Cmdr. Dave Pettinari
Pueblo County Sheriff's Office
davepet@cops.org

Cyberstalking investigation and prevention

Cyberstalking, a relatively new form of electronic crime, affects victims who are mostly invisible, and its violence is primarily what is said, and not what is eventually done.

Even so, too often online harassment escalates into real-life stalking, where its victims are largely female, and who occasionally become victims of homicide that started out as online "following" and badgering.

Even if it does not get to that point, cyberstalking in and of itself can be as frightening and as real as being followed and watched in your neighborhood or in your home.

To prevent this unnecessary worry and fear among Internet users, law enforcement is stepping up its efforts to educate and make people aware of this crime and its potential. Even so, not all law enforcement agencies respond aggressively to allegations of online stalking, for a variety of reasons.

Typical of other types of victims, the majority of cyberstalking victims do not report the incidents to law enforcement either because they feel that a criminal offense has not yet occurred, or because they feel that law enforcement will not take them seriously. In addition, most law enforcement agencies have not had the training to recognize the serious nature of cyberstalking, or on how to investigate these offenses. Unfortunately, some yet-to-be-enlightened officers have recommended to victims that they either turn off their computers, or that they call law enforcement again if the cyberstalkers confront or threaten them offline, in person.

Three areas where an online user is vulnerable are primarily where the user interacts with others:

1. **Live chat or Internet relay chat (IRC),** where users can talk "live," or type messages to one another in real time. This makes it easy to target other people, which makes IRC and chat the most common places for cyberstalking.
2. **Usenet newsgroups**, the next most common place where cyberstalkers prey because people exchange messages in a group.
3. **E-mail.** E-mail harassment usually is an outgrowth of and a continuation of initial contact in chat servers or Usenet newsgroups.

Cyberstalking can take many forms. One of the most common forms of harassment is unsolicited hate mail, or obscene or threatening e-mail. A cyberstalker can also cause a lot of havoc in a chat group through flooding a target's Internet chat channel to disrupt conversation. A cyberstalker can also post messages in newsgroups to start malicious rumors. More complex forms of harassment include mail bombs, sending the target a devastating virus, or spamming the target with electronic junk mail.

Any of these forms of cyberstalking can easily escalate into real-life stalking through threatening phone calls, property vandalism, threatening mail, or in-person physical attacks.

Stalkers and victims can e any:

- Age

- Gender
- Race
- Socioeconomic group
- Educational level
- Occupational group
- Religious group

How serious is cyberstalking?

Cyberstalking shares important characteristics with offline stalking. Many stalkers - online or off - are motivated by a desire to control their victims. The majority of cyberstalkers are men and the majority of their victims are women, although there have been reported cases of women cyberstalking men and of same-sex cyberstalking.

Since cyberstalking does not involve physical contact, some misperceive this criminal attempt as something much tamer and less threatening than physical stalking. This is not necessarily true. As the Internet becomes entwined with our personal and professional lives, stalkers can take advantage of the ease of communications as well as increased access to personal information. Given the enormous amount of personal information available through the Internet, a cyberstalker can easily locate private information about a potential victim with a few mouse clicks or keystrokes.

Other things that pave the way for a cyberstalker are the often anonymous character of the Internet, and the practiced use of non-confrontational and impersonal communications. A potential stalker may be unwilling or unable to confront a victim in person or over the telephone, but he or she may have little hesitation about sending the victim harassing or threatening electronic communications.

Finally, just as in physical stalking, online harassment and threats may be a prelude to physical violence or serious property damage. In that sense, they must all be taken seriously on the first report by the victim.

Similarities and differences between online and offline stalking

Similarities

- While stranger stalking occurs in the real world and in cyberspace, the majority of cases involve stalking by former intimates.

- Most stalkers are men, most victims are women.

- Stalkers are generally motivated by the desire to control the victim.

Differences

- While offline stalking generally requires the perpetrator and the victim to be located in the same geographic area, cyberstalkers may be located across the street or across the country.

- Electronic communications technologies make it much easier for a cyberstalker to encourage third parties to harass or threaten a victim. For example:

    - The cyberstalker might impersonate the victim and post inflammatory messages to bulletin boards or in chat rooms, causing viewers of that message to send threatening messages back to the victim who they believe sent them the offending messages.

- A stalker may post a controversial or enticing message on the board under the name, phone number, or e-mail address of the victim, resulting in subsequent responses being sent to the victim.

Each message -- whether from the actual cyberstalker or others -- will have the intended effect on the victim, but the cyberstalker's effort is minimal. With an electronic buffer between him and his victim, the cyberstalker feels more comfortable in engaging than he would physically confronting his victim. And the lack of direct contact between the cyberstalker and the victim can make it difficult for law enforcement to identify, locate, and arrest the offender.

Actual cyberstalking incidents

In the first successful prosecution under California's new cyberstalking law, prosecutors in the Los Angeles district attorney's office obtained a guilty plea from a 50-year-old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances.

The suspect terrorized his 28-year-old victim by impersonating her in various Internet chat rooms and online bulletin boards where he posted, along with her telephone number and address, messages that she fantasized about being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her. The former security guard pleaded guilty in April 1999 to one count of stalking and three counts of solicitation of sexual assault.

Another recent incident demonstrates how the lack of law enforcement training and expertise can frustrate cyberstalking victims. A woman complained to a local police agency that a man had posted information on the web claiming that her nine-year-old daughter was available for sex. The web posting included their home phone number with instructions to call 24 hours a day. That complaint, too, was met with quizzical looks and shrugging of shoulders.

Anonymity emboldens cyberstalkers

A cyberstalker's true identity can be concealed by using different Internet service providers and by adopting different screen names. More experienced stalkers can use anonymous remailers that make it all-but-impossible to determine the true identity of the source of an e-mail.

Anonymity gives the cyberstalker a definite advantage in that, without the target knowing, he could be around the corner, in the next cubicle at work, or in another state. The cyberstalker could be a former friend or lover, a total stranger met in a chat room, or a teenager playing a practical joke.

Knowing his or her victims are unable to identify the source of the harassment or threats makes the cyberstalker bolder, encouraging him or her to continue the harassment. This makes many perpetrators more willing to continue pursuing the victim not only at work, but at home, with all the information in the world about the target. Numerous websites provide personal information, including unlisted telephone numbers and detailed driving directions to a home or office. For a fee, other websites will provide social security numbers, financial data, and other personal information. This is the type of information that can easily get someone killed, as happened to Amy Boyer, whose shooter purchased her Social Security number from the Docusearch site.

