Stalking resource center

THE NATIONAL CENTER FOR Victims of Crime

THE SOURCE

Newsletter of the Stalking Resource Center Volume 7, Number 1, Winter 2008

# Social Networking Sites: A Bonanza for Stalkers?

“Vengeance will be mine...,” declared a defiant message on MySpace.com. “I should have killed you all when I had a gun and some drugs.” This violent monologue, one of several postings on the writer’s site, threatened his ex-wife, who had fled the state to escape his abuse. In postings on other sites, he demanded photos of his family and warned that if he didn’t get to see the kids, “it isn’t going to be real good, because I’m gonna see them whether you let me or not.”

The increasing use of MySpace to threaten and stalk victims raises many important questions. Do social networking sites enable stalking? What recourse do victims have when these sites are used to stalk? And what tools can help block the use of these sites to stalk?[1]

## What Are Social Networking Sites?

Social networking sites such as MySpace and Facebook are virtual communities where people with mutual interests meet online to share information and build relationships. Site visitors can chat, debate, network, and socialize. On many sites, members may post details about themselves—photos; educational backgrounds; favorite books, movies, and music; and relationship status. Others sites promote business, activism, networking, counseling, socializing, or many types of recreational interests. Sites such as MySpace, Facebook, Friendster, and Xanga have attracted millions of members, particularly among teenagers and young adults.

## How Do They Work?

On many social networking sites, anyone with a computer and Internet access can become a member. Some sites require only an e-mail address, and many sites have no system to verify the validity of information that registrants provide. A few sites, including MySpace and Friendster, have minimum age requirements (14 and 16, respectively) although these sites have no reliable method to verify a user’s age. Once a member, anyone can post personal information, images, music, or other data on their Web pages, depending on the site’s features. On many sites, members select a circle of “friends” who can post messages on their profiles, add comments, or access pages not visible to other users. Unless the site allows members to control access to specific information (and members actually exercise those options), everything posted on a profile may be visible to all site visitors. Most sites require members to agree to terms of proper conduct, but enforcement of such terms is sporadic and often depends on members to report violations.[2]

## Links to Stalking

The attractions of social networking—access to an ever-widening world of “friends”—can lead users to overlook the pitfalls of these sites. Young people, in particular, may tend to view such sites as “part of their own little world,”[3] not a public bulletin board with millions of other visitors. They may not recognize that posting personal information may lead to contacts from sexual predators, identity theft, fraud, or stalking—or that anyone could post a bogus profile to disparage, misrepresent, harass, threaten, or embarrass them.[3]

## Cases

Several recent cases suggest how stalkers and predators are beginning to use social networking sites  In the months the Virginia Tech massacre, the shooter, Seung-Hui Cho, allegedly used Facebook to locate and stalk female classmates. In July 2007, authorities in Lorager, Louisiana, arrested a 17-year old for stalking and cyberstalking another teenage boy. The alleged stalker's MySpace page featured a video of the accused pistol-whipping another boy posing as the victim.

In 2006, a University of Kansas student received death threats from someone who found her class schedule on-line. He posted photos from the victim's MySpace account on his own site, along with insults about her appearance and her major. Also last year, National Public Radio's Veronica Miller discovered "Becky," a MySpace "cyber twin" who had copied a photo of Miller from Facebook and published it—along with photos of Miller's family—on the imposter's site. Although Miller's impersonator did not threaten or stalk her (and MySpace promptly removed "Becky's" site), the incident shows the potential of such sites for stalking or harassment.

## Features to Watch

Several social networking site features may increase users' vulnerability to stalkers and other predators. For example, new MySpace members are asked to supply a name or nickname and information about their marital status, sexual orientation, hometown, school, religion, education, interests (e.g., music, movies, television, books, and heroes), children, or income. Although most of these questions are optional, users may automatically answer them because they are using the site to meet other people. On many sites, all these answers go "public," remaining open to anyone who uses the site. Stalkers may use such information to gain access to site members.

Many social networking sites (e.g., Stalkerati) also have search tools that can simultaneously pull personal information about the same person from a number of different sites, including MySpace, Friendster, Flickr and Google. A recently shut-down site called fbstalker.com tracked changes in the profiles of users' friends while saving copies of each page to compare to subsequently updated files.[5] Other sites, such as Profilesnoop and Link View, allow visitors to trace a user's Internet Protocol (IP) address (and even physical location on Google Maps) with many social networking sites, including Facebook.[8]

Stalkers can also use social networking sites to introduce spyware into the computers of their victims. Spyware infection rates are increasing, an anti-spyware company spokesman told *Business* Week, in part because "people are creating multiple profiles, and the links on their sites will take you to sites that will download adware and spyware."[9] Stalkers can exploit this vulnerability on their victims' profile pages. Once downloaded, spyware can help stalkers gather information about all their victims' computer activity, including e-mails, chats, instant messages, keystrokes, passwords, and Web sites visited.

