

# **Use of the Internet to Facilitate Sexual Assault of Adolescent and Adult Victims**

Content of this module was developed primarily on the basis of material provided by the San Diego Police Department Child Abuse Unit. Additional material was provided by Special Agent Bruce M. Applin, FBI Los Angeles, Sexual Assault Felony Enforcement Team (SAFE).

The *National Center for Women & Policing* would like to gratefully acknowledge the assistance of these organizations and individuals.

Internet usage has grown exponentially over the past few years. In 1997, there were 12 million users worldwide; in 1999 there are over 300 million. By some estimates, by the year 2000, there will be 900 million users. Fifty-nine percent of Web users are in the United States. An estimated 40% of households have Internet access. Of all usage areas, "adult" interests rate second after news and information. The most common complaint concerning Web issues is child pornography (35% of all complaints). No single legal jurisdiction polices the Internet.

The Internet presents an unprecedented opportunity for law-abiding citizens. It also offers an overwhelming arena for criminals to perpetrate various types of crimes such as stalking and exploitation of adolescents in addition to providing opportunities for offenders to develop "relationships" and potentially meet unsuspecting victims.

Traditionally, preferential sex offenders assumed considerable risk in searching out victims and cohorts. On-line, the exploiter has nearly unlimited access to vulnerable prey, and can operate in virtual anonymity to all but the most expert of investigators. The Internet also provides a previously unavailable forum for people who are sexually interested in children, bondage, torture, or rape, to identify and communicate with each other. With encryption techniques, information and graphics can be transported with greatly reduced chance of detection.

On-line sexually explicit publications and photographs provide an ease of transmission and secrecy never before possible. Pornographers may encrypt photos or put them in a code that can only be viewed with special software. Unlike photocopies, the quality of the images is not degraded by multiple Internet transmissions.

To a great extent, persons entering chat-rooms and similar on-line activities are anonymous. Unlike face to face contacts, a perpetrator may assume whatever persona will best win the potential victim's trust. Time is plentiful, with no neighbors, teachers or friends to become suspicious. After hours of on-line conversation, a victim comes to trust the new "friend." Gradually, the perpetrator wears down the victim's inhibitions and fosters curiosity and intimacy. These contacts often lead to invitations to meet in person, sometimes including long-distance travel. Thus, the predator can even choose the location of the molestation or "consensual" sex. Molesters also trade names of their victims amongst themselves.

Many adolescents are exploited by adults who encourage or force them to prostitute themselves. Some of these adults are pimps, guardians or other acquaintances who take whatever money is earned; others are in it strictly as a "hobby." The Internet provides a perfect venue for adults to meet adolescents whom they may engage in prostitution, to advertise and recruit clients for their business, and to trade victims.

"Successfully Investigating Acquaintance Sexual Assault: A National Training Manual for Law Enforcement"

Developed by the *National Center for Women & Policing*, with support provided by the Violence Against Women Office, Office of Justice Programs (Grant #97-WE-VX-K004)

---

Perpetrators may continue to harass and threaten their victims, either to frighten them away from telling about their sexual contacts, or to coerce further interaction. Offenders may also continue

to trade names of their victims with cohorts for years. There have also been situations where drug facilitated sexual assaults have been photographed or video taped and placed on the Internet.

Perpetrators usually assume they are relatively invisible in the commission of their crimes. In fact, in the cyber world of crime, offenders leave more unwitting "fingerprints" and trails to follow than their counterparts in the physical world. In cyber-crime, if someone has touched it anywhere, it's recorded somewhere, and skilled forensic investigators can trace the evidence back to the perpetrator.

The virtual world of on-line interactions tends to obviate jurisdictions, time zones and national boundaries. Nevertheless, when it comes time for an investigation and arrest, the cognizant law enforcement agency still needs to be physically proximate to the offender in order to apprehend the criminal as well as to seize and investigate the involved computer and video equipment, files, information and images. Perpetrators are computer-literate and skilled at evading traditional law enforcement methodologies. This requires unprecedented collaboration and cooperation between government agencies, the Internet industry, schools, corporations, families and others.

The Internet facilitates the adoption of multiple covert "personalities," and renders normal geographic and jurisdictional boundaries meaningless. Rules and methods of evidence recovery and storage, discovery, warrants, seizures and prosecution for computer crimes are complex and changing. It is critical that investigations and operations be collaborative and coordinated amongst the many potential criminal justice agencies. Otherwise, it is possible for investigators to duplicate efforts, interfere with others' investigations, or even inadvertently investigate one another.

Undercover investigators can gain the trust of suspects with the goal of eliciting information and admissions by perpetrators that they took certain photographs. Investigators need to be familiar with Internet pornography to recognize the victims, styles, backgrounds, sources, etc., develop evidence, connect producers, develop series, execute search warrants, seize equipment and materials, and prosecute offenders.

One of the primary functions of law enforcement is to deter crime by establishing a presence in crime-prone areas so that criminals recognize that the risk outweighs the benefits of potential crime, and so that potential victims and witnesses have an immediate source to which to report. The Internet is particularly well adapted to this purpose, as it is by definition a high-speed, long distance information delivery system. Investigators can establish a crime prevention presence through their on-line persona, without compromising covert investigations conducted under other identities.