The challenge of anonymity

Another complication for law enforcement is the presence of services that provide anonymous communications over the Internet. To be sure, anonymity provides important benefits, including protecting the privacy of Internet users. Unfortunately, cyberstalkers and other cybercriminals can exploit the anonymity available on the Internet to avoid accountability for their conduct.

Anonymous services on the Internet come in one of two forms:

1. One allows individuals to create a free electronic mailbox through a web site. While most entities that provide this service request identifying information from users, these services almost never authenticate or confirm this information. Payment for these services is typically made in advance through the use of a money order or other non-traceable form of payment. As long as payment is received in advance by the ISP, the service is provided to the unknown account holder.

2. The other involves mail servers that purposefully strip identifying information and transport headers from electronic mail. By forwarding mails through several of these services serially, a stalker can nearly perfectly "anonymize" the message.

Both these services make it relatively simple to send anonymous communications, while making it difficult for victims, providers, and law enforcement to identify the person or persons responsible for transmitting harassing or threatening communications over the Internet.

Problems with jurisdiction and statutory authority

The outcome for a person victimized by cyberstalking may vary considerably depending on where the person lives and the cyber skills of the officers at the agency that the victim would report the stalking to.

In one case, a couple received numerous harassing phone calls after being stalked on the Internet, and reported the problem to the local police agency on numerous occasions. This particular agency advised the couple to change their home phone number. The couple next contacted the FBI, and the FBI investigation revealed that the local police agency did not have a computer expert, nor had the investigating officer ever been on the Internet. The local agency's lack of familiarity and resources may have resulted in a failure to understand the seriousness of the problem and the options available to law enforcement to respond to such problems.

This is not an isolated case. In fact, many local law enforcement agencies and their officers do not have the training or expertise to recognize the magnitude of the problem in their jurisdictions.

Some state and local agencies also have been frustrated by jurisdictional limitations. In many instances, the cyberstalker may be located in a different city or state than the victim, making it more difficult (and, in some cases, all but impossible) for the local authority to investigate the incident. Even if a law enforcement agency is willing to pursue a case across state lines, it may be difficult to obtain assistance from out-of-state agencies when the conduct is limited to harassing e-mail messages and no actual violence has occurred. A number of cases have been referred to the FBI and U.S. Attorney's offices because the victim and suspect were located in different states and the local agency was not able to pursue the investigation.

The lack of adequate statutory authority also can limit law enforcement's response to cyberstalking incidents. At least 16 states have stalking statutes that explicitly cover electronic communications, and cyberstalking may be covered under general stalking statutes in other states. It may not, however, meet the statutory definition of stalking in the remainder. In many cases, cyberstalking will involve threats to kill, kidnap, or injure the person, reputation, or property of another, either on or offline and, as such, may be prosecuted under other federal or state laws that do not relate directly to stalking.

Finally, federal law may limit the ability of law enforcement agencies to track down stalkers and other criminals in cyberspace. In particular, the Cable Communications Policy Act of 1984 (CCPA) prohibits the disclosure of subscriber records to law enforcement agencies without a court order and advance notice to the subscriber (See 47 U.S.C. 551(c), (h)). As more and more people turn to cable companies for Internet services, the CCPA is posing a significant obstacle to the investigation of cybercrimes, including cyberstalking.

For example, under the CCPA, a law enforcement agency investigating a cyberstalker who uses a cable company for Internet access would have to provide the person notice that the agency has requested his or her subscriber records, thereby jeopardizing the criminal investigation. While it is appropriate to prohibit the indiscriminate disclosure of cable records to law enforcement agencies, the better approach would be to harmonize federal law by providing law enforcement access to cable subscriber records under the same privacy safeguards that currently govern law enforcement access to records of electronic mail subscribers under 18 U.S.C. 2703. In addition, special provisions could be drafted to protect against the inappropriate disclosure of records that would reveal a customer's viewing habits.

The laws against stalking

State laws that protect stalking victims

All states except Maine have enacted anti-stalking laws. California enacted the first anti-stalking statute in 1990, primarily in response to the public outcry over the stalking and subsequent murder of Rebecca Schaeffer, an actress appearing on the television sitcom, My Sister Sam. Many states have both criminal and civil anti-stalking laws.

Some online stalking statutes include Alaska's anti-stalking law, California's anti-stalking law, Penal Code Section 646.9, and Family Code Section 6320, Indiana's anti-stalking law, and West Virginia's anti-stalking law. The National Victim's Rights Center lists various other state statutes on stalking and victim's rights. Canada enacted a comprehensive anti-stalking law in 1993.

Federal laws that protect stalking victims

Currently, there are few federal laws that deal directly with stalking.

The Interstate Stalking Punishment and Prevention Act of 1996 punishes persons with a fine and/or imprisonment for crossing state lines "with the intent to injure or harass another person...or place that person in reasonable fear of death or serious bodily injury..." (18 USC § 2261A, 2261, 2262).

18 USC Section 875

The federal law on interstate communications reads:

> (a) Whoever transmits in interstate or foreign commerce any communication containing any demand or request for a ransom or reward for the release of any kidnapped person, shall be fined under this title or imprisoned not more than twenty years, or both.
>
> (b) Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than twenty years, or both.
>
> (c) Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.

> (d) Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both.

Two laws authorize grants for law enforcement agencies to develop programs addressing stalking and for states to improve the process for entering stalking-related data into local, state and national crime information databases such as the National Crime Information Center. (42 USC §§ 3796gg, 14031)

Another law requires a training program for judges to ensure that when they issue orders in stalking cases, they have all the available criminal history and other information from state and federal sources. (42 USC § 14036)

The Drivers' Privacy Protection Act, 18 U.S.C. Chapter 123, Sections 2721 - 2725, prevents state motor vehicle departments from releasing personal information about any individual unless that department has permitted the individual an opportunity to opt out of disclosure.

42 U.S.C. Section 14038 requires the U.S. Attorney General to compile information about stalking as part of the National Incident-Based Reporting System (NIBRS).

