



# TECH SAVVY STUDENTS

NNEDV

## CHOOSING WHO GETS TO SEE YOUR INFO

### BLOGS & SOCIAL NETWORKING

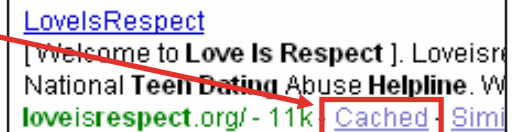
**HAVE YOU PUT YOUR PROFILE ON A SOCIAL NETWORKING SITE LIKE MYSPACE OR FACEBOOK, AN ONLINE DATING OR ALUMNI SITE?** Have you set your profile to be private? If not, anyone who visits that site, including college admissions offices, teachers, family, potential employers or even stalkers can see your personal information.

**DO YOU USE FREE EMAIL, A BLOG, INSTANT MESSAGING, OR SHARE MUSIC OR PHOTOS ONLINE?** When you signed up for that service, did you give your name, age, gender, the town you live in or your hobbies? If so, the company that got your information might post it online for everyone to see. Many times, you can choose not to have your information included in public directories. You can also provide very little information if you want (only your first name or a fake name, for example).

**HAVE YOU EVER PLAYED IN THE SCHOOL BAND, HAD YOUR WORK INCLUDED IN AN ART SHOW, OR BEEN ON A SPORTS TEAM?** If so, your name, personal details, and contact information might be posted online. Some websites will remove information at your request, but if the site is archived, your information may not really be gone. If you don't want information posted online, you should act quickly to have it removed.

### ARCHIVES

Websites can be "archived" or "cached" so people can still access the old content even if the website disappears or changes. This means that any information posted to the web could be online for a long time - maybe even forever. Internet Archive ([www.archive.org](http://www.archive.org)) has 55 billion web pages!



### OTHER WAYS YOUR INFORMATION GETS ON THE WEB:

- ... A store asks for your phone number or zip code when you buy something and that information is put into a database. The store might later sell your information to a data broker who posts it in an online directory.
- ... A friend or classmate posts information or photos that include you. Or, a relative posts a family photo album with you in it.
- ... If you have a drivers license, have gotten a traffic ticket or gone to Court, your name, address, and other personal information may be available online on a court or county website.



### REMOVING INFORMATION

Sometimes it's okay to leave certain information online, especially if it's harmless. When trying to remove your information from any website, consider not sharing your correct information because data brokers make money by selling accurate information. If you want something removed, the website may have instructions, or provide a form or email address to contact them. If the information is in a government record, you may need to fill out an official petition, motion, request or letter.

### HOW DO I KNOW WHAT IS ON THE WEB ALREADY? If you can find it, someone else can too.

- ... Search the web for your personal information and photos. Some places to start: Google, Yahoo, Classmates.com, YouTube and Flickr.
- ... Look on websites for groups and places where you might have a connection: your school, clubs, jobs, faith community, sports teams, community and volunteer groups, etc.

## PHONES

### ARE YOU RECEIVING HUNDREDS OF TEXT MESSAGES OR VOICEMAILS FROM SOMEONE YOU DON'T WANT TO TALK TO?

If you're being stalked via phone or text message, you have options:

- ... For support, you can call the free National Dating Abuse Helpline at 1-866-331-9474 (TTY 1-866-331-8453)
- ... You can talk to your phone service provider about call blocking and other call features, or about changing your number.
- ... You can talk to the police to find out if there is evidence for a stalking or harassment charge. Harassing phone calls and text messages are often illegal.

## SPYING ON YOU

### DOES SOMEONE SEEM TO KNOW ABOUT EVERY EMAIL YOU'VE WRITTEN OR EVERYTHING YOU WROTE IN AN INSTANT MESSAGE?

Someone may be using the logging feature on your instant messaging program, or may have changed your email program settings to secretly send them copies. It's also possible that someone may have installed spyware on your computer. Stalkers can install spyware even if they don't have physical access to your computer or handheld device. Some stalkers might hack into your computer from another location via the Internet. Some might send spyware as an attached file that automatically installs itself when you open the email or initially view it in a preview window. Others may email or instant message a greeting card, computer game or other decoy to lure you into opening an attachment or clicking a link.

