Spyware: Computer & Phone Monitoring Software

Description/Risks

- It enables a person to secretly monitor someone else's entire computer activity.
- It can be installed remotely by sending an email, photo, or instant message.
- It runs hidden on a computer. It is very difficult to detect and almost impossible to remove. Some secretly reinstall if removed.
- It can record and send screenshots (pictures of what's on the screen), all keystrokes typed, web sites visited, emails sent, instant messages (IM), accounts accessed, passwords typed, and more.

Safety Strategies

- When you first get a new computer or phone, increase security by enabling firewalls for your computer, network or phone (see settings) and install or run anti-spyware and anti-virus software; set your computer or device to automatically install updates.
- Don't open any attachments if you don't know the sender, or you suspect abuse. Instead delete the attachment or have IT staff look at it.
- Trust your instincts. If someone knows too much about your computer activity, your computer may be monitored. Use a "safer" computer (one the abuser does not have any access to) for private communications and web browsing.
- Consider changing passwords and creating new accounts on another computer. Do not access those accounts or use those passwords on the monitored computer.

Keystroke Logging Hardware

Description/Risks

- It provides a record of all keystrokes typed on a keyboard.

- Someone needs physical access to the computer to install and later retrieve the device with the data log of all your keystrokes.
- An abuser may use it to see the passwords you type and then be able to access your email, credit card, or bank accounts, etc.

Safety Strategies

- Has someone fiddled with, fixed, or given you a new part for your computer?
- Look for a small piece that connects the keyboard cord to the computer; it can also be part of an external keyboard, or something installed inside a laptop.
- Change passwords on accounts from another computer and do not access those accounts from the compromised computer. With some services, you can ask to get an alert (e.g. fraud alert) if your password gets changed or your account gets changed.

Global Positioning System (GPS) Devices

Description/Risks

- They are small, easily hidden, and affordable devices that provide the ability to monitor someone's location.
- Many cell phones also have GPS devices.
- They might be used to track your location real-time (as you move) and to map your location history.
- Depending upon the service or application used to access GPS data, the stalker may be able to secretly monitor your location via websites or sometimes via their phone. Some devices must be physically retrieved for the abuser to review your location data.

Safety Strategies

- Trust your instincts. If someone seems to know too much or show up in random places, check for hidden GPS devices or other location tracking services. Consider notifying law enforcement.

- A device can be hidden in your belongings or vehicle. Check the trunk, under the hood, inside the bumper and seats. A mechanic or law enforcement can also do a search.
- Safety plan around/before removal of any location tracking device, as it may alert the abuser.

Mobile Phones

Description/Risks

- Phones can be a lifeline for victims.
- Phones can be hidden inside vehicles as listening devices by using the "silent mode" and "auto answer" features.
- Most phones have GPS chips and location tracking abilities, which can be used to determine someone's location. Some abusers install additional applications on a cell phone to track your application.
- Logs showing phone usage may be monitored on the actual phone or over the Internet via the phone company's online billing record.
- Joint phone plans with an abuser may give that person access to phone features and calling log information.
- If your phone has a Bluetooth device, the stalker might try to connect with your phone using the Bluetooth to access information on your phone or intercept your communications.

Safety Strategies

- For additional privacy and safety, consider getting a separate donated phone from a shelter or purchasing a new phone (e.g. a pay-as-you-go phone).
- Mechanics or law enforcement can check the vehicle to determine if a phone has been hidden somewhere.
- Contact carrier to add a password or code to account to protect from wrongful access.
- You can change the phone's location setting to "E911 only" or "911 only" so that the phone company only access your GPS if you dial 911.

- Also check if your phone has any applications installed that separately ask to access and use your real-time location, such as for mapping directions. Settings such as “show all/hidden applications” might unveil some hidden applications. Consider turning off or uninstalling these applications.
- Use phone settings to change your default Bluetooth password, set Bluetooth to hidden, and turn Bluetooth off.
- Always give location information to 911 in an emergency.

Caller ID & Spoofing

Description/Risks

- Reverse directories can provide location based on a phone number.
- Services like Trapcall, can unblock a blocked number without notice.
- Caller ID can be spoofed to falsify the number displayed when you get a call.
- If you call a person using an Internet phone, your blocked number may be displayed.

Safety Strategies

- Survivors can contact the phone company and ask that their phone number be blocked to protect privacy. Blocking is supposed to prevent your caller ID from displaying. However, even with a blocked number, sometimes your caller ID will still display. Consider using another phone or outgoing phone number.
- Regularly test the line by calling other phones to ensure it is blocked.
- Use an Internet phone (i.e., Skype) or a pay-as-you-go phone purchased with cash to make calls if you are worried about your number / location being revealed.

Faxes

Description/Risks

- Fax headers include sender’s fax number, which can be used to determine location thru reverse look-up.

- Fax machines often now have hard drives and extensive memory. Consider privacy, confidentiality and privilege issues when deciding what fax machine to use.
- Electronic faxes (e-fax) are sent through the Internet as email attachments and, like all email, can be intercepted.
- Also, because e-faxes get sent via a 3rd party and are temporarily stored on a 3rd party Internet server, there are different confidentiality and security risks.