Statutes that require a showing of a "credible threat" may be problematic in the prosecution of stalking. Stalkers often do not threaten their victims overtly or in person; rather, they engage in conduct that, when taken in context, would cause a reasonable person to fear violence.

In the context of cyberstalking, a credible threat requirement would be even more problematic because the stalker, sometimes without the victim knowing, may be located a great distance away and, therefore, the threat might not be considered credible. The better approach, codified in the federal interstate stalking statute, 18 U.S.C. 2261A, is to prohibit conduct that places a person in reasonable fear of death or bodily injury.

Legislation to prohibit stalking via electronic mail has been introduced in Congress.

The National Center for Victims of Crime has additional information on federal and state laws at its web site www.ncvc.org/law/fedstalk.htm.

What evidence must a victim put forth to prove stalking?

Many states' anti-stalking criminal codes provide that someone is a stalker if he willfully and repeatedly follows, communicates, or harasses another and/or makes a "credible threat" to place the victim or the victim's immediate family in fear for their safety.

In many states, the behavior must be "repeated," meaning it has to happen more than once either to constitute criminal harassment or behavior that the civil courts can address.

Many states provide, however, that if the stalking is prowling a place where you live, work, or visit, then one stalking instance may be sufficient to commence criminal or civil proceedings.

In some states, like California, you need not prove your stalker had the intent to carry out his threat. In Canada, you need not prove your stalker meant to scare you, only that you were scared. You do, however, need to prove your fear is reasonable.

Preservation of evidence

Preservation of evidence is a critical issue when it comes to stalking. Although harassment online usually leaves an electronic trail, the trail leads to a computer rather than an individual. Establishing who was using that computer terminal at that particular time is not easy.

Another issue regarding evidence is that stalking targets often destroy evidence when they receive it. They need to not only print out a copy of the correspondence, but maintain the digital copy so that headers can be revealed to trace the offending communication.

Restraining Orders

Stalking victims can usually obtain a restraining order from a local civil court. These orders, which may be temporary or permanent, generally require the stalker to stay a certain distance from the target and to cease communication with the victim. If the stalker violates the civil court's order, he can be held in contempt of court and could be fined or imprisoned. Civil courts have only recently become sensitive to the need for restraining orders in stalking situations. It is at the judge's discretion whether to grant or deny a request for a restraining order. The drawbacks of a restraining order is that it is usually limited to the court's jurisdiction, it is enforced only after a violation, and the restraining costs money, time, and legal counsel to obtain.

Vulnerabilities, and dealing with the threat

Protecting oneself from cyberstalking is made much easier once computer users become aware of the different ways cyberstalking can occur.

- **E-mail.** With an e-mail account, it is recommended that the user consider a gender neutral e-mail address or username. If the user's e-mail address reads "sexigal@domain.com," then she is likely to gain the attention of online stalkers. It might be the user's intention to "play," but people often judge a computer user's character and intentions online based on the person's username. Even a username like JaneDoe@domain.com, for example, is more likely to be targeted than JDoe@domain.com, for the simple reason that the vast majority of cyberstalkers are on the lookout for female targets.

  - **It would help if the computer user chooses an unusual password** and changes it regularly. The best passwords don't spell anything and don't follow a logical pattern. .If the user's chosen username is "wizard," the user is making it easy for someone to break into his or her account if the user chooses "spell," "wand," "cat," or even "abracadabra" as the password. Users should make their passwords at least seven letters long and ensure that it includes numbers mixed with meta-characters: Example: "s*2wt#e%" . Users should never tell another person what their password is.

- **Chat.** Users can reduce their risks by using a good IRC (Internet relay chat) client. Two highly recommended programs are mIRC if you use a personal computer and IRCLE if you use a Mac. These two chat clients are recommended because they enable the computer user to both protect themselves and also to perform rapid analysis of someone if they are harassing. Chat clients that do not give a user these capabilities should be avoided.

  - **Users should also find a chat network where there is an Acceptable Use Policy** (no harassment permitted) and where that AUP is enforced well by the IRC administration. A good chat network has online assistance only a message away. To check a network, as soon as you sign on, type your nickname. If you don't get any response, or you get an incoherent message you will have limited protection and no way to trace a cyberstalker should he decide to make you his victim.

- **Usenet newsgroups. Users should consider using an anonymous remailer,** or e-mail alias service, to post messages. This prevents drawing unwelcome attention to yourself if you post messages, which results in your sharing your e-mail address with others. While posts are often deleted from newsgroup servers after a short period of time, posts are often stored in the Usenet's archives, which means anyone at a later date can read all the posts you ever made by using a newsgroup search engine. With an anonymous remailer this danger is eliminated.

In summary, the types of threats one faces in these various arenas on the Internet include:

1. Unsolicited e-mail
2. Live chat harassment
3. Hostile Usenet postings
4. Spreading vicious rumors
5. Leaving abusive messages on site guest books
6. Impersonation of the user online
7. Electronic sabotage, (sending viruses, etc.)
8. Threatening phone calls
9. Threatening mail
10. Vandalism of property
11. Physical attack

Remember, the goal of a cyberstalker is control. A potential victim's task is to reverse this situation by keeping control of whom they communicate with on the Internet.

Investigation

What are you looking for?

- Elements
- Corroboration
- Inconsistencies
- Potential defenses
- Other crimes or victims

Elements

- Repeated following or harassing
- Threat placing the victim in reasonable fear
- Intent to place the victim in fear

Corroboration

- **Physical evidence:** letters, e-mail phone messages, items sent by the suspect, store videos
- **Witnesses:** Neighbors, co-workers, family members, friends
- **Records:** phone records, receipts, credit card bills, etc.
- **Suspect statements**
- **Photographs of items vandalized, damaged, etc.**

- **Fingerprints**
- **Surveillance (**stalking the stalker)

Inconsistencies

- No corroboration -- witnesses, lost documentation, erased messages
- Victim contact with suspect (obtain both defendant and victim's phone records)
- Hidden motives or bias (false victimization)

False victimization

- Victim sets up stalking scenario
- 2% to 5% of all stalking cases
- Conscious or unconscious desire to be placed in the role of a victim

Alibi

- Obtain documentary evidence: work logs, credit-card bills, DMV, receipts

Potential defenses

- Diminished actuality: alcohol, drugs, mental illness
- Lack of intent to place the victim in fear
- First Amendment

Legitimate purpose

- Private investigators
- Divorce/custody issues
- Ongoing civil dispute

Lack of intent to place victim in fear

- Warnings by police, family members, the victim
- Restraining order
- Victim's conduct towards the defendant when approached or phoned
- Prior arrests for R/O violations, stalking, etc.

