Who's Spying on Your Computer?

Spyware, Surveillance, and Safety for Survivors

SAFETY ALERT: While stalking is an age-old crime, 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 handheld/phone could be dangerous since the abuser could be alerted to your searches immediately
- Use a safer computer or handheld device (one that the stalker does not have remote or physical access to) to perform Internet searches or send emails that you wouldn't want an abuser to intercept
- If you want to preserve evidence of Spyware on your computer, contact your local police, a domestic violence hotline, a trained victim advocate, or Safety Net to learn what to do.

Simply type "spy on girlfriend" into any search engine, and instantly see listings and links advertising easy-to-install computer Spyware programs and devices that can be used to "spy on a lover, girlfriend, boyfriend, partner, husband or wife and secretly record computer activities to catch a cheating spouse."

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. Whether computer monitoring is legal or illegal depends on the state you live in, and the context in which it is installed and used. Regardless of the legality, Spyware is invasive, intrusive, and may put victims in grave danger.

Spyware programs are sometimes marketed as ways to monitor your children or your employees. As an employer, it is always best to have your employees read and sign a "Technology Use Policy." This policy should explain allowable uses of company property, expectations of online behavior, and TELL employees if their computer will be monitored. Additionally, choose a software package that displays an icon to remind your employees that they're being monitored. (* Also - see note to parents at the end of this piece).

There are some similarities and differences between Spyware and its close relatives.. For example:

- **Adware**: These are hidden marketing programs that deliver advertising to consumers, and might also profile users' Internet surfing & shopping habits. Adware is often bundled or hidden in something else a user downloads. Most average computer users are infected with adware fairly regularly, and common symptoms include a sluggish system and lots of advertising pop-ups.
- **Malware**: This is any program that tries to install itself or damage a computer system without the owner's consent. Malware includes viruses, worms, spyware and adware.

For more information on adware and malware, see "Protecting Your Computer" at
http://www.antispywarecoalition.org/documents/documents/ProtectingYourComputerflyerletter.pdf

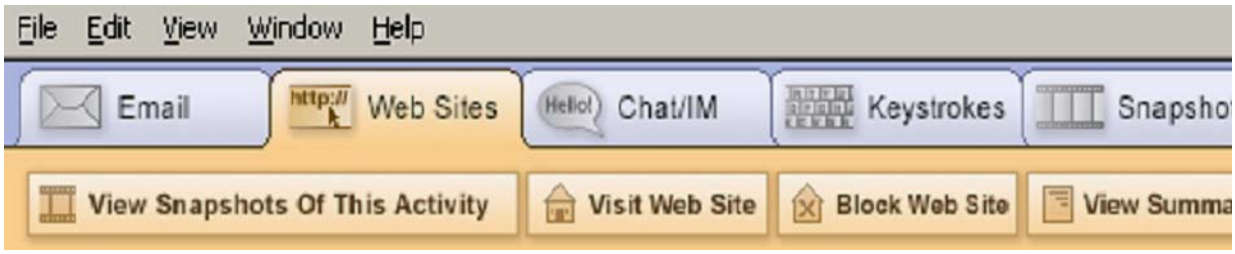
Web: nnedv.org/safetynet • Email: safetynet [at] nnedv.org • Phone: 202-543-5566

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 gives the abuser 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 use a special key combination that will cause a log-in screen to pop-up. After entering the password, an options screen will pop up that allows the installer to view all of the computer activity since their last login, including emails you sent, documents printed, websites visited, and more. Perpetrators without physical access to your computer can set the spyware to take pictures of the computer screen (screen shots) every few seconds and have these pictures sent to them over the Internet without a victim's knowledge.

One example of the types of computer activity that can be easily monitored:



How does it get on my computer?

Abusers can install Spyware on your computer if they have physical or Internet access to your computer or handheld device. 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 or when you initially view it in a preview window. Others may email or instant message a greeting card, computer game, or other ruse in order 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 tiny keylogging devices may appear to be a normal computer part. However, 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 onto its small hard drive. Additionally, there are keyboards with keystroke logging capabilities built-in.

Note: Remember that many handheld devices are mini-computers. There are now spyware programs available for cell phones and other handheld devices, so that the perpetrator can track every text message sent and every phone number dialed. *(note: phone records can also be obtained by non-spyware methods, such as guessing your account password and accessing your account on the phone company website, or by viewing your call history stored in the phone.)*

How do I find out if there's spyware on my computer?

- If your computer is currently being monitored it may be dangerous to try to research spyware or use anti-spyware scanners. If your computer is compromised, spyware will log all of this research activity and alert the perpetrator.
- 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.

Spyware typically runs in stealth mode using disguised file names so it can be extraordinarily difficult to detect spyware programs that are already on your computer.

While your computer is being monitored by Spyware there might be no noticeable changes in the way your computer operates (i.e. your computer won't necessarily slow down or freeze up). Also, like computer viruses, there are hundreds of Spyware programs. So while some are created by large software companies, other spyware programs are written by individual "hackers".

There are a variety of programs marketed as Anti-Spyware detectors that primarily identify Adware and Malware, but may not discover surveillance Spyware. Additionally, anti-spyware detection programs typically does not detect hardware, like keystroke loggers.