Safety Strategies

- Cover sheet can request that the header be removed before forwarding.
- If it's legal, consider changing the outgoing fax number displayed to a different number on a case by case basis for safety or privacy reasons.
- Never send personally identifying or sensitive information in an E-Fax.
- Make sure you know who is receiving the fax. Call ahead. Some fax machines require the receiver to type in a password to see the fax.

Cordless Phones

Description/Risks

- Because cordless phones transmit your conversation wirelessly between the base unit and phones, they can more easily be intercepted by scanners, baby monitors, & other cordless phones.
- If you do not unplug the base unit, the phone may continue to broadcast for the duration of a call, even after you switch to a corded phone, allowing for the possibility of continued interception.

Safety Strategies

- Switch to a corded phone before exchanging sensitive information.
- Unplug a cordless phone from the power source, even after the corded phone has been turned off or hung up to ensure that the current call's conversation won't still be broadcast and overheard.

- Best practice is to limit information discussed or not use cordless phones for confidential communications with victims.

TTY (Teletypewriters)

Description/Risks

- A communication tool for people who are Deaf or hard-of-hearing that connects to a phone line.
- Can be misused to impersonate someone.
- All TTYs provide some history of the entire conversation. The history and transcripts of TTY calls might be recorded on paper or electronically. The abuser might monitor this information or misuse it; in some cases, a survivor might be able to introduce a transcript of a threatening TTY conversation as evidence.

Safety Strategies

- Create a code word or phrase to ensure the identity of the person on other end and to avoid impersonation.
- Regularly clear TTY history unless a cleared history would increase risk.
- Best Practice: Agencies should clear their TTY memory, avoid printing transcripts, and shred all printed transcripts of TTY calls, unless the victim explicitly requests that one printed transcript be kept for safety or evidence reasons.

Relay Services

Description/Risks

- A free service where a third party (operator) facilitates a conversation for a person who is Deaf, hard-of-hearing, or has a speech disability.
- Users may access relay services via a video phone, web cam, computer, TTY or other device. They might use a phone line, Internet or cable connection.
- Can be used to impersonate someone.
- Relay conversations and devices may be monitored.

Safety Strategies

- Establish secret code words or phrases to ensure identity of person.
- If possible, use a "safer" TTY, device, or computer to access relay (one an abuser hasn't had access to).
- Be aware that relay conversations might be secretly recorded by an abuser using spyware or video recording.
- When possible, meet in person to discuss sensitive information.
- Best practice: Relay services are not a substitute for providing interpreters. Agencies should always offer an in person certified sign language interpreter. Additionally, agencies can contract with Video Remote Interpreter (VRI) services. These are not video relay services but use similar technologies; an agency would need to have a high-speed connection and video phone or web camera. An agency can contract with a VRI provider to be on call remotely 24X7 in case a survivor arrives and needs an interpreter quickly.

Email

Description/Risks

- It is like a postcard and is not a private form of communication.
- Can be monitored and intercepted in a variety of ways, many times without your knowledge. Stalkers can intercept and monitor email using spyware or by getting your password; they might change your email settings so they can get secretly forwarded or secretly copied (designated as bcc) on every email you send or receive from that account.

Safety Strategies

- Avoid using email for sensitive or personal information.
- If you think your email is being monitored, consider creating an additional new email account on a safer computer. Never access the new accounts on a monitored computer (see above).
- When setting up a new email account, don't use any identifying information.

- Avoid passwords that others can guess.
- If you receive threats by email, save the electronic copies. Keep the emails in the system, but also consider forwarding a copy to another email account. You can also print copies of the email; see if the print version can display the full email header.
- Consider reporting email threats or hacked accounts to law enforcement. These are crimes and the police can use email header information to help trace emails to the original sender.

Hidden Cameras

Description/Risks

- Affordable, accessible, and easy to install, cameras come hidden in various items (clocks, plants, etc.).
- Can be wired into your house or transmit wirelessly.
- Can be very difficult to detect.
- Can create image files that include time, date and location data.
- Abuser can install camera surveillance and monitor all your activity remotely over the Internet.
- *Safety Strategies*
    - Trust instincts. If abuser knows something that can only be seen, a camera may be being used.
- Camera detectors can help to find wireless cameras that are giving off a signal, but will not detect a wired camera.
- Law enforcement may help to search for hidden cameras.

Personal Information & the Internet

Description/Risks

- All kinds of public and private organizations, agencies, services, and businesses collect and share information about people. These can include government and nongovernmental organizations, community groups, schools and online sites such as social networking, gaming or job sites. Search engines index the

web and create virtual card catalogs. Some search deep into online databases and compile extensive profiles on people.

- Identifying information may be online without victims' knowledge.
- Stalkers use the Internet to find information about the victim including the location and contact information of victim. They also use online spaces to defame, target and damage the reputation of the victim.

Safety Strategies

- Do searches on yourself to see what information is available.
- Be cautious and creative when providing personal information: only provide information that you feel is critical and safe for things like store discount cards.
- Ask schools, employers, courts and government services about Internet publications. Request that your information and photos not be posted in public directories or online. In court systems, ask up front how your court records can be sealed and not posted online for safety reasons.
- If you have a restraining order, providing that can expedite these requests.

Supported by US DOJ-OVC Grant# 2007-TA-AX-K012. 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.