First Amendment

The question in every case is whether the words are used in such circumstances and are of such a nature as to create a clear and present danger.

Interview Victim

- In person -- NOT on the phone
- Always have investigator or another person present
- If possible, tape or video record the interview

Other crimes

- Kidnapping/false imprisonment
- Assault/battery
- Vandalism

- Criminal trespass
- Burglary
- Child/pet abuse
- Telephone harassment
- Possession of a firearm
- Witness intimidation

Questions

- What is the nature of the relationship?
- When did the relationship begin?
- Describe the relationship from beginning to end.
- Ws there any mental or physical abuse during the relationship?
- Is the victim aware of any other acts of violence in the suspect's background?
- Does the suspect have a criminal background? Is the victim aware of his background?
- Does the suspect own a gun?
- Does the suspect or victim have drug, alcohol, or mental problems?
- Dates, times and places of each incident.
- Description of each incident, including exact words that were used.
- Was anyone else present during these incidents?
- Are there any divorced, custody, child support, or property actions currently being litigated?
- Will the victim promise to cooperate with the police and prosecutor?
- Is there a valid restraining order in effect, served on the suspect, temporary or permanent? When does it expire?
- When was it obtained?
- Why was it obtained?
- Is the victim currently afraid of the suspect? Why?
- Does the victim believe the suspect will carry out the threat? Why?
- Are there prior police reports filed by the victim? When, where?
- What is the victim's current relationship with the suspect?
- When was the last time the victim contacted or me with the suspect?
- Does the victim or witnesses have a criminal background?

Search warrant

- Surveillance devices/catalogs
- Phone records (suspect and victim)
- Maps, letters, journals, photos, articles
- Computer/hard drive/software
- Weapons
- Receipts

Alternatives

- Watch, wait and document
- Protective/restrainingorders
- Police contact with the suspect
- Mental health system
- Federal laws
- Probation/parole violation

Federal laws

- Interstate Stalking Punishment And Prevention Act (18 USC Section 2261 (2) (A)
    - "It is a crime for any person to travel across state lines with the intent to injure or harass another person and, in the course thereof, places that person or a member of that person's immediate family in reasonable fear of death or serious bodily injury."
- 18 USC 875
    - "It is a crime to transmit any communication in interstate or foreign commerce containing a threat to injure the person of another" (includes telephone, e-mail, beepers, or the Internet) -- up to five years in prison.
    - 47 USC 223
        - "It is a crime to use a telephone or telecommunications device to annoy, harass, abuse, or threaten the person at the called number. Requires that the suspect does not reveal his name. Up to two years in prison.

Prosecution

One reason for the lack of successful prosecution of cyberstalkers is that there usually is a lack of sufficient evidence available for officials to determine "probable cause" in order to investigate further.

In addition, a person's perception is everything. "It is not the policy of the law to punish those unsuccessful threats which it is not presumed would terrify ordinary persons excessively; and there is so much opportunity for magnifying or misunderstanding undefined menaces that probably as much mischief would be caused by letting them be prosecuted as by refraining from it." (U.S. v. Jake Baker and Arthur Gonda, 890 F. Supp. 1375, 1995)

The main objective as the case is being prepared is to keep he victim safe -- before, during and after the trial. This involves educating the victim, law enforcement, and judge and jury about potential dangers and countermeasures.

Bring to the filing

- Restraining orders, temporary, permanent, proof of service (include victim's affidavit)
- Proof of prior stalking convictions (certified)
- Audio and videotapes
- Copies of letters, etc.
- Rap sheet
- Chronology of stalking activity

Restraining orders

- 25% female victims obtained R/O
- 69% said stalker violated the order

Probation/parole

- Request that suspect be paroled 35 miles from victim's last known address.
- Incorporate the terms of a restraining order into the terms of probation/parole (i.e., defendant shall have no contact with the victim either directly or through third parties).
- Electronic monitoring
- Continuing mental health treatment

Revocation of phone privileges

- Supported by victim's declaration regarding continuing harassment

Appointment of expert

- Handwriting
- Computer
- Fingerprint
- Domestic violence
- Stalking
- Workplace violence
- Drug/alcohol
- Consultant
- Bail hearing
- Trial
- Sentencing

What is the punishment for stalking?

State criminal and civil codes vary.

In California, the criminal penalty for stalking is imprisonment for up to a year and/or a fine of up to $500. If the stalker pursued the victim in violation of a previous court order, then the punishment may be two to four years' imprisonment. In Canada, stalkers may be imprisoned for up to five years.

Since stalking isn't high on the list of local criminal court activities, victims can also pursue civil remedies and ask a civil court to issue a restraining order against stalkers. In California, a victim may request to be notified 15 days before a stalker is released from prison. In addition, California state laws prohibit those convicted of stalking from owning and/or buying guns.

CYBERSTALKING PREVENTION TIPS

Regardless of our law enforcement specialty (patrol, investigations, computer crimes, administration) we encounter crime victims or potential crime victims who are concerned and want good advice on how to prevent threats such as cyberstalking. This section contains information and advice you can use to deal with actual or potential victims.

Often, stalkers are mentally unstable, paranoid, delusional, and extremely jealous, and have extremely low self-esteem. Stalkers may display selfishness, malice, and sadism, and be very cunning and arrogant. Most are anti-social, and to put it in layman's terms, are "control freaks" who enjoy manipulating other people.

The best protection against becoming a target of these people is not to reveal anything personal about yourself.

In live chat, where often the agenda calls for role-playing, watch for red flags or alarm bells. Indications that you might be in danger include someone asking where you live, whether or not you are married, what school you attend, what you are wearing right now, what you look like, and other such personal inquires. Trust your feelings regarding how much information you choose to disclose.

The three most common ways cyberstalking can start are:

1. sexual harassment
2. a flame war (an online argument that gets out of hand)

3. users who show their technological power by attacking innocent users, channels or even networks. .

Take care when turning these people away, as the are highly sensitive to rejection and humiliation, and could cause a vendetta to start against you.