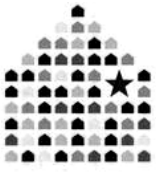
Once spyware is on your computer, it can run in stealth mode and is difficult to detect or completely uninstall. If the person who installed spyware has physical access to your computer, a special key combination can be used to make a secret log-in screen appear. After entering the password, the spyware program lets that person view a record of all computer activities since the last login, including emails you sent, documents printed, websites visited, searches you did and more. Even without physical access to your computer, stalkers can set up the spyware to take pictures of your computer screen (screen shots) every few seconds and have these pictures sent to them over the Internet without your knowledge.



## PROTECTING YOUR PRIVACY

If you think there may be spyware on your computer try to use a safer computer when you look for help. It may be safest to use a computer at a library, friend's house, community center, or Internet café.

- ... If you suspect that someone has the password to any of your accounts, go to a computer that this person doesn't have access to and change your password. Only check that account from a computer that this person cannot access. The most secure passwords are at least 8 characters long and use a combination of letters and numbers.
- ... If you suspect that an abuser can access your email or Instant Messages (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](mailto:bluecat@email.com) and not [Your-RealName@email.com](mailto:Your-RealName@email.com)) Also, carefully read the registration screens so you can choose not to be listed in any online directories.
- ... Remember that many phones are just mini-computers. Stalkers can put spyware programs on cell phones and other handheld devices to track every text message sent and phone number dialed. Also, if someone knows or can guess your password, that person can log on to your phone account, bank account or other accounts online. So keep your passwords secret and change them often!



NNEVDV

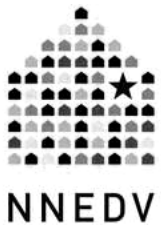
# Technology Safety Planning with Survivors

## *Tips to discuss if someone you know is in danger*

*Technology can be very helpful to victims of domestic violence, sexual violence, and stalking, however it is important to also consider how technology might be misused.*

- 1. Trust your instincts.** If you suspect the abusive person knows too much, it is possible that your phone, computer, email, or other activities are being monitored. Abusers and stalkers can act in incredibly persistent and creative ways to maintain power and control.
- 2. Plan for safety.** Navigating violence, abuse, and stalking is very difficult and dangerous. Advocates at the National Domestic Violence Hotline have been trained on technology issues, and can discuss options and help you in your safety planning. Local hotline advocates can also help you plan for safety. (*National DV Hotline: 1-800-799-7233 or TTY 800-787-3224*)
- 3. Take precautions if you have a “techy” abuser.** If computers and technology are a profession or a hobby for the abuser/stalker, trust your instincts. If you think he/she may be monitoring or tracking you, talk to a hotline advocate or the police.
- 4. Use a safer computer.** If anyone abusive has access to your computer, he/she might be monitoring your computer activities. Try to use a safer computer when you look for help, a new place to live, etc. It may be safest to use a computer at a public library, community center, or Internet café.
- 5. Create a new email account.** If you suspect that anyone abusive can access your email, consider creating an additional email account on a safer computer. Do not create or check this new email from a computer your abuser could access, in case it is monitored. Use an anonymous name, and account: (example: [bluecat@email.com](mailto:bluecat@email.com), not YourRealName@email.com) Look for free web-based email accounts, and do not provide detailed information about yourself.
- 6. Check your cell phone settings.** If you are using a cell phone provided by the abusive person, consider turning it off when not in use. Also many phones let you to “lock” the keys so a phone won’t automatically answer or call if it is bumped. When on, check the phone settings; if your phone has an optional location service, you may want to switch the location feature off/on via phone settings or by turning your phone on and off.
- 7. Change passwords & pin numbers.** Some abusers use victim’s email and other accounts to impersonate and cause harm. If anyone abusive knows or could guess your passwords, change them quickly and frequently. Think about any password protected accounts - online banking, voicemail, etc.
- 8. Minimize use of cordless phones or baby monitors.** If you don’t want others to overhear your conversations, turn baby monitors off when not in use and use a traditional corded phone for sensitive conversations.
- 9. Use a donated or new cell phone.** When making or receiving private calls or arranging escape plans, try not to use a shared or family cell phone because cell phone billing records and phone logs might reveal your plans to an abuser. Contact your local hotline program to learn about donation programs that provide new cell phones and/or prepaid phone cards to victims of abuse and stalking.
- 10. Ask about your records and data.** Many court systems and government agencies are publishing records to the Internet. Ask agencies how they protect or publish your records and request that court, government, post office and others seal or restrict access to your files to protect your safety.
- 11. Get a private mailbox and don’t give out your real address.** When asked by businesses, doctors, and others for your address, have a private mailbox address or a safer address to give them. Try to keep your true residential address out of national databases.
- 12. Search for your name on the Internet.** Major search engines such as “Google” or “Yahoo” may have links to your contact information. Search for your name in quotation marks: “Full Name”. Check phone directory pages because unlisted numbers might be listed if you have given the number to anyone.

