Internet social networks offer users many benefits, but they also attract criminals who exploit the web sites for illegal activity and jeopardize youth users.

Every day, more criminals establish a presence on the Internet. Consequently, more crimes become linked to online resources and content. MySpace.com is the most popular web site for social networking and a resource for other content. The site also has many criminal users. Law enforcement is using the Internet and web sites like MySpace.com to gather intelligence on suspects, keep tabs on gang activities, lure sex offenders into arrests, and learn more about other types of cyber crime and ways to prevent online victimization in their community.

MySpace.com and other Internet social networking sites offer users the opportunity to communicate with friends and meet new people online. Users of these sites set up “profiles,” a homepage where their hobbies, interests, friends, family, and ambitions can be explored—exposing as much of their life online as they wish. The freedom, ease of use, and possibilities of MySpace.com attracts users in droves. MySpace.com currently has 63 million registered users and attracts 200,000 new users daily, making it the largest networking portal on the World Wide Web. It is almost certain that those numbers will dramatically increase in a matter of months. And anything attracting that many people will draw more than a few bad seeds.

MySpace.com is not the only popular website catering to social needs. Other major networking sites include facebook.com, bebo.com, piczo.com, xanga.com, and friendster.com. These sites work in the same basic way that MySpace.com does, allowing users to create profiles, upload music, pictures, and videos, communicate with one another and form special interest groups.

Social networking sites offer users many positive benefits, such as a sense of community, interaction, information, ability to explore mutual interests with others, social outlets, and more. But like most technologies, the benefits come with a price. MySpace.com attracts criminals such as scam artists, drug pushers, and computer hackers (MySpace.com content is a major source of spyware and Trojan programs). Last month, an Arizona woman was arrested on murder conspiracy charges after hiring an undercover detective (posing as a contract killer) to kill a woman whose picture she had seen on her boyfriend’s MySpace.com page. But the worst-case scenario with MySpace.com use is the tremendous number of low self-esteem, attention-seeking youth attracted to the site who can become prey to sexual predators and gang recruiters.

**Sexual Predators**

MySpace.com emboldens sexual predators by providing an environment that they can easily use to suggestive ads on MySpace.com may encourage sexual deviants.

A large part of the problem with sex crime related to MySpace.com involves juveniles posting...
revel in their fantasies and gather information on children without immediately revealing their motives. Molesters and rapists are extremely dangerous groups on their own, but content found on MySpace.com can encourage their perversion.

For starters, advertisers on the site know that most users are looking for romantic relationships, and the ads on MySpace.com reflect that. Many of the ads are risqué and may encourage sexual deviants. Ads and other content on the site promote the idea to youth that such subject matter is commonplace, appealing, and necessary for them to achieve their goals when using the site. In fact, MySpace.com users are frequently invited to become friends with members or join existing groups simply to promote and pull in traffic to pornographic sites.

Teen self-promotion and questionable content posted by users are the main problems with MySpace.com. It is difficult to be noticed in an Internet community consisting of millions of users; many juveniles (female and male) will upload personal photos that are very suggestive if not explicit. MySpace.com has a policy to remove such graphic photos and content, but that content must usually be reported to MySpace.com by other users if it is to be removed. Despite the site’s resources, combing through tens of millions of personal pages for objectionable content is not feasible. Furthermore, many of the posted pictures would only be questionable and not removed. The images may be of scantily clad girls, girls in compromising positions, or a teenage boy showing off his physique, which may not be graphic enough to constitute removal from the site, but definitely are encouraging material to a pedophile.

“A lot of social machines are small companies that struck it rich, so they’re lacking layers of security,” said Parry Aftab, Executive Director of CyberLawEnforcement.org, a watchdog group that works with law enforcement and social networking sites to promote online safety. “There’s no way for those sites to authenticate users, and kids are putting themselves at risk. They make it easy for the serious bad guys.”

Aftab said that social dynamics in cyberspace have changed the conventions for sexual predators.

“Sixty percent of eight to 15-year-olds have been involved in cyber bullying and/or harassment, making it the most prevalent form of online abuse. Cyber bullying becomes sexual harassment and cyber stalking,” said Aftab. “At 11, children start to fall to sexual predators. That used to end when they reached 15 because they used to be smart enough to avoid it after that. Social networking changed that. To be noticed on social networks, 16 and 17-year-olds are taking more risks, acting outrageous to get someone to notice their profile.”

Children and teenagers may also act uncharacteristically online because they feel safe doing so. They do not realize the danger should someone want to find them.

“Perceived anonymity makes
kids portray themselves differently and attract predators. But social networks are public. Young girls sometimes think that to play around with men who approach them online is funny. They are not prepared for the level of risk and they don’t use optional privacy settings because they want to be out there,” said Aftab.