The difference between a normal cyber harasser and a cyberstalker is this: the harasser moves on to others and forgets you. A stalker will come back to stalk you another day.

The major "clue" to cyberstalking, is when the stalker pushes for information regarding your personal life, private life, or life away from the 'net. A rule of thumb is: "NEVER GIVE ANY PERSONAL INFORMATION ACROSS THE INTERNET!" NEVER.

You can take these steps to protect your online privacy:

1) Never specify gender.
2) Use neutral-gender names.
3) Change your password often.
4) Edit your online profiles often.
5) Review your email headers and signatures often.
6) Use secure chat programs that do not permit tracking of your Internet service provider/
7) Use a good chat network.
8) Use standard names and non-descriptive names to avoid drawing attention to you.
9) Use an anonymous remailer.
10) Use an anonymous browser.
11) Use encryption to authenticate email.
12) Discuss privacy with your server or Internet service provider administration.
13) learn your technology

Other Internet safety tips:

1. Beware of new acquaintances who want to talk privately to you and start sending you private messages. Give any acquaintance online time to develop trust, and take the time for that trust to be shown, before disclosing personal information. REMEMBER where the "off" button is on the IRC program, or on your machine.

2. Before you arrange to meet someone face-to-face in person, you should first talk with them on a telephone, and talk to others whom they chat with. Tell them the person wants to meet you for real, and find out their opinions about the situation and about the individual. Ensure your privacy in the event that the situation turns out to be undesirable. Remember to enable your Call Blocker because the other party might have Caller ID. Or consider using a public phone. If you choose to actually meet the other person, use a visible, public place.

3. Use a private post office box. Residential addresses of post office box holders are generally confidential. However, the U.S. Postal Service will release a residential address to any government agency or to people serving court papers. The post office only requires verification from an attorney that a case is pending. This information is easily counterfeited. Private companies such as Mail Boxes Etc. are more strict and will require that the person making the request have an original copy of a subpoena. Use your private post office box address for all of your correspondence. Print it on your checks instead of your residential address. Instead of recording the address as "Box 123," use "Apartment 123."

4. File a change-of-address card with the U.S. Postal Service giving the private mail box address. Send personal letters to friends, relatives and businesses giving them the new private mailbox address.

Give a true residential address only to your most trusted friends. Ask that they not store this address in rolodexes or address books that could be stolen.

5. Obtain an unpublished and unlisted phone number. The phone company lists names and numbers in directory assistance (411) and publishes them in the phone book. Make sure you delete your information from both places. Don't print your phone number on your checks. Give out a work number when asked. This will also prevent your phone numbers from being listed in free Internet phone search databases, which could give you away to a stalker.

6. Order complete Blocking. This ensures that your phone number is not disclosed when you make calls from your home.

7. Avoid calling 800, 888 and 900 number services. Your phone number could be "captured" by a service called Automatic Number Identification. It will also appear on the called party's bill at the end of the month. If you do call 800 numbers, use a pay phone.

8. Have your name removed from reverse directories. The entries in these directories are in numerical order by phone number or by address. These books allow anyone who has just one piece of information, such as a phone number, to find where you live. Reverse direct-ories are published by phone companies and direct marketers.

9. Let people know that information about you should be held in confidence. Tell your employer, co-workers, friends, family and neighbors of your situation. Alert them to be suspicious of people inquiring about your whereabouts or schedule.

10. Do not use your home address when you subscribe to magazines. In general, don't use your residential address for anything that is mailed or shipped to you.

11. Avoid using your middle initial. Middle initials are often used to differentiate people with common names. For example, someone searching public records or credit report files might find several people with the name, Jane Doe. If you have a common name and want to blend in with the crowd, don't add a middle initial.

12. When conducting business with a government agency, only fill in the required pieces of information. Certain government agency records are public record. Anyone can access the information you disclose to the agency within that record. Public records such as county assessor, county recorder, DMV and business licenses are especially valuable finding tools. Ask the agency if it allows address information to be confidential in certain situations. If possible, use a post office box and do not provide your middle initial, phone number or your Social Security number. If you own property or a car, you may want to consider alternative forms of ownership, such as a trust. This would shield your personal address from the public record.

13. Put your post office box on your driver's license. Don't show your license to just anyone. Your license has a lot of valuable information to a stalker.

14. Don't put your name on the list of tenants on the front of your apartment building. Use a variation of your name that only your friends and family would recognize.

15. Be very protective of your Social Security number. It is the key to much of your personal information. Don't pre-print the SSN on anything such as your checks. Only give it out if required to do so and ask why the requester needs it. The Social Security Administration may be willing to change your SSN. Contact the Social Security Administration for details.

16. Alert the three credit bureaus -- Experian, Equifax and Trans Union -- to your situation. Ask them to "flag" your record to avoid fraudulent access.

17. If you are having a problem with harassing phone calls, put a beep tone on your line so callers think you are taping your calls. Use an answering machine to screen your calls, and put a "bluff message" on your machine to warn callers of possible taping or monitoring. Be aware of the legal restrictions on taping of conversations.

18. If you use electronic mail and other online computer services, change your e-mail address if necessary. Do not enter any personal information into online directories.

19. Keep a log of every stalking incident, plus names, dates and times of your contacts with law enforcement and others. Save phone message tapes and items sent in the mail.

20. Consider getting professional counseling and/or seeking help from a victims support group. They can help you deal with fear, anxiety and depression associated with being stalked.

21. Report the incidents to law enforcement. Consider getting a restraining order if you have been physically threatened or feel that you are in danger. When filed with the court, a restraining order legally compels the harasser to stay away from you or be arrested. Be aware that papers filed for a restraining order or police report may become public record. Put minimal amounts of information and only provide a post office box address. You should contact an attorney or legal aid office if a restraining order becomes necessary. (Note: Some security experts warn that restraining orders sometimes lead to violence).

22. For your own protection, carry pepper spray and a car phone or cell phone. Carry a Polaroid, digital or video camera.

23. Never verify anything, like your home address, over the phone.

24. Don't flirt online, unless you're prepared for the consequences.

25. Save offending messages and report them to your service provider

26. Get out of a situation online that has become hostile. Log off or surf elsewhere.

DEALING WITH A CYBERSTALKER

It is important to differentiate between inconvenient or mildly annoying conversations and cyberstalking. The main features of online stalking are systematic and malicious harassment, involving physical threats, and usually involving an attempt to locate your address and telephone number.