**For more safety information, call the  
National Domestic Violence Hotline at  
1-800-799-SAFE (7233) or TTY 800-787-3224**



# Un Plan de Protección de la Tecnología para las(os) Sobrevivientes

*Unos consejos para analizar si usted conoce a una persona que está en peligro*

*La tecnología puede ser de mucha ayuda para las víctimas de la violencia doméstica, de la violencia sexual, y del acoso, pero es importante considerar que también puede ser usada indebidamente.*

- 1. Confíe en sus instintos.** Si usted sospecha que la persona abusiva sabe demasiado, es posible que su teléfono, su computadora, su correo electrónico, o que sus otras actividades estén siendo monitoreadas. Los agresores y los acosadores pueden ser muy persistentes y crean maneras para mantener el poder físico y el control psicológico.
- 2. Planee su protección.** Es muy difícil y peligroso navegar con la violencia, el abuso, y el acoso. Los representantes de la Línea Nacional de la Violencia Doméstica están entrenados tecnológicamente, y pueden platicar con usted acerca de sus opciones y pueden ayudarle a planear su protección. También los programas locales pueden ayudarle con el plan. (*Línea Nacional de la Violencia Doméstica*: 1-800-799-7233 o TTY 800-787-3224)
- 3. Sea precavida(o) si el agresor es un “técnico”.** Confíe en sus instintos propios si las computadoras y la tecnología son la profesión o el pasatiempo del agresor/acosador. Si usted piensa que él/ella puede estar controlándole o vigilándole, hable con la línea nacional o con la policía.
- 4. Use una computadora que esté más protegida.** Si una persona abusiva tiene acceso a su computadora, él/ella pudiera estar observando sus actividades en la misma. Trate de usar una computadora que esté más protegida cuando busque ayuda, cuando esté buscando otro lugar para vivir, etc. Podría ser más seguro si usa una computadora en la biblioteca pública, o en el centro comunitario, o en un café de Internet.
- 5. Cree una dirección nueva en su correo electrónico.** Si usted sospecha que una persona abusiva puede tener acceso a su correo electrónico, considere crear otra cuenta en una computadora más segura. No abra o vea ésta cuenta nueva en la computadora que el agresor pudiera usar, en caso de que ésta esté siendo vigilada. Use anónimos (por ejemplo: [gatoazul@email.com](mailto:gatoazul@email.com), no use su NombreReal@email.com) Vea el correo electrónico gratis, y no les proporcione información detallada de usted.
- 6. Revise su teléfono celular.** Si usted ésta usando un teléfono que la persona abusiva le dio, considere apagarlo cuando no lo esté usando. También muchos teléfonos le permiten “cerrar” las teclas para que el teléfono no conteste automáticamente o para que no llame automáticamente en caso de que se golpee en algún lugar. Cuando esté prendido, revise la programación, si su teléfono tiene un servicio de colocación, querrá apagar/prender ese servicio cambiando la programación apagando y prendiendo el teléfono.
- 7. Cambie la contraseña y sus números de identificación personal (PIN).** Algunos agresores usan el correo electrónico de la víctima y otras cuentas para hacerse pasar por ellas(os) y causar un daño. Si una persona abusiva sabe la contraseña de su correo electrónico o puede adivinarla, cámbiela rápido y frecuentemente. Piense en las cuentas que son protegidas con una contraseña - como el banco a través del Internet, el sistema de mensajes, etc.
- 8. Trate de no usar teléfonos sin cordón o los monitores para los bebés.** Si usted no quiere que otros escuchen sus conversaciones, apague los monitores para bebés cuando no los use y use un teléfono con cordón cuando tenga conversaciones sensitivas.
- 9. Use un teléfono celular donado ó un celular nuevo.** Cuando llame o reciba llamadas privadas o para preparar el escape, trate de no usar un teléfono compartido o en un plan familiar, por que los cobros vienen con detalles que podrían revelar sus planes al agresor. Comuníquese con la línea local para aprender más acerca de los programas que donan teléfonos celulares nuevos y/o tarjetas de teléfono prepagadas para las víctimas del abuso y del acoso.
- 10. Pregunte acerca de sus documentos y de sus datos.** Muchos sistemas en las cortes y en las agencias de gobierno están publicando los documentos en el Internet. Pregúnteles cómo protegen o cómo publican sus datos y pídale a la corte, al gobierno, al correo y otras agencias que nadie tenga acceso a sus documentos para proteger su seguridad o que sellen los documentos.
- 11. Obtenga un servicio de mensajes privado y no proporcione su dirección verdadera.** Cuando un negocio, o el doctor, u otras personas le pregunten por su dirección, tenga listo un correo postal o una dirección segura. Trate de mantener su dirección lejos de la colección de información nacional.
- 12. Busque su nombre en el Internet.** Los buscadores más grandes como “Google” o “Yahoo” pudieran tener enlaces a su información. Busque su nombre entre comillas: “Nombre Completo”. Revise las páginas del directorio telefónico, por que los números que no deben de ser enlistados pudieran estar en la lista si usted se lo ha dado a alguien.