If you think there may be spyware on your computer, consider the tips below:

TIPS FOR SURVIVORS OF ABUSE

- If you use the monitored computer to try to research spyware or try to access anti-spyware scanners, spyware will log all of this activity and alert the perpetrator which could be dangerous.
- Try to 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.
- 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 strongly consider using non-identifying name & account information. (example: bluecat@email.com and not YourRealName@email.com) Also, make sure to carefully read the registration screens so you can choose not to be listed in any online directories.
- Be suspicious if someone abusive has installed a new keyboard, cord, or software, or recently or done computer repair work that coincides with an increase of stalking or monitoring.
- If you are thinking about buying a new computer, there are steps you can take to reduce the chance of spyware getting on your new machine but it is impossible to eliminate the risk.
    - 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 at least one anti-virus protection program installed and actively scanning your computer, and make sure your anti-virus definitions are up-to-date because new dangerous viruses are released daily. This may involve setting your computer to automatically updates its virus definitions and run anti-virus scans daily and making sure to renew your anti-virus software subscription every year.
    - Install anti-spyware programs before you even connect to the Internet and make sure their spyware definitions are updated automatically and regularly.
- 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, there may be spyware on your computer. If you think you're being monitored by an abuser, you probably are.

Can't I just "clear" and "delete" my history or trail?

- It is not possible to clear the traces on the computer, especially since Spyware will record all of your attempts to clear your many computer histories. There are literally hundreds of histories hidden in the computer. Also, an abuser may become suspicious and escalate control if he/she has been monitoring your computer history and activities for a while and then one day sees empty histories.
- Spyware records everything you do on the computer or device, and then records all your attempts to delete your computer activities. Sometimes, Spyware is impossible to detect without a forensic examination of your hard drive or unless you know the password and keycode your abuser uses to view screenshots of your computer activities.
- Attempting to clear your histories, trying to find whether Spyware is installed on your computer, or reaching out for help through a domestic violence webpage could be dangerous on a computer that your stalker or abuser is monitoring.

Web: nnedv.org/safetynet • Email: safetynet [at] nnedv.org • Phone: 202-543-5566

TIPS FOR ORGANIZATIONS THAT ASSIST VICTIMS

Post a Safety Alert on every page of your Website

- Posting a clear, but brief safety alert can make victims aware of risks. (Example: "Your computer activities might be impossible to erase. If someone might be monitoring you, please use a safer computer or call a hotline for more information.)

Take steps to increase your organization's data security.

- Organizations should protect any personally identifiable information collected about a victim since any data leaks or breaches could be fatal. For safety reasons, we recommend that organizations not store confidential or personally-identifiable information about a victim on any computer that is connected to the Internet. Without an internet connection, there is significantly less risk that an abuser will hack in and access your organization's data, or, that a virus will infect your computer and automatically emailing confidential files out to others.
- It is important to have organizational policies that address electronic and paper information practices including who can or can't access certain data, and the secure disposal of confidential papers, computer hard drives, and other electronic media (i.e. external or USB hard drives) that contain victim data. For a data security checklist see: http://nnedv.org/SafetyNetDocs

Carefully consider computer safety issues before contemplating providing services via the Internet

- Know the facts! 60-80% of computers are infected with viruses, adware, or other malware which can compromise the safety of both the victim/survivor and your agency's computers. (www.pewinternet.org)
- Know that you cannot guarantee the safety and/or security of the computer of every person who uses your services. Provide upfront and complete disclosures to service users about safety, confidentiality and capacity issues so they can make realistic and informed choices about use.
- Provide information about the technology, confidentiality and security limits of online service provision, including disparities in access to technology varied internet speeds and internet connection outages.
- Discuss in your organization the potential harm that could come to victims if an abuser is monitoring a victim's entire escape plan that the victim shares through online service provision.

Use Firewalls and keep Anti-Virus & Anti-Spyware Definitions Updated

- As always, updated protection software is the first line of defense against Malware and Adware. However, these programs offer limited protections against surveillance spyware, since monitoring software can appear to be a legitimate product and might not be flagged by these programs. Regardless of the precautions a user takes, spyware allows an abuser to monitor computer and Internet activities and discover a victim's efforts to escape or access help.

Secure your Computers

- Make sure all of your agency's computers require strong alphanumeric passwords to log in. Each user should have a different password, and they should not use the name of your organization, your address, or any similar information.
- If you have computers that are for public use, consider setting them so that users cannot download software.

TIPS FOR PARENTS

- After educating yourself about the Internet and computers, have a conversation with your children about the Internet and its benefits and risks. Together, come up with a set of Internet safety rules for your family. If your children take part in creating the rules, they will be more likely to follow them.
- Keep the family computer in a public space like the family room or living room. If your children know that you could walk past at any moment, they're much less likely to break your agreed upon rules.
- If you choose to use Parental Monitoring Software: TELL your child that you will be using it and explain why. Building trust and respect around computer use is extremely important, so that your children will feel comfortable coming to you if an issue or problem does arise. Also look for one that displays an icon somewhere on the screen while in use. The icon will help children remember that they're being watched and encourage them to follow your Internet safety rules.

Web: nnedv.org/safetynet • Email: safetynet [at] nnedv.org • Phone: 202-543-5566