If you are being cyberstalked, here is a list of options for you to consider:

Ignore the stalker

Your first and probably your best response to online harassment is to ***IGNORE IT***, and to seek ways to ***AVOID IT***. If you rush head-first into a confrontation, you risk starting a "flame war," which can rapidly escalate into all types of harassment, including hate mail.

1) Take no notice of the person, and ignore their comments. Silence can be your best defense.

2) Use the IGNORE box or command, if you have one. Put his IP number in the IGNORE box, or you can use the ignore command:

```
/ignore (username)
```

3) Use the Silence command. The silence command is better in that it stops all communications from a designated address at the server level, so signals never even reach you. Generally this is done: /quote silence+*!*username@hostname.net or com. This technique varies from server to server, check with your Internet service provider for the exact command to use.

6) You can also avoid a harasser by going invisible and changing your nickname while you are invisible. To do this type: /mode (name) +i and then type: /nick (new name) Once you are invisible, the harasser cannot see your new nickname unless he or she is on the same
channel as you. Now you can set up a new channel, make your channel secret, prevent messages from coming in from outside the channel, and make it "invite only." You do this by issuing the /join3channelname command and then a /mode command for the channel combining three codes: +s +n +i . So, your command line reads:

```
 /join #mychannel
/mode #mychannel +sni
```

Now all you have to do is /msg your friends and invite them to your new secure channel (/invite nick) and you can continue without your harasser.

There are also various other options that are too numerous to list, such as changing your newsgroups, deleting your postings from newsgroups, and removing www.guestbook options.

More information for protection

To obtain a guide for stalking victims, write or call the National Center for Victims of Crime
2111 Wilson Blvd.
Ste. 300, Arlington, VA 22201
Phone: (800) FYI-CALL or (703) 276-2880
Web: www.ncvc.org

The National Organization for Victim Assistance (NOVA) is a nonprofit referral center. Contact them at:

NOVA
1757 Park Rd. N.W.
Washington, D.C. 20010
Phone: (202) 232-6682
Hotline: (800) 879-6682
E-mail: nova@try-nova.org
Web: www.try-nova.org

National Domestic Violence Hotline -- (NDVH helps victims find safe houses.)
(800) 799-SAFE, (512) 453-8117
Web: www.ndvh.org
E-mail: ndvh@ndvh.org.

Other helpful web sites:

www.stalkingbehavior.com

www.lovemenot.org

www.stalkingrescue.org

www.stalkingvictims.com

www.privacyrights.org

www.antistalking.com

www.ncjrs.org/victstlk.htm

www.p3p.com/features/stalker.shtml

www.gdbinc.com

Security Recommendations For Stalking Victims

Residence Security

1. Be alert for any suspicious people.

2. Positively identify callers before opening doors. Install a wide-angle viewer in all primary doors.

3. Install a porch light at a height that would discourage removal.

4. Install deadbolts on all outside doors. If you cannot account for all keys, change door locks. Secure spare keys. Place a dowel in sliding glass doors and all sliding windows.

5. Keep garage doors locked at all times. Use an electric garage door opener.

6. Install adequate outside lighting.

7. Trim shrubbery. Install locks on fence gates.

8. Keep your fuse box locked. Have battery lanterns in your residence.

9. Install a loud exterior alarm bell that can be manually activated in more than one location.

10. Make your phone number unlisted. Alert household members to unusual and wrong number calls. If this continues, notify law enforcement.

11. Any written or telephone threat should be treated as legitimate and must be checked out. Notify law enforcement.

12. All adult members of the household should be trained in the use of any firearm kept for protection. Store it out of reach of children.

13. Household staff, if you hire them, should have a security check prior to employment and should be thoroughly briefed on security precautions. Strictly enforce a policy of the staff not discussing family matters or movement with anyone.

14. Be alert for any unusual packages, boxes, or devices on the premises. Do not disturb these objects.

15. Maintain all-purpose fire extinguishers in the residence and in the garage. Install a smoke detector system.

16. Tape emergency numbers on all phones.

17. When away from the residence for an evening, place lights and radio on a timer. For extended absences, arrange to have deliveries suspended.

18. Intruders will attempt to enter unlocked doors or windows without causing a disturbance. Keep doors and windows locked.

19. Prepare an evacuation plan. Brief household members on plan procedures. Provide ladders or rope for two-story residences.

20. A family dog is one of the least expensive but most effective alarm systems.

21. Know the whereabouts of family members at all times.

22. Accompany children to school or bus stops.

23. Vary routes taken and time spent walking.

24. Require identification of all repair and sales people prior to permitting entry into your residence.

25. Always park in a secured garage if available.

26. Inform a trusted neighbor about your situation. Provide the neighbor with photo or description of the suspect and any possible vehicles.

27. Inform trusted neighbors of any extended vacations, business trips, and the like.

28. During vacations, have neighbors pick up mail and newspapers.

29. If you live in an apartment with on-site manager, provide the manager with a picture of the suspect. If you live in a secured condominium, provide information to the doorman or valet.

Office Security

1. Central reception should handle visitors and packages.

2. Do not accept any package unless you personally ordered an item.

3. Office staff should be alert for suspicious people, parcels, and packages that do not belong in the area.

4. Establish key and lock control. If keys possessed by terminated employees are not retrieved, change the locks.

5. Park in secured area if at all possible.

6. Have your name removed from any reserved parking area.

7. If there is an on-site security director, make him or her aware of the situation, and provide suspect information.

8. Have secretary or co-worker screen calls if necessary.

9. Have a secretary or security personnel screen all incoming mail (personal) or fan letters.

10. Be alert to anyone possibly following you from work.

Personal Security

1. Remove your home address on personal checks and business cards.

2. Place your real property in a trust, and list your utilities under the name of the trust.

3. Use a private mailbox service to receive all personal mail. Do not obtain a mail box with the United States Post Office. File a change of address card with the post office giving the mailbox address as your new address. Send postcards, instead of postal change of address cards, to friends, businesses, etc., giving the mailbox address and requesting that they remove the old address from their files and rolodexes.

4. All current creditors should be given a change of address card to the mailbox address. Some credit reporting agencies will remove past addresses from credit histories if you make a request, which will prevent your being discovered through this means.