In 2002, Christina Long, a 13-year-old Connecticut girl, became the first confirmed fatality in the U.S. by an Internet sexual predator. She was strangled to death by Saul Dos Reis, an illegal alien from Brazil, who was married and worked in a restaurant. Long had a troubled family life, but she was popular, an honors student, altar girl, and cheerleader. She did not fit the common profile of a young victim—typically a quiet loner. The Internet made the difference.

Christina Long lived an alternate life online. She used provocative screen names, had a website that stated she was “ready for anything,” and routinely met for sex with partners she had met in online chat rooms. She had been with Dos Reis several times before he killed her. While Long was the first child killed by an online predator, she was not the last. Sadly, there will be many more.

**Criminal Gangs Online**

“Netbanging” is the term used for gang activity online. It has existed for years, but is now becoming prevalent enough to catch the attention of law enforcement. Using sites such as MySpace.com and YouTube.com, an online video-posting site, gang members can pose with colors, signs, and weapons, post gangsta-rap videos, promote themselves, and threaten their rivals.

**STATISTICS OF ONLINE YOUTH VICTIMIZATION**

According to 2005 data from the National Center for Missing & Exploited Children published in *Online Victimization of Youth and Internet Sex Crimes Against Minors: The Response of Law Enforcement*:

- One in seven children were exposed to unwanted sexual solicitations on the Internet
- One in three youth were exposed to unwanted sexual material (despite usage of blocking filters and monitoring software)
- One in 11 youth were harassed online
- Off-line acquaintances accounted for 14 percent of online solicitation and harassment
- 67 percent of offenders who committed any type of Internet sex crime against minors possessed child pornography
- The majority of offenders were white males older than 25, acting alone
- 39 percent of all Internet sex-crime arrests are crimes against identified victims
- 36 percent are for Internet child pornography
- 25 percent of arrests are Internet solicitations to undercover law enforcement
- Indications are that law enforcement activity and subsequent arrests are growing in the Internet crime domain

Gang members love to show off. They are limited by time, exposure, and possible police intervention elsewhere, but believe that they can get away with anything on the Internet. Gang sites vary in complexity depending on the clique and its resources. Online exposure now exists for commonplace street gangs (Bloods, Crips, etc.), flourishing Hispanic gangs.
(MS-13, Surenos, 18th Street, etc.), hate groups (Ku Klux Klan, National Alliance, Hammerskins, etc.), and even typically more professional and cautious motorcycle gangs (Hells Angels, Outlaws, Iron Horsemen, etc.).

Parental Intervention

Parental involvement is crucial in preventing kids from getting involved in gang activity via the Internet or becoming the victim of a sexual predator.

“It’s easy for a child to get online and be recruited into a gang or put in a sexual predator’s grasp,” said Rehm. “The threat level boils down to how much you’re involved. Talk to your kids.”

Rehm also mentioned specific measures to help keep kids safe.

“Bring your computer into a common area and use monitoring software. If nothing else, get on there and see how it works,” he said.

Both Det. Rehm and Parry Aftab of Cyberlawenforcement.org encouraged parents to take classes to familiarize themselves with Internet safety. Consulting www.wiredsafety.org’s Wired-Ed program is a good place to start.

Aftab said that parents should teach their children to restrict what they post online.

“Use the least amount of personal information possible for the purpose. Make sure that the photos and photo backgrounds don’t give away information that could tip off a predator, such as a school name.”

MySpace.com does have some safeguards in place to protect children. For instance, no one under 14 is allowed to have a MySpace.com profile, and MySpace.com users are largely prevented from searching for members who are younger than 18. However, if a child really wants to increase their presence on the site, usually all they have to do is lie about their age. The number of 98-year-olds on MySpace.com who don’t look a day older than 13 is impressive.

Mainly, children need to understand the danger that the Internet can pose. Parents should encourage children to use common sense and discretion online, especially with strangers. Victims of online abuse should not hesitate to report it to proper authorities.
Law Enforcement MySpace.com Use

MySpace.com can be a tremendous resource for investigation and undercover work by law enforcement. Because of online bragging by gang members and luring efforts of predators, tech-savvy officers can investigate local gangs and individual members and act as child decoys to lure predators to arrests.

Gang members can be careless when using the Internet, and checking their web sites can reveal crimes, associates, and valuable prosecution information.

Being familiar with gang jargon is important in order to perform a thorough search online for gang members in the area. Remember to search for numbers and colors associated with the gang. Hiring an informant to provide monikers or translate online content may be necessary.

Some gangs are becoming more cautious and using site-privacy filters to make their online networks less permeable.

