Global Information Assurance Certification Paper

Cyber-stalking, Privacy Intrusion at It's Scariest
Pamela Valentine
GSEC Version 1.2b

Many crimes that are committed in the real world also occur on the Net. These include fraud and embezzlement, harassment, "stealing" an identity, and stalking. A lot of information is available about you on the Net, and an enterprising criminal can find out a lot about you and use this information to his/her disadvantage. A criminal could use basic information about you (discovered on the Net), and then engage in "social engineering"--contacting your friends, co-workers, relatives, etc.--to learn even more. Social engineering is the art of soliciting participation of a person instead of hacking into a system directly. Most often the target is information the person or victim gives without knowing it, at least until it's too late. Because even though it's a slower process, human vulnerabilities make it easier to obtain information that leads to more information via the net. But what if the target is the physical person instead of data or hardware? It's called Cyber-stalking, a serious problem that is increasingly becoming more of a threat as stalkers take advantage of the Internet and other technologies. This paper describes Cyber-stalking and what you can do, or not do, to prevent it.

What is Cyber-stalking?

Cyber-stalkers use the Internet, e-mail, or other methods of electronic communications to stalk or harass another person. Although the term 'cyber-stalking' does not involve physical contact, it is just as threatening as being stalked physically.

"Make no mistake: this kind of harassment can be as frightening and as real as being followed and watched in your neighborhood or in your home."[1] Vice President, Al Gore.

Some people believe that cyber-stalking is an intrusion but not a physical threat which is not necessarily true. A potential stalker may not be comfortable in a face-to-face confrontation but will not hesitate to use electronic communications to harass the victim.

Who is the Cyber-stalker?

Most of the stalkers are men with the victims being women. In many of the cases documented, the cyber-stalker and the victim had a prior relationship that ended bitterly. However, there also have been many instances of cyber-stalking by strangers. With the enormous amount of personal information available through the Internet, a cyber-stalker can easily locate private information about the victim with a few clicks of the mouse. With the Internet offering anonymity,

[1] Vice President Al Gore, August 1999

a cyber-stalker's identity can be concealed. Knowing that they may not ever be identified, the cyber-stalker might carry the harassment further by contacting the victim incognito.

Who is the victim?

The victims can be of any age and gender. In physical stalking, the perpetrator and the victim are located in the same geographic area but in cyber-stalking the perpetrator can be on the other side of the globe. Perpetrators obtain personal information about the victim through the Internet.

Methods of contact:

Live Chat or IRC (Internet Relay Chat): where a user talks live with other users, a common place for cyber-stalking. One incident involved a 13 year old girl who entered a teen chat room and engaged in a conversation with a user who identified himself as another teenage female. For the sake of a short story… the victim was followed from softball practice to her home and raped. The perpetrator was caught and gave the police the details of how easy it was to find the victim a state away from him. Although the victim didn't give information such as name, address, etc., she did give clues that lead the perpetrator right to her. After 30 minutes of chatting, he learned that she had softball practice every Tuesday and Wednesday after school, her team wore navy shirts, her jersey number was 22, she was the catcher, her team name was Falcons, her hair was long and blond, she was an only child and that her parents didn't get home until 6:00 pm through the week. There was only one thing left to learn, what city? Since the perpetrator was able to gain her trust through the common ground of softball, he simply asked her what city she lived and she immediately replied. All he had to do was check the city directory on the net for recreational sports and find which school falcon players attended, since the city recreation teams are formed according to school districts. He showed up at her school and followed the girls to softball practiced, looked for jersey #22, and followed her home without her even noticing.

Message boards and newsgroups: a user converses with other users by posting messages and responding to them. Sometimes the perpetrator has a strong opinion on a subject matter that strongly differs from the potential victim. A cyber-stalker can use bulletin boards to encourage third party harassment. Jayne Hitchcock's cyber-stalker found her through writers' newsgroup on the Internet. The controversy began when the cyber-stalker got angry at a statement Jayne published on the newsgroup's bulletin. Her cyber-stalker sent sexually explicit emails with forged addresses to look like they came from her. One of the emails contained her home phone number and address. Another stated that she was interested in sedo-sexual fantasies. The cyber-stalker didn't stop with Jayne… he sent emails to her husband, her literary agent and colleagues. Jayne was mail-bombed as was her friends and family.