5. File a change of address with the DMV to reflect the person's new mailbox address. Get a new driver's license with the new address on it.

6. File for confidential voter status or register to vote using your mailbox address.

7. Destroy discarded mail.

8. Phone lines can be installed in a location other than the person's residence and call-forwarded to the residence.

9. Place residence rental agreements in another person's name. The person's name should not appear on service or delivery orders to the residence.

Vehicle Security

1. Park vehicles in well-lit areas. Do not patronize parking lots where car doors must be left unlocked and keys surrendered; otherwise surrender only the ignition key. Allow items to be placed in or removed from the trunk only in your presence.

2. When parked in the residence garage, turn the garage light on and lock the vehicle and garage door.

3. Equip the gas tank with a locking gas cap. The hood-locking device must be controlled from inside the vehicle.

4. Visually check the front and rear passenger compartments before entering the vehicle.

5. Select a reliable service station for vehicle service.

6. Keep doors locked while vehicle is in use.

7. Be alert for vehicles that appear to be following you.

8. When traveling by vehicle, plan ahead. Know the locations of police stations, fire departments, and busy shopping centers.

9. Use a different schedule and route of travel each day. If followed, drive to a police station, fire department, or busy shopping center. Sound the horn to attract attention.

10. Do not stop to assist stranded motorist. Instead, phone in for help.

Your Online Setup

1) Consider a gender-neutral e-mail address (username). If your e-mail address is "sexygal@domain.com,'" then you are flashing your intention to "play." Know that people judge your character and your purpose online by your username. Choose a name that does not imply a feminine gender. The username "janedoe" is definitely feminine, whereas "jdoe" is not. Cyberstalkers tend to target feminine usernames for the simple reason that the vast majority of cyberstalkers are men looking for women.

2) Choose a good account password and change it regularly. The best passwords don't spell anything and don't follow any logical pattern. If your chosen username is "wizard," then using a password such as "spell," "wand," "cat," or "abracadabra" is logical, but not wise. Make your password at least seven letters long, as longer passwords are harder to break. NEVER TELL ANYONE your password.

3) Edit your online profile. Get familiar with "Finger" command, which is a way of looking up your username and domain and obtaining information about you from what is called your Plan file. Try out your own email address with Finger and see what comes up. If you don't like what you see, change it. Take out personal information so no one can find out about you. You can try a finger search on yourself by going to one of the following sites on the WWW: http://www.rickman.com/finger.html or http://www-bprc.mps.ohio-state.edu/cgi-bin/finger.pl

4) Review your e-mail signature and e-mail headers. What does your e-mail signature say about you? Your e-mail signature is added to every piece of e-mail you send. To check yours, send yourself some e-mail and then look at the headers at the top and the signature at the bottom. Make sure this does not give away your home telephone number or any other personal details. You can configure the e-mail headers yourself.

3) Use a good IRC client to chat. Two good ones are mIRC for a personal computer and IRCLE for a Mac. Both support a full range of IRC commands and procedures. They both enable you to protect yourself and perform rapid analysis if someone is harassing you. Many chat clients do not permit IRC commands - these are best avoided. You can get mIRC and IRCLE from: mIRC - http://www.mirc.co.uk IRCLE - http://www.xs4all.nl/~ircle

4) Chat on a good IRC network where there is a good "Acceptable Use Policy" enforced by the IRC administration. Make sure the chat network supports all IRC commands you need to protect

yourself. Too, a good chat network has online assistance only a message away. To check a network, as soon as your sign on, type: /whois. If you don't get any response, or you get a message like: ***:No such nick/channel, then you have limited protection and no way to trace anyone who attacks you.

5) Consider your choice of nickname, username, realname, finger file and user info file when you set up your IRC client. Choose a username that is boring and neutral-gender. Also, it is suggested that an alternative e-mail address be used such as hotmail or netaddress (usa.net). These e-mail are limited to the server homepages and can't be traced to your local domain.

6) Consider using an anonymous remailer (or e-mail alias service) to post messages to newsgroups. Posting in newsgroups, bulletin boards, and other Usenet postings enables cyberstalkers to trace you. Many of the postings are stored in archives such as Dejanews and can be accessed for months after the posting is made. To read about anonymous remailers, visit: http://www.well.com/user/abacard/remail.html.

7) Consider using an anonymous web browser (browse the WWW by going through an anonymous Web browsing service). This will make it impossible for your web-surfing to be logged by Websites so no one will be able to pick up any information on you. Information on this service is located at http://www.anonymizer.com

8) Consider using encryption to authenticate your e-mail messages. Encryption prevents someone from impersonating you. PGP is a program often used for this type of e-mail, and is a difficult program to learn but is very valuable for authentication of e-mail. Information on this program is located at http://www.well.com/user/abacard/pgp.html.

9) Discuss your safety and privacy requirements with your Internet service provider and enlist their help and advice. Don't be afraid to discuss these issues with your local Internet provider. You are paying them to use their service, and you have a right to assistance.

10) Learn your technology. Cyberstalkers prefer to target beginners for harassment, because beginners are less likely to know what to do, and how to fight back. Never let anyone in a chat room, or by e-mail or newsgroup posting, know that you might possibly be a beginner.

11) Keep evidence of possible harassment by saving messages, or copying and pasting to self-e-mails. Archive chat logs in the event of trouble. If no trouble occurs, then discard the logs.

Other precautions you can take

- Never leave your computer logged in unattended.

- Request the privacy policy of your commercial or online service provider. Shop around for one that has a policy that protects your privacy. Many provider agreements permit e-mail to be monitored.

- Unless you use encryption such as PGP (Pretty Good Privacy), your e-mail may not be private. Therefore, limit the personal information you release online.

- Be careful posting to Usenet newsgroups. Many proprietors of online white pages obtain their personal information about you from archives of Usenet postings.

- Don't create an online biography that is available for other users.

- If your child is using commercial or online service providers, various parental control programs can prevent your child from releasing your home address, telephone number, or credit-card number in an e-mail or online posting.

-

- If you have your own domain name, create multiple mailboxes and only give out your main mailbox address to friends and colleagues.

- Save all e-mail messages that you consider harassing both in digital and hard-copy form. Contact your service provider about these messages.