## Legal Recourse

Stalkers who use social networking sites as part of a pattern of stalking may be subject to criminal charges. For example, someone who repeatedly follows and tracks a victim in her car, as well as posts a lewd photo of the victim on a social networking site, can be charged with the crime of stalking. Also in many states, cyberstalking statutes enable prosecutors to charge those who use technology to stalk and harass their victims. Other states have general stalking laws that define 'pattern of conduct' broadly enough to cover the use of technology to stalk. Most of these laws are relatively new, however, and few cases involving social networking sites have yet been prosecuted. offensive or defamatory material regarding the victim from the site.

## New Laws

Lawmakers are starting to propose measures to govern the use of social networking sites. In April 2007, for example, the California legislature introduced a bill to prevent individuals from using social networking sites to incite harassment or abuse against an individual. Harassment would include posting digital images or messages on Web sites to cause fear, harassment, or harm to an individual.[10]

## Prevention: The Best Defense

The best defense against social networking site stalking is to use the sites with extreme caution. Wise users carefully consider what they post (see "Think Before You Post, p. XX). Last names, school names, favorite hangouts, phone numbers, and addresses make it easy for stalkers to locate victims. Photos with identifiers (like school names or locations) also increase a victim's vulnerability. Posted information is permanently public. "You can't take it back," warn experts Larry Magid and Anne Collier, about information posted on-line. "Deleted" information can be recovered, for example, from Google's cache of deleted and changed Web pages and from Internet Archive (*archive.org*), which offers access to deleted postings.[12]

Users can also boost security by limiting online "friends" to people they actually know and by activating all available privacy settings. Since June 2006, MySpace has allowed all users to keep their profiles private—open only to those designated as "friends." MySpace also offers other privacy options: to control how others may add their names to friends lists, to approve friends' comments before hosting, to hide the feature that shows when they are online, or to prevent e-mailing photos. To activate these features, members must change their settings and choose the privacy options they prefer. Although stalkers can find ways around these protections, members who use them are less vulnerable than those who do not.

## Networking Safely

The social networking revolution presents complex dilemmas. The convenience and appeal of these sites are undeniable, and stalking cases that involve social networking are still quite rare. Yet as stalkers diversify their tactics, they are likely to exploit any available technology. For stalking victims as well as the public, safe social networking will require awareness and vigilance.

As the Stalking Resource Center continues to track this issue, we welcome insights from the field about these sites, related cases, and new features to keep them safe. We will periodically report our findings at www.ncvc.org/*src*. For more information, please visit the SRC Web site or call 202-467-8700.

**For victim assistance, please call 1-800-FYI-CALL M-F 8:30 AM - 8:30 PM EST or email gethelp@ncvc.org**

[1] As told to staff by a stalking survivor.

[2] Massachusetts Attorney General, "Consumer Advisory: AG Reilly Warns Parents about the Potential Dangers of Children Using Social Networking Sites Such and MySpace and Xanga," August 29, 2006, *www.ago.state.ma.us/sp.cfm?pageid=986&id=1710* (accessed February 26, 2007).

[3] Justin Pope, "Colleges Warn about Networking Sites," the Associated Press, August 2, 2006 (accessed March 4, 2007).

[4] Adam Geller, "VA Gunman Had 2 Past Stalking Cases," Associated Press, April 18, 2007, www.newsday.com (accessed July 24, 2007).

[5] Florida Parishes Bureau, "Loranger Teen Booked in Threats to Harm Other Teen, Cyberstalking," Capital City Press, July 12, 2007.

[6] KUJH-TV News, "Facebook Used to Aid Stalkers, May 4, 2006, *www.tv.ku.edu/newsd* (accessed March 5, 2007).

[7] Veronica Miller, "Stalking Becky, The Girl Who Stole MySpace," National Public Radio, All Things Considered, August 6, 2006, http://www.npr.org/templates/story/story.php?storyId=5622009 (accessed July 25, 2007).

[8] Andy Meyers, "On-line Stalking Nothing New," *The Brandeis Hoot*, September 8, 2006, www.thehoot.net (accessed March 5, 2007).

[9] Arik Hesseldahl, "Social Networking Sites a 'Hotbed' for Spyware, *Business Week*, August 18, 2006, http://www.msnbc.msn.com/id/14413906, (accessed October 12, 2007).

[10] Jaikuman Vijayan, "California Eyes Stronger Cyberstalking Laws, *ComputerWorld* Government, 04/25/07. www.computerworld.com (accessed July 24, 2007).

[11] Larry Magid and Elaine Collier, *Myspace Unraveled: A Parent's Guide to Teen Social Networking*, Berkeley, CA: Peachpit Press, 2007, pp. 122-3.

[12] Ibid.