Some law enforcement agencies have home pages with hot buttons inserted, directly linking to the sites for law enforcement. This is a potential way to implement blind reporting, as described in the

chapter on victim interviewing. Victims can provide informational reports via internet without initiating a full investigation.

*What follows is briefly described information to help make sense of the terms and concepts involved in internet use. It was adapted from material provided by Special Agent Bruce M. Applin, FBI Los Angeles, Sexual Assault Felony Enforcement Team (SAFE).*

### **Types of Computer Systems**

- PC - Personal Computers (most common)
- Mac - Macintosh
- Networked System - Terminal connected to a network, common with businesses and colleges

### **Bulletin Board Services**

- Old technology
- Person calls another commuter by telephone
- Other commuter is set up to share with other users
- Person can chat with other users in private or as a group
- Exchange e-mail within the BBS
- Upload/download images and files from the BBS Library or another user connected to the BBS

### **On-Line Service**

- Special membership
- Gateway to the Internet
- Examples: America On Line, CompuServe, MSN (Microsoft)

### **What is Internet Addressing?**

In general, Internet addressing is a systematic way to identify people, computers and Internet resources. On the Internet, the term "address" is used loosely. Address can mean many different things from an electronic mail address to a URL.

### **What is an IP Number?**

- A number to identify machines on the Internet
- Unique and global
- An IP address is a unique number that identifies computers on the Internet; every computer directly connected to the Internet has one
- An IP address consists of four numbers separated by periods. Each number must be between 0 and 255.

### **What is a protocol?**

- Standard way to communicate
- When computers communicate with one another, they exchange a series of messages
- To understand and act on those messages, computers must agree on what a message means. Examples of messages include establishing a connection to a remote machine; sending or receiving e-mail; and transferring files and data
- There are different protocols for different types of network services. For example, the Internet is based on the TCP/IP

Some of the protocols used on the Internet are:

- Simple Mail Transfer Protocol (SMTP) - to send and receive electronic mail
- File Transfer Protocol (FTP) - to transfer files between computers
- Hypertext Transfer Protocol (HTTP) - to transfer information on the World Wide Web
- Network News Transfer Protocol (NNTP) - to transmit network news

### **Components of the Internet**

- World Wide Web (WWW)
- News groups (Usenet)
- File Transfer Protocol (FTP)
- Electronic Mail (E-mail)
- Chat Communications - typing, audio, video, paging

### **World Wide Web**

- Early 1990's saw the advent of HTML and the World Wide Web was born
- Collection of text, images, video files, and sounds
- Information is displayed on pages that can be read by the user

### **Internet Addressing - URL**

- Uniform Resource Locator
- Easier to remember than IP numbers

### **Web Browsers**

- Used to view Web pages
- Point and click features

### **News Groups**

- Bulletin Board-type system
- Post messages, images, movies
- Over 30,000 topics and growing daily

"Successfully Investigating Acquaintance Sexual Assault: A National Training Manual for Law Enforcement"

Developed by the *National Center for Women & Policing*, with support provided by the Violence Against Women Office, Office of Justice Programs (Grant #97-WE-VX-K004)

---

- News reader needed to read

## **FTP Applications**

FTP (File Transfer Protocol) is the ability to send and receive files from other computers  
Numerous FTP applications exist with different features

## **Electronic Mail (E-mail)**

- E-mail is perhaps the most popular use of the Internet
- Exchange text, images, or programs to other users
- Receive subscription information from special resources like list serves
- E-mail accounts are assigned by the Internet Service or On-line service company
- Anonymous e-mail accounts can be accessed by going to a specific Web site or a e-mail client that can download multiple accounts
- An Internet electronic mail, or e-mail address is used to identify a person (or persons) and a computer for purposes of exchanging electronic mail messages

## **Chat Communications (Three basic Types)**

- Chat - Type messages between two users or a group
- Voice - Communications between two users or a group, can include type communications
- Video - Communications between two users or a group, can include voice and or type communications
- Pager System - Used on certain programs to notify the user when a specific person is on-line
- IRC (Internet Relay Chat) allows many users on different systems at different locations to converge into one "room" and have a discussion, similar to a conference call or party line
- IRC is used both for entertainment and serious discussion purposes
- Special software is required

## **Other Chat Programs**

- Yahoo Chat
- WB
- Java Chat - Inside Web Pages
- Instant Messenger - Chat with other AOL users

## **Audio/Video conferencing**

Persons can communicate by audio and/or video to another user or a group. With the simple microphone and sound card that is now installed with most computers a user can communicate by audio to another person. A small video camera attached to the computer can give another person a live video picture. Only one person needs to have a camera.