Cracking Down on E-Mail Harassment

Someday, someone you make angry on the Internet could you sign you up for services you did not order, flooding your inbox with unwanted electronic communications, including offers for pornography and subscriptions to online magazines such as "Workstation Tip of the Day" and "WebShoppers Hot Products Daily."

The mechanics of the Internet – mailing services and free e-mail accounts -- make it possible to send vast numbers of anonymous messages with one keystroke – making the Internet a fertile field for those seeking to frighten or intimidate. Victims report everything from e-mail "bombs" that flood them with hundreds of messages to outright extortion and death threats.

In a variation on the old "for a good time call Sally" prank, a 30-year-old Alexandria woman discovered that her name and phone number had been posted on matchmaking and sexual Web sites, leading other Internet users to send her suggestive or obscene messages.

Often, law enforcement agencies can use existing laws against stalking and telephone harassment to go after those who abuse e-mail in this fashion. But there are a lot of things authorities can't even tough. On the Internet, where quite often "anything goes," people can be rude, crude, nasty, or act like jerks. None of these are state or federal crimes.

Cyberstalking Resources Online

CyberAngels: A volunteer group that assists victims of online harassment and threats, including cyberstalking. www.cyberangels.org

GetNetWise: Online safety and education resources for families to help kids use the Internet safely. www.getnetwise.org

International Association of Computer Investigative Specialists: IACIS is an international volunteer group of law enforcement computer crimes forensic investigators. IACIS offers training to law enforcement agencies in a wide range of computer crime investigative techniques. www.iacis.com

National Center for Victims of Crime: Provides referrals and advocacy services to victims through its toll-free national hotline. The National Center publishes bulletins on domestic violence, sexual assault, stalking, and similar topics. www.ncvc.org

National Cybercrime Training Partnership: This interagency, federal/state/local partnership, led by the Department of Justice with extensive support from the Office of Justice Programs and the National White Collar Crime Center, is developing and delivering training to federal, state and local law enforcement agencies on the investigation and prosecution of computer crime. The NWCCC web site has information: www.cybercrime.org

Privacy Rights Clearinghouse: Nonprofit consumer information and advocacy program that offers consumer advice on protecting personal privacy. PRC has a hotline to report privacy abuses and request information on ways to protect privacy. PRC fact sheets on privacy issues includes " Are You Being Stalked? Tips For Your Protection." www.privacyrights.org

Search Group, Inc.: SEARCH, the National Consortium for Justice Information and Statistics, provides assistance to state and local criminal justice agencies on a wide variety of information technology issues. SEARCH, through its National Technical Assistance and Training Program, provides comprehensive, hands-on training on computer crimes investigation at its headquarters in Sacramento, CA, and at regional training sites around the country. www.search.org

Women Halting Online Abuse (WHOA): Founded by women to educate the Internet community about online harassment, WHOA empowers victims of online harassment and develops voluntary policies that systems administrators can adopt to create an environment free of online harassment. WHOA educates the online community by developing web site resources, including the creation of a safe-site and unsafe-site list to help users make informed decisions. www.whoa.femail.com

What To Do If You Are Being Cyberstalked

- If repeated contact is not wanted, make it clear to that person that you would like him or her not to contact you again.
- Save all communications for evidence. Do not edit or alter them in any way. Also, keep a record of your contacts with Internet system administrators or law enforcement officials.
- You may want to consider blocking or filtering messages from the harasser. Many e-mail programs such as Eudora and Microsoft Outlook have a filter feature, and software can be easily obtained that will automatically delete e-mails from a particular e-mail address or that contain offensive words. Chat room contact can be blocked as well.
- Although formats differ, a common chat room command to block someone would be to type: /ignore <person's screen name> (without the brackets). However, in some circumstances (such as threats of violence), it may be more appropriate to save the information and contact law enforcement authorities.
- If harassment continues after you have asked the person to stop, contact the harasser's Internet service provider. Most ISPs have clear policies prohibiting the use of their services to abuse another person. Often, an ISP can try to stop the conduct by direct contact with the stalker or by closing the harasser's account. If you receive abusive e-mails, identify the domain (after the "@" sign) and contact that ISP. Most ISPs have an e-mail address such as abuse@(domain name) or postmaster@(domain name) that can be used for complaints. If the ISP has a web site, visit it for information on how to file a complaint
- Contact your local law enforcement agency and inform them of the situation in as much detail as possible. In appropriate cases, they may refer the matter to state or federal authorities. If you are afraid to take action, there are resources available to help you, Contact either:
  - The National Domestice Violence Hotline, 800-799-SAFE (phone); 800-787-3224 (TDD), or
  - a local women's shelter for advice and support.

Other resources

There are many resources for stalking victims:

- The National Organization for Victim Assistance, 1757 Park Rd. NW, Washington, D.C. 20010, (202) 232-6682, Email: nova@access.digex.net
- National Victim's Center, 2111 Wilson Blvd., Ste. 300, Arlington, VA 22201, (800) FYI-CALL,
- Survivors of Stalking, Inc., (813) 889-0767, e-mail: soshelp@gate.net
- How to Lose Anyone Anywhere, Stealth Publishing, 564 Fineview, Kalamazoo, MI 49004 ($16.95 includes shipping/handling), e-mail: besafenow@aol.com.
- A great site for cyberstalking laws, opinion articles, and guidance can be found at:

http://cyber.findlaw.com/criminal/cyberstalk.html

- Women Halting Online Abuse (WHOA) A great page with lots of links and help, including:
  - Online Harrassment
  - Social and Technical Means for Fighting Online Harassment
  - Gender Harassment on the Internet

  - Cyberstalking Awareness and Education
- Be Safe Online has some good articles about cyber-safety and protection against stalking.

- State Stalking Laws for all states provided by the National Victim Center.

- The CyberLaw Center's Cyberstalking page has some great legal information.

- NotVictims. This site contains lots of links and information for persons who have undergone various kinds of abuse including cyberstalking. Many links to support sites.

http://www.haltabuse.org/resource.html

Privacy Rights Clearinghouse http://www.privacyrights.org/

Jenson, Barbara, August 1996. :
http://www.law.ucla.edu/classes/archive/s96/340/cyberlaw.htm

1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR
LAW ENFORCEMENT AND INDUSTRY

http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

Home | **What's New** | **Articles** | **Links**
Library | **Staff** | **Contact Us**