Jayne is now the president of WHOA (Working to Halt Online Abuse), a support group for cyber-stalking victims.

In a similar case, a woman in Hollywood rejected advances made by a security guard she met at church. Gary Dellapenta got back at her through the Internet. He posted personal ads using her name that described her fantasies of being raped by an intruder in her home. Six times over the next few months men showed up at her home to make her fantasy come true. Gary Dellapenta was sentenced to six years in prison. He was the first person jailed for cyber-stalking.

IRC and Newsgroups, are common ground for new exploits and viruses. It's where hackers meet to scan IP addresses and help each other hack systems. Important steps with using IRC: (Windows-specific)

- Use a firewall and keep the rules up to date from your vendor.
- Do not accept any DCC file transfers regardless unless you absolutely know the person.
- Make sure your browser is set to NOT accept cookies and security is set to the highest setting.
- The command: */fserve 1 c:*\ will open up a fileserve to your C drive. Don't follow commands if you don't know what they will do.
- When issuing commands to *nickserv* or *chanserv*, be sure to issue them from the status window. Here is a normal nickserv identify with a password: */nickserv identify {your password}*. What happens if you forget the "/" . Everyone can see your password and change it.

Email: a user writes to anyone about anything and can also attach files to the email containing pornographic pictures, viruses, or other damaging executables such as a Trojan horse. A student from the University of San Diego sent hundred of violent and threatening emails to five female schoolmates over the course of a year. When that didn't get the girls' attention, he sent them executables disguised as jpeg files that destroyed their hard drives.

A Trojan horse is an executable program that damages data, files or hard drives. A Windows executable has extensions ("bat", "pif", "scr", "lnk", etc.). A Trojan can hide by having more than one extension. Only the last extension counts so a Trojan can hide the last extension and look something like this… pretty.jpg.exe. Remember the "Love Letter for You" Trojan? Even though users didn't recognize it, their human instinct took over and they opened it. Bad decision. Remember to unhide extensions. If you do get a Trojan, you can get fix instructions on the Internet. One site I have used is: http://www.irchelp.org/irchelp/security/.

Data brokers are people who sell information that they get mostly through government records. They sell social security numbers, employer name and address, and financial information. For a small fee they will give information

that is buried in government databases to anyone who pays. Amy Boyer was a dental assistant in New Hampshire who was killed in 1999 by a man that paid $45 for information used to track her down and kill her. Ms. Boyer was 20 years old her assailant first paid the Florida firm Docusearch for her social security number. Then he bought her employer name and address from them. Ms. Boyer was killed at work.

Laws

State and federal laws on cyber-stalking are few and weak however there are strides being made. California recently amended its stalking law to also cover cyber-stalking. Gary Dellapenta was the first person tried and prosecuted under the newly amended stalking law in California. Less than one third of the states have laws that cover stalking through the use of the Internet. Although the federal government has passed laws concerning cyber-stalking, the first amendment protects harassment via electronic communication. By definition, stalking via the Internet is not a crime. The conduct of the stalker has to be defined by a definite set of acts directed at the potential victim before a crime is actually committed. The first amendment and other legal considerations basically protect a cyber-stalker that harasses, threatens, and forces himself into the life of the victim. Under the federal law, 18 U.S.C. 875, it is a federal crime to transmit communication containing a threat to injure or harm another person when the communication device is the Internet, email, or beepers. The burden of proof of such an act is the sole responsibility of the potential victim. The anonymity of the Internet and the lack of direct contact between the cyber-stalker and the victim make it difficult for law enforcement to identify, locate, and arrest the offender. Many law enforcement agencies have created special task forces to deal with cyber-stalking. The problem is lack of proper training and technical expertise in local and federal agencies. According to WHOA, most cases of cyber-stalking are not reported to law agencies because the victim can't identify the perpetrator. Evidence from support groups supports that cyber-stalking is a growing problem in the Unites States. Currently there are more than 90 million people with access to the Internet. Ten million of those people are children. The Los Angels District Attorney's office estimates that 20% of the cases reported to their Stalking Unit were cyber-stalking cases. In New York City, the unit of Computer Investigations and Technology reports that approximately 40% of their caseload for the last few years involve cyber-stalking crimes. One ISP reported that in the last year 15 complaints per month are due to cyber-stalking. The same ISP also reported that they received virtually no such complaints one year ago.

