

## ***ON-LINE WISDOM***

---

Enjoy the fun that comes with on-line communities, but be smart about it. **Remember** anything you post on-line is PUBLIC information, it is not private!

### ***IDENTITY THIEVES ARE LOOKING FOR:***

- Your photo (which can be used to make fake I.D.)
- Your birth date (even if you just post your month and date, they can easily figure out the year if you have posted other info like the year you graduated.)
- S.I.N., Student numbers, credit cards or bank accounts etc.
- Your address.

### ***ASK YOURSELF THE FOLLOWING:***

- Would I still post it if it was on a public bulletin board on campus?
- If it were published in the paper?
- If someone passed the info or photo on to my parents?
- If I knew a potential employer might see it?, my professors?, Campus Police?

The preceding information and guidelines have been adapted from the following literature:

- <http://www.enough.utoronto.ca>
- [www.missingkids.com](http://www.missingkids.com)
- <http://tcs.cybertipline.com>
- [www.metrac.org/programs/info/cyber.htm](http://www.metrac.org/programs/info/cyber.htm)
- [www.sfwa.org/gateway/stalking.htm](http://www.sfwa.org/gateway/stalking.htm)
- [www.usatoday.com/tech/news/2006-01-08-myspace-teens.htm](http://www.usatoday.com/tech/news/2006-01-08-myspace-teens.htm)
- [www.facebook.com/press/php](http://www.facebook.com/press/php)
- Mendelson, B. (2005). Facebook not fun and games: colleges, potential employers may scope out Facebook profiles. UWire Service. 06 December, 2005.
- Montermini, F. (2005). Facebook raises privacy concerns. The Trinity Tripod. 29 November 2005.

## **COMMUNITY SAFETY OFFICE** **“YOUR PERSONAL SAFETY MATTERS”**

UNIVERSITY OF TORONTO  
21 Sussex Ave. 2nd Floor  
Toronto, Ontario

Phone: 416-978-1485  
[www.communitysafety.utoronto.ca](http://www.communitysafety.utoronto.ca)

## **COMMUNITY SAFETY OFFICE**

---

# **ON-LINE COMMUNITIES AND YOUR SAFETY**

**COMMUNITY SAFETY OFFICE**  
**“YOUR PERSONAL SAFETY MATTERS”**

**21 Sussex Ave. 2nd Floor**

---

**Tel: 416-978-1485**

## ***GENERAL INFO ABOUT ON-LINE COMMUNITIES, SOCIAL NETWORKING SITES AND BLOGS:***

### ***DID YOU KNOW:***

According to USA Today, blogs and social networking sites have recently exploded in popularity. The number of visitors to Myspace went from 4.9 million in 2005 to currently over 67 million.

According to Chris Hughes from [press@facebook](mailto:press@facebook), approximately 85% of students in colleges & universities in North America have a profile on Facebook.

These sites are a great way for students to connect with friends and seek like-minded individuals. The majority of the activity on these sites is legal and can be positive. However, many users of these sites assume that everyone is like them and tend to be less cautious and more free when interacting with others. Many users don't realize that they are potentially putting themselves and others in danger by giving out too much personal information. This information can be used by others for the purposes of bullying/harassing and/or identity theft.

### ***THINGS TO KEEP IN MIND:***

- Employers may look up potential candidates on-line before making hiring decisions.
- Police may use these sites to track illegal activity.
- According to news reports, Social Networks and other sites may sell personal information about people who use their service. Therefore your profile can be viewed by others without your knowledge.

### ***CONTINUED:***

- Your personal information can be used for the purposes of stalking and/or identity theft. Take time to consider the potential consequences of posting such things as your picture, address, student number, class schedule etc.
- Information you post can follow you around for years to come. Even if you remove certain information, someone may already have copies or may have distributed that information on the internet.
- Websites may have privacy policies but that does not prevent people with access (other members of Facebook for example) from redistributing your information elsewhere on the internet.

### ***TIPS TO KEEP YOURSELF SAFE:***

- Never post your personal information such as cell phone numbers, address or the name of your residence on campus.
- Use a "nonsense" password that has no relation to you as a person and never give out your personal password. Change it on a regular basis.
- Limit access to your profile, only add people as friends to your site if you know them in real life.
- If you plan to meet someone that you have met on-line, meet this person in a busy area (ex: coffee shop). Tell someone where you are going and when you expect to return. Have a friend call you on your cell phone to check in with you.

- Remember that posting information about your friends could put them at risk. Seek permission from your friends before posting any of their personal information. Avoid posting any plans or activities on your site, as well.
- Check the Privacy settings of the social networking site that you use. Set it so that people can only be added as your friend if you approve of it. Also set it so that people can only view your profile if you have approved them as a friend.
- Report violations of Terms of Service to the networking sites if they violate.
- Electronic communication that is unwanted, and that is persistent, repeated, obscene or otherwise unwelcome may be harassment, and action may be taken under University policy. If you are concerned about your personal safety and/or would like more information contact the University of Toronto's Community Safety Office.
- If the comments are threatening in nature, you can contact Campus police and/or Toronto Police for assistance.