



---

## Online Safety and Cyberstalking

The Internet is fast becoming the main way in which people work, communicate, relax, and research. Therefore, it is important that you be aware of what information you should be protecting. Most of us are aware of software packages that protect us from spyware, adware, spam, and viruses, but in today's networked lifestyle, there are other dangers lurking in the corners of cyberspace.

Since online capabilities are branching out from the desktop computer to the laptop computer to the cellular telephone, predators and stalkers can now reach us at any time and any place. Keeping yourself safe is a priority.

### Keeping Yourself Safe Online

- *Keep your identity private.*  
Sites such as MySpace and Facebook encourage you to post personal information and pictures. This can be very dangerous. You may think that your friends and family are the only ones interested, but since this is a public forum, you never know who is looking at this information with the intent of using it against you. Never give your last name, address, phone number, work information, or any other identifying information. Never post information that you wouldn't want published in a newspaper or broadcast on TV or on the radio. This is exactly what you are doing when you post information online. Never post personal information about your friends or family members without their permission. Create an identity that makes you virtually unidentifiable – use a nickname for your screen name and a cartoon or other art for your picture.
- *Never meet face-to-face with someone you have “met” online.*  
Don't meet after a short time of communicating with someone. Give it time. If you do decide to meet with someone you have been chatting with online, DO NOT go alone. Take someone with you and meet in a public place that you are familiar and comfortable with. If you have to travel to meet someone, use your own transportation. Take your cell phone. Give your location to friends or family just in case, and if you have it, give them your date's contact information as well.
- *Never respond to email, IM's, chat comments, or other messages that are hostile, belligerent, inappropriate, or make you uncomfortable.*  
The person simply wants some kind of response. When you send a response, you are rewarding that behavior and are encouraging the person to send more. Be wary of anger, demeaning or disrespectful comments, physically inappropriate comments, frustration from the other person, or attempts to pressure or control you.
- *Use common sense and be cautious.*  
Don't believe everything you read in a profile, on message boards, or in a chat room. If someone or something sounds too good to be true, it probably is. Be wary of odd behavior. Trust your gut! If your gut tells you something is wrong or someone is lying, listen to your intuition.

## Cyberstalking

Estimates show that roughly 20% of stalking cases in Los Angeles involve electronic media. While it may seem farfetched to apply this statistic to Arkansas, law enforcement agencies across the state and the US are beefing up training in cyberstalking and harassment. Cyberstalking is using electronic media to harass or stalk another person. This may include sending threatening or obscene emails, sending lewd pictures, or even creating harassing, intimidating websites. Not only are cyberstalkers researching their victims online but also they are using the information gathered to wreak havoc in the lives of their victims. The Department of Justice has recently reported that the ability to hide behind a computer screen may be creating more harassers. Federal legislation prohibiting stalking was passed in 1996. Most states followed and passed antistalking legislation as well. However, many states do not have anticiberstalking laws. Arkansas has expanded its laws to include unlawful computerized communications.

## If You Are Harassed Online

- State clearly once and only once that you do not wish to receive any further communication.
- Don't respond if the email is from a stranger; when you reply, you are verifying your email address.
- Save all communications. Save the messages from the sender as well as your one reply to stop all emails. Print them and save them to the hard drive or a disk. Try to get all the header information because this serves as a tracking device.
- File a complaint with the administrator of the harasser's ISP. Usually you can do this by typing [postmaster@\(name of ISP\)](mailto:postmaster@(name of ISP)). You can also search the ISP for further information about how to report the harassment.
- Contact the authorities. If the local police is unable to help, you can try the county or state police department. If the harasser lives in another state, you should also contact the local office of the FBI.

## To Keep Yourself Safe from Cyberstalkers

- Select an address or screen name that is gender-neutral.
- Send yourself an email to see what information is included in your "signature". Remove any personal information.
- Consider separate email accounts. Have a primary address that you give to family and friends and a secondary account that you use for all other online activity. You can get free accounts through several online services.
- Once a month, do an Internet search on your name. If any personal information comes up, you may have your name removed from the directories by contacting each search engine on which you are listed.

Information adapted from The Aurora Center for Advocacy and Education of the University of Minnesota, Andrea Rock, *Ladies' Home Journal*, 2000, and Catholic Singles Mingle, "Catholic Singles Online Dating Safety", retrieved 6/12/2002, from [www.catholicmingle.com/catholicsinglesdating.htm](http://www.catholicmingle.com/catholicsinglesdating.htm)

---

**STAR Central – Office of Support, Training, Advocacy, & Resources on Sexual Assault and Relationship Violence**  
*a program of*



Updated: July 2006