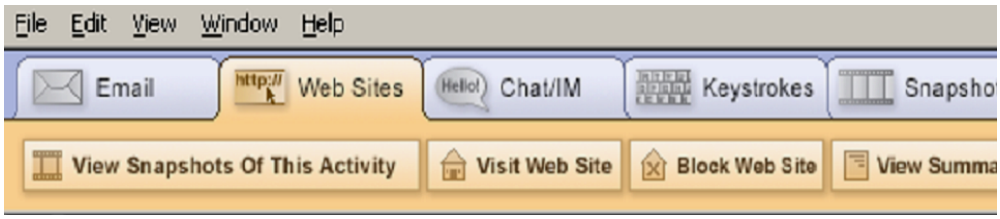
There are many types of computer software programs and hardware devices that can be installed to monitor your computer activities. They can be installed on your computer without your knowledge, and the person installing them doesn't even need to have physical access to your computer. Spyware is invasive, intrusive, and may put victims in grave danger.

HOW DOES SPYWARE WORK?

Spyware can keep track of every keystroke you type, every software application you use, every website you visit, every chat or instant message you send, every document you open, and everything you print. Some spyware software gives the person monitoring the ability to freeze, shutdown or restart your computer. Some versions even allow the abuser to remotely turn on your webcam or make your computer talk.

Once spyware is installed, it can run in stealth mode and is difficult to detect or uninstall. If the person who installed it has physical access to your computer, he or she can log into the computer with a special password to see all of the computer activity (emails sent, documents printed, websites visited, and more) since their last log in. Perpetrators without physical access to your computer can receive reports showing all of your computer activities, including copies of emails and instant messages sent, websites visited, etc., as well as screenshots of the computer screen every few seconds. This can all occur without the user knowing.

Below are the computer activities that can be easily monitored:



HOW DOES SPYWARE GET ON MY COMPUTER?

Abusers can install spyware on your computer if they have physical or Internet access to your computer. Some abusers might hack into your computer from another location via the Internet. Some might send spyware to you as an attached file that automatically installs itself when you open the email. Others may email or instant message a greeting card, computer game, or other ploy to entice you or your children to open an attachment or click on a link. Once opened, the program automatically installs spyware on the victim's computer, in stealth mode without notification or consent, and can then send electronic reports to the perpetrator via the Internet.

While most spyware is software based (a program that can be installed on your computer), there are also some 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 your keyboard to the computer. Once the keylogger is

plugged into your computer, it can record every key typed, capturing all passwords, personal identification numbers (PIN), websites visited, and any emails sent.

HOW DO I FIND OUT IF SPYWARE IS ON MY COMPUTER?

Even if a computer is being monitored by spyware, there may not be noticeable changes in the way your computer operates (i.e., your computer won't necessarily slow down or freeze up). You might suspect that your computer is being monitored by the abuser's suspicious behavior: for example, he or she knows too much about your computer activities. If you suspect that someone has installed spyware to monitor your activities, talk to a victim advocate before attempting to remove the spyware. Law enforcement or a computer forensics expert may be able to assist you if you want to preserve evidence that may be needed for a criminal investigation.

Unfortunately, detecting spyware on your computer may be difficult. If a hardware device has been installed, you might see an additional component between the computer and the keyboard cord, or it might be the keyboard or mouse itself. In laptops, hardware device would be installed inside the laptop, through the access panel. Hardware spyware cannot be detected by anti-spyware software.

Software spyware typically runs in stealth mode using disguised file names that look legitimate. Sometimes, running anti-spyware software may detect this type of spyware but not all of it.

TIPS FOR SURVIVORS

Trust your instincts and look for patterns. If your abuser knows too much about things you've only told people via email or instant messenger or things you've done on your computer, there may be spyware on your computer.