“We’re going to try to get recruited by a local gang and have set up a profile to do that,” said Det. Rehm of the Port St. Lucie P.D. “Some gangs invite you into their group only after they have viewed your profile.”

Recent cases demonstrate how useful online communities can be in helping police find suspects and gather evidence and intelligence for arrests. Criminals using the sites often post comments that are functional confessions before they even know they’re wanted. Anything posted online may be treated as evidence, according to Justice Department guidelines.

In January, 2006, Palmetto Bay, Fla. officers ar-

---

### SPECIFICS OF DEALING WITH MySpace.com

**Custodian of Records** MySpace.com contact information for law enforcement:

- **Phone:** (310) 969-7399
- **Fax:** (310) 969-7394
- **Email:** lawenforcement@MySpace.com

The primary set of laws regarding MySpace.com’s ability to disclose information is the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2701. For questions about these laws, contact the Department of Justice’s Computer Crime and Intellectual Property Section at (202) 514-1026.

For assistance with online communities or to obtain a copy of the MySpace.com Law Enforcement Investigators Guide, contact the ROCIC Criminal Intelligence Unit at (800) 238-7986.

Data retention periods for information on MySpace.com vary from 10 to 180 days, depending on the type of data. MySpace.com will honor written requests to preserve data longer than is legally required if officers seek such an extension. MySpace.com will also act in good faith with law enforcement personnel issuing a written request to disclose information without delay, given that there is danger of serious injury or death. To make an emergency information request, contact the hotline number above.
rested a teen for attempted second-degree murder after other members of his gang boasted about their violent activities on Myspace.com message boards.

Doing computer homework can also keep law enforcement safe—perhaps even save officer lives.

On Dec. 1, 2006, officers were forced to fire on a Wilmington, N.C. teenager, killing him, after serving a warrant on his home for assault and theft. The officers went to the residence with heavily armed backup because of a picture they had seen on the Internet of the teen and two friends posing with an assault rifle, shotgun, and two pistols.

Investigators must be properly educated on securing evidence because of the complex technologies that are involved in web-based crime. Law enforcement should undergo training before attempting online investigations.

Only approximately a fourth of law enforcement agencies are properly trained for online investigations. Such training can be expensive, but there are free and low-cost options available. Agencies should contact their local Internet Crimes Against Children (ICAC) Task Force (www.icactraining.org), the National White Collar Crime Center (www.nw3c.org), and the ROCIC Training Department to inquire about applicable training opportunities and funding.

Once incriminating information is found, many officers have difficulty working with MySpace.com and other sites to subpoena private information from users (public information useful for prosecution can and should be saved by officers viewing it). To address that problem, Cyberlawenforcement.org has written a thorough Law Enforcement Investigators Guide that deals with the specifics and best ways of approaching MySpace.com for purposes of investigation.

**Conclusion**

MySpace.com and sites like it may be useful for criminals, but they can also be used by law enforcement as tools for turning the tables. Law enforcement familiarization with the technology and legal guidelines for law enforcement use is essential.

A large part of the problem is that sexual predators, gang members, and other criminals feel like they are safer using the Internet than any real-world scenario. That paradigm is beginning to shift, however. Myspace.com continues to step up security measures in the interest of public safety. Recently, Hemanshu Nigam, Myspace.com’s chief security officer (and a former federal prosecutor) said that the site would develop technologies to help block convicted sex offenders from access by screening their names and physical descriptions through an automated database. The system will then alert employees to possible matches.

Increased police presence online and increased public awareness of online dangers can erase the advantages of Internet-related crimes and lead to an increased number of arrests for cyber criminals.
Sources of Information

• Detective Lee Rehm, Juvenile and Gang Investigations, Port St. Lucie, Fla. Police Department; Director of Intelligence, Florida Gang Investigators Association

• Parry Aftab, Esquire, Executive Director, Cyberlawenforcement.org, Wiredsafety. org, Stopcyberbullying.org


Special Research Reports by ROCIC Publications

Accessible to RISS member agencies on the ROCIC secure Intranet website. Complete listing of ROCIC Bulletins, Special Research Reports, User’s Guides, and Training Conference Reports at http://rocic.rriss.net/publications.htm