So what can we do?

- Don't argue with other users. It's really not worth it. NEVER respond messages that make you feel uncomfortable such as ones that are sexually suggestive, obscene, aggressive, or threatening.
- Remember that you are chatting with strangers. So be careful about sharing

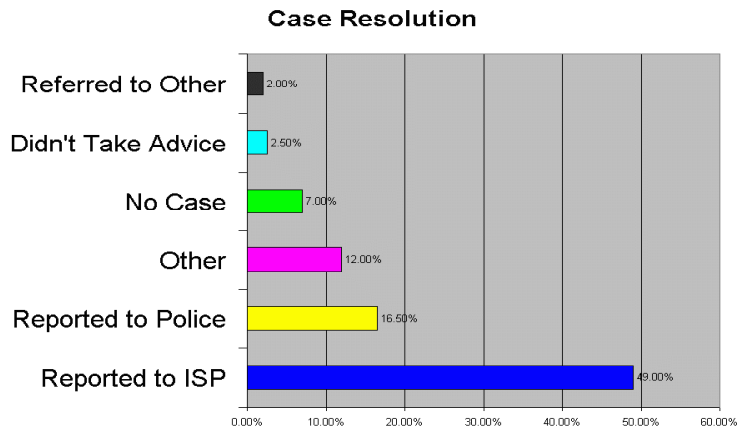
personal information about yourself.
- Use dummy email accounts for general use.
- Try not to offend others for the sake of an argument.
- Be educated. Easy victims of electronic harassment are illiterate Internet users.
- If you feel threatened, do not continue the communication and log off.
- Monitor your children's Internet use.
- Change your password often.
- Use secure chat programs that do not permit tracking of your ISP number.
- Use an anonymous browser.
- Use encryption when sending personal information via the Net.
- NEVER give out your name, phone number, address, or any other personal information on IRC.
- Keep your identity invisible by typing "/mode yournickname +I".
- NEVER accept a DCC chat or file sent from someone you don't know. This is the cause of 95% of all IRC security problems. Disable the Auto Get option.
- Don't be fooled into a false sense of security because you have an anti-virus program. They don't protect against many viruses and Trojans
- NEVER download an executable program just to see what it is - if it's a Trojan, you're in trouble.
- Use mIRC as your IRC program. It is easily configured to maintain your anonymity.

What if you are a victim?

- Report incidences of cyber-stalking to the appropriate law enforcement agency.
- Save all communications you had with the perpetrator for evidence.
- Block the email address or chat room.
- Capture and contact the perpetrator's ISP and file a complaint.

Online Harassment Statistics for 2000
Resolution of Cases[2]

[2] WHOA



Of the cases resolved in 2000:

- 49% were resolved through complaints filed with the ISP used by the perpetrator.
- 16.5% were referred to the appropriate law enforcement agency
- 2% were referred to non-law enforcement agencies
- 7% were determined not to be actual cyber-stalking cases
- 2.5% didn't take the advice of WHOA; no tracking was done on these cases to determine if they were resolved or not
- 12% were reported resolved by the victim where the harassment stopped, the victim installed a firewall to protect themselves from further attacks or they filed civil suits against the perpetrator through an attorney.

It's evident that cyber-stalking is going to increase as fast as Internet accessibility does. It has become a serious threat and should be treated as such. Take the necessary steps to protect your privacy while on the Internet.

References

CYBER-STALKING, A Real Life Problem
http://www.grafx-specs.com/News/Cybstlk.html

WHOA
http://www.haltabuse.org/scripts/errordocs/404.html
http://www.haltabuse.org/resources/stats/resolution.shtml)

"Cyber Stalking: Are You at Risk?" Security World.com
URL: http://www.securityworld.com/library/workplacetech/cyber-stalking.html

Cohen, Adam. "Internet Insecurity". Time Magazine. July 2, 2001"45-51.

Hartman, Rachel R. "Cyber-stalking and Internet Safety FAQ"
URL: http://www.sfwa.org/gateway/stalking.htm

1999 REPORT ON CYBER-STALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY
A Report from the Attorney General to the Vice President
August 1999
http://www.usdoj.gov/criminal/cybercrime/cyber-stalking.htm

Spencer, Susan. An Online Tragedy. CBS News
http://www.cbsnews.com/now/story/0,1597,175556-412,00.shtml

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event