**Para más información sobre la protección,  
llame a la Línea Nacional de la Violencia  
Doméstica al 1-800-799-SAFE (7233) ó  
TTY 800-787-3224**



# 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

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.

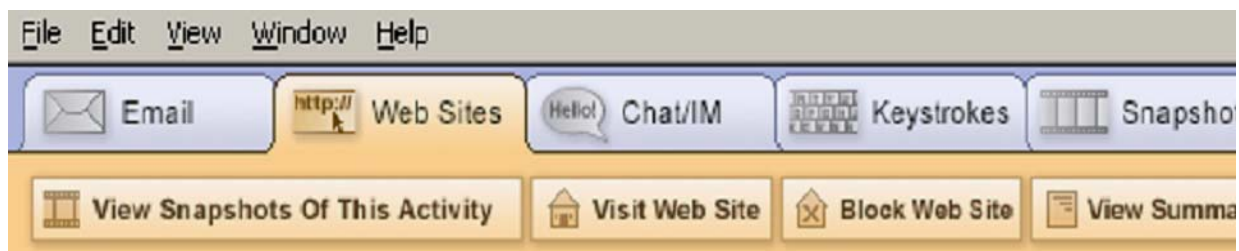
For more information on adware and malware, see "Protecting Your Computer" at [www.antispywarecoalition.org/documents/documents/ProtectingYourComputerflyerletter.pdf](http://www.antispywarecoalition.org/documents/documents/ProtectingYourComputerflyerletter.pdf)

## **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](mailto:bluecat@email.com) and not [YourRealName@email.com](mailto: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](http://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.

## 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: [www.nnedv.org/SafetyNet/Publications/NNEDV\\_DataSecurityHandout.pdf](http://www.nnedv.org/SafetyNet/Publications/NNEDV_DataSecurityHandout.pdf)

### **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](http://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.