Everything is being recorded. If you suspect your computer is being monitored, remember that all that you do, including research on spyware and computer

monitoring, will be revealed to the abuser. Strategize around the safety concerns that may arise if the abuser thinks that you know and are attempting to remove their control. If you can, use a safer computer when you look for domestic or sexual violence resources. It may be safer to use a computer at a public library, community center, or internet café. Clearing or deleting your internet browsing history or deleting documents from your computer will not prevent the spyware from capturing what you're doing. The spyware will actually record everything you do, including attempts to clear your browsing history.

Create new accounts & change passwords. If you suspect that anyone abusive can access your email or Instant Messaging (IM), consider creating additional email/IM accounts on a safer computer. Do not create or check new email/IM accounts from a computer that might be monitored. Look for free web-based email accounts, and consider using non-identifying name and account information. (Example: bluecat@email.com and not YourRealName@email.com.) Also consider changing passwords to sensitive accounts such as online banks, social media accounts, etc. from a safer computer.

New software or hardware? Be suspicious if someone abusive has installed a new keyboard, cord, or software or updated or "fixed" the computer—particularly if this coincides with increased monitoring or stalking. Beware of gifts from the abuser to you or your children, such as new keyboards, cell phones, or games for the computer as it may contain spyware.

Preventive measures you can take: There are steps you can take to reduce the chance of spyware. Note that these suggestions will help prevent spyware from being installed and work best before your computer has been compromised.

- Install and enable a firewall. There are both software and hardware firewalls. If a firewall didn't come with your computer, you can download a software one for free from www.zonealarm.com.
- Have a anti-virus protection program installed. Make sure your anti-virus definitions are up-to-date because new dangerous viruses are released daily and that it scans your computer regularly. This may involve setting

your computer to automatically update its virus definitions and run anti-virus scans daily. When your anti-virus software subscription ends, make sure to renew it.

- Install anti-spyware programs and make sure the spyware definitions are updated automatically and regularly.
- These programs will only protect you from spyware software or programs but not hardware devices, such as a keystroke logging keyboard or device.

Buy a new computer. It is almost impossible to completely delete, erase or uninstall spyware from your computer. The safest way to ensure that your computer is no longer being monitored is to purchase a new computer. Be careful about moving files (including software, documents, pictures, videos) from the infected computer to the clean computer as the spyware may reinstall onto the new computer.

Include the children and other family members. It is important for you and your children to be educated about spyware and to make sure that the kids don't inadvertently install spyware onto the computer. Talk to your children about opening emails from people they don't know or from opening attachments from the abusive person. An innocuous picture or video may be something that the child wants to see but can also contain spyware. Instead of sharing files and media via email between the abuser and you and the children, consider creating online spaces to share pictures, videos and documents. Some online spaces will allow you to create private spaces, so no one else can access it but authorized users.

Safety when removing spyware. Many abusers use spyware as a way to monitor and control survivors. Some abusers may escalate their control and monitoring if they suspect that the survivor is cutting off their access. Think through your safety as you consider ways to protect yourself.

Additional resource. For more information on avoiding and removing spyware from your computer, please see the document Protecting Your Computer.

Spyware for Smartphones & Cell Phones

Spyware programs are now available for cell phones and other mobile devices so perpetrators can track phone activities, including calls and texts that are sent or received, record conversations, and can even be used as a listening device. The abuser will need to have physical access to the phone to manually install the software onto the phone. If you suspect that your cell phone is being monitored, keep an eye on excessive battery or data usage and suspicious patterns of behavior from the abusive person. You can take steps to protect your phone by putting a passcode on your phone and running an anti-spyware/anti-malware app on your phone if your phone has that capability. *(Don't forget that some phone activities can be monitored without spyware. Phone records can be obtained by guessing your account password and accessing your account online or by viewing your call history stored in the phone.)*

Supported by US DOJ-OVC Grant# 2011-VF-GX-K016. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of DOJ.

We update out materials frequently. Please visit TechSafety.org for the latest version of this and other materials.