- The International Driver’s Permit and the Myth of the International Driver’s License
- Auto Theft in the 21st Century
- Crowd Control: Dynamics, Psychology, Law Enforcement Tactics
- Jamaat ul-Fuqra: Gilani Followers Conducting Paramilitary Training in U.S.
- Khat: Trafficking in Foreign Plant Linked to Terrorist Financing
- Active Shooter: Protecting the Lives of Innocents in Shooting Situations
- Terrorism Threat Assessment for Large Facilities
- Check 21: New Banking Technology Challenges Law Enforcement
- ICE: Crystal Methamphetamine: Imported High-Purity Meth Replacing Domestic Lab Output
- Meth Lab Safety Issues: How to Protect Law Enforcement, First Responders, and the General Public from the Dangers of Clandestine Methamphetamine Labs
- CERT (Community Emergency Response Team): Civilian Support for First Responders
- Taxing Illegal Drugs: States Attacking Profit Motive of Dealers
- Diplomatic Immunity: Rules of Engagement for Law Enforcement
- Violence Against Law Enforcement: Law Enforcement Officers Murdered, Accidentally Killed, Assaulted in the Line of Duty
- Mara Salvatrucha (MS-13): Violent Street Gang with Military Background
- Indicators of Terrorist Activity: Stopping the Next Attack in the Planning Stages
- Internet Fraud: Techniques Used to Scam Online Consumers
- DXM: Teens Abusing Cough Medicine Risk Brain Damage, Death
- RISS Activity Report for G-8 Summit
- Mail Center Security
- Safety & Security for Electrical Infrastructure: Protecting Law Enforcement and the Public in Emergency Situations
- Crisis Response Report: Terrorist Attacks & Natural Disasters
- Eco Terrorism: Extremists Pose Domestic Threat
- Cold Case Units: Turning up the Heat
- Gypsies and Travelers
- User’s Guide to ATIX: Automated Trusted Information Exchange
- DNA: Law Enforcement’s New Investigative Tool
- False ID: National Security Threat
- Salvia Divinorum: Herbal Hallucinogen Raises Law Enforcement Concerns
- Smallpox: The Deadly Virus
- Human Trafficking: International Criminal Trade in Modern Slavery
- Network Security: Safeguarding Systems Against the Latest Threats
- Dirty Bombs: Radiological Dispersion Devices
- Ethics in Law Enforcement
- Law Enforcement Officers and Safety
- Computer Forensics: Following the Electronic Trail
- Huffing: Teens Abusing Inhalants
- RISSLeads Bulletin Board: Information in an Instant
- Bioterrorism
- Criminal Intelligence: Its Use in Law Enforcement in Our Changing World
- Terrorism: Defending the Homeland
- Law Enforcement and the Mentally Ill
- Civil Disorder: Preparing for the Worst
- Ecstasy: Harmless Party Drug Or Dangerous Trend?
- Heroin: More Purity For Less Money
- OxyContin Abuse Explodes In Southeast
- Just Say NO To Telemarketers
- School Security Crisis Response Manual
- XML: Communications Through Connectivity
- Credit Card Security Features
- Stop Phone Cramming: Check Your Phone Bill
- Shaken Baby Syndrome: What To Look For, What To Do
- Children and Internet Safety
- RAVES: When It’s More Than A Party
- Identity Theft: From Low Tech to High Tech
- Hoaxes and Legends: How to Detect Hoaxes on the Internet
- Truce or Consequences: Motorcycle Gangs Talking to Each Other
- Child Pornography: Protecting the Innocent
- Meth Threat: Seizure of Labs by Untrained Personnel Recipe for Death and Destruction
- Illusion and Confusion: The Crime and Culture of Irish Travelers
- Date Rape Drugs: Rohypnol, GHB Gaining Popularity in Southeast, Southwest
- Security Threat Groups in Prison

ROCIC has been serving its criminal justice members since 1973, and served as the prototype for the modern RISS (Regional Information Sharing Systems) Centers.

ROCIC serves more than 180,000 sworn personnel in over 1,800 criminal justice agencies located in 14 southeastern and southwestern states, Puerto Rico, and the U.S. Virgin Islands.

ROCIC provides a variety of services, free of charge, to its criminal justice member agencies:
- Centralized law enforcement databases with connectivity among law enforcement agencies and the RISS Centers using the RISS Nationwide Intelligence Network.
- Analytical processing of criminal intelligence, including phone tolls and document sorts
- Loaning of specialized, high-tech surveillance equipment and vehicles
- Publications, including criminal intelligence bulletin
- Specialized training and membership & information exchange
- Use of investigative funds
- On-site personal assistance by law enforcement coordinators

© 2006 ROCIC • This publication was supported by Grant No. 2005-RS-CX-0002, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The Office of Justice Programs also coordinates the activities of the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency, and the Office for Victims of Crime. This document was prepared under the leadership, guidance and funding of the Bureau of Justice Assistance (BJA). Office of Justice Programs, U.S. Department of Justice in collaboration with the Regional Organized Crime Information Center (RODIC). The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice. Regional Organized Crime Information Center and ROCIC are protected by copyright laws.