



TECH SAVVY TEENS

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) has 55 billion web pages!

[LoveIsRespect](http://LoveIsRespect.org/)

[welcome to [Love Is Respect](http://LoveIsRespect.org/)]. LoveIsRespect.org is the National Teen Dating Abuse Helpline. www.loveisrespect.org/ - 11k [Cached](#) [Similar](#)

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:

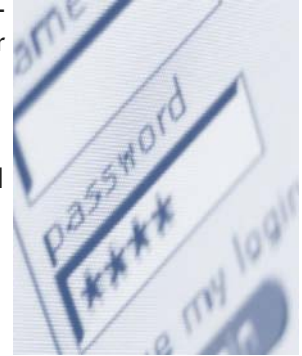
- For support, you can call the free U.S. National Teen Dating Abuse Helpline at 1-866-331-9474 (TTY 1-866-331-8453)
- You can talk to your phone service provider about call blocking and other call features, or about changing your number.
- You can talk to the police to find out if there is evidence 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 pre-view 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 and not 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!