## **ICQ/Instant Messaging/Buddy List**

"Successfully Investigating Acquaintance Sexual Assault: A National Training Manual for Law Enforcement"

Developed by the *National Center for Women & Policing*, with support provided by the Violence Against Women Office, Office of Justice Programs (Grant #97-WE-VX-K004)

---

- Programs broadcasting that you are on line or allow you to see if a specific user is on line
- Instant Messaging - The ability to send private messages to an individual that no one else can read

### **What is AOL?**

The largest on line service in the world. It is similar to the Internet with a few exceptions:

- Allows persons to sign up for monthly membership to access the AOL Network
- Within the AOL Network members are allowed outside access to the Internet
- To connect to AOL, the program must be preinstalled on the person's computer system
- Proprietary software AOL has must be used
- Can stay within the AOL network and visit many service areas that are similar to Internet Web pages
- Access group chat rooms, e-mail (read and send)
- Conduct private message with other AOL members or others that use Instant Messenger

### **Personal Profile**

- AOL offers members the ability to have a personal profile
- Give details about hobbies, geographical location, age, etc.
- Only other AOL members can read personal profiles

### **AOL E-mail**

- Using AOL is very simple. Attachments of files such as a graphic image are commonly sent to a group of other users
- This is very useful for suspects that want to send an image to several members at one time
- Users are allowed to access the Internet. The user can access the same protocols as if he/she had been connected to a Internet Service Provider
- AOL is popular because it provides easy access and it allows the beginner to access on line services
- The Graphical User Interface is so simple a child can easily log on and access most of the areas of AOL

### **How does a person log on to AOL?**

- Dial-up modem into a local POP (point of presence)
- Several of AOL POP's record the phone number that the user was calling from when accessing he POP
- The POP will also give a geographical location as to where the person resides.

Note: It is important to confirm that the account has not been compromised, i.e., the subscriber information belongs to a person living in Florida but the POP's that were being used during the incident were in California.

### **Why AOL is one of the major sources for meeting unsuspecting adults?**

"Successfully Investigating Acquaintance Sexual Assault: A National Training Manual for Law Enforcement"

Developed by the *National Center for Women & Policing*, with support provided by the Violence Against Women Office, Office of Justice Programs (Grant #97-WE-VX-K004)

---

- Easy to use and access chat rooms
- Personal profiles give the suspect detailed information about their victims on-line

### **AOL Accounts and Compromise**

- With social engineering many on-line users compromise their account
- Security check with the user on-line
- AOL accounts are targeted by hackers since most AOL users are relatively new

### **Reactive Cases**

- Law enforcement agencies need to be familiar with AOL
- Prepare to handle or investigate a case
- Look for other resources for assistance
- Call AOL Legal Team for assistance
- AOL has mechanisms in place to cooperate and they are very helpful
- AOL consent forms

### **Danger Areas: WWW**

- Japan
- Russia
- Former Yugoslavia Republics
- GEO Cities
- Free WWW Page hosts
- Hidden text/messages

### **Danger Areas: E-mail**

- Communication tool
- Sex acts solicited
- Images can be attached and viewed
- Covert e-mail accounts can be established; many sexual predators may direct the establishment of such accounts

### **Danger Areas: FTP**

- Automation of image transfer possible
- Exchanges can be made with trusted partners, thus avoiding Usenet posts and law enforcement activity

### **Danger Areas: IRC**

- Others with similar interests can be located
- Behavior is validated
- Major source of illegal picture trading
- Targets are identified, located and pursued

### **Danger Areas: Other Chat**

- Same as IRC
- Targets located, pictures traded, harmful matter sent, behavior validated
- Most chat is unmonitored and unregulated

### **Danger Areas: Video/Audio Conferencing**

- Real-time sex shows/rape/molestations can take place
- Can be easier for a sexual predator to convince a target to meet
- Harmful matter transmitted

### **Danger Areas: Pagers/Notify Programs**

- Subject has the ability to determine when a target is on-line
- Subject has the ability to know when a favorite trading partner is on-line
- Allows for message delivery like e-mail

### **Danger Areas: TELNET**

- More secure than WWW applications
- Dial-up is directly to remote machine
- Dated technology; not used much today

### **Danger Areas: Usenet Newsgroups**

- Bulletin Board type system
- Virtually any subject matter
- Uncensored newsfeeds available offshore
- Elicit images easily obtained

### **Legal Issues**

Legal issues concerning the Internet are rapidly evolving. Among the most pertinent are:

- The Privacy Protection Act, 42 USC, S 2000aa, applies to certain searches and seizures of computer equipment
- The Stored Wire and Electronic Communications and Transactional Records Access Act, 18 USC, Ss 2701-2711, governs law enforcement's ability to obtain information from Internet Service Providers (ISP's) without notice to subscribers.

For those interested in more information on this topic, please contact the International Association of Chiefs of Police for their manual entitled, *Best Practices for Seizing Electronic Evidence*. This manual was produced in collaboration with the United States Secret Service.

"Successfully Investigating Acquaintance Sexual Assault: A National Training Manual for Law Enforcement"

Developed by the *National Center for Women & Policing*, with support provided by the  
Violence Against Women Office, Office of Justice Programs (Grant #97-WE-VX-K004)

---