The Internet: A Breeding Ground for Online Pedophiles

*An In Depth Analysis o*f Crimes Against Children *Via the Internet*

By: Robert B. Fried, BS, MS

Have you ever had the opportunity to watch a youngster play on the computer? It's amazing how they instinctively move the mouse or bang on the keyboard. Ask any grandparent and they are most likely to say that their grandchildren are light years ahead of them when it comes to technology. Children just seem to have a knack for computers. A Computer can definitely be great learning tool for a growing child. However, there is something that all parents should know before they bring this technology into their home and to their child's fingertips. The personal computer has become the latest tool utilized by offenders in their quest to exploit vulnerable children who venture off into their new virtual playgrounds.

A majority of children generally use the computer to play games or to do homework. However, with the recent growth of the Internet, specifically the World Wide Web, more children are beginning to take a journey into cyberspace. In a recent study conducted by the Office of Juvenile Justice and Delinquency Prevention (OJJDP), "by 2002 some 45 million children will be surfing the net" [1].

The Internet provides a wealth of information. As a result, many children utilize the Internet for school related research or to simply improve their understanding or knowledge of a subject of interest or study. As more children sign online and become 'netizens', the potential for exploitation by offenders seeking these vulnerable subjects increases. In fact, "the very same offenders that once combed the playgrounds seeking victims now lurk into cyberspace" [2].

Besides schoolwork, many youngsters are also beginning to utilize the Internet to communicate with family or friends that may be located around the block or even throughout the world. There are many ways one can go about communicating with others on the Internet. A Bulletin board service, for example, allows for its users to dial into a central computer and post/read messages or even engage in conversation with others who have been granted access by the system administrator. Today, active bulletin board services are rare; now, most people resort to 'chat rooms' or a multi-user chat system known as Internet Relay Chat (IRC). Here, individuals can engage in conversations on an endless number of subjects or issues [3]. It is also here were many offenders prey on vulnerable youngsters. One such example is known as a 'chicken hawk', which refers to "an online pedophile who uses chat lines and member profiles to locate potential victims, sometimes posing as another youth to establish a bond" [4].

There are different ways in which an offender can exploit a vulnerable child in cyberspace. Many offenders resort to seduction to lure their victims in. "These individuals are often willing to devote considerable amounts of time, money and energy in this process. They listen to and empathize with the problems of children. They will be aware of the latest music, hobbies, and interests of children" [3]. In a sense, these individuals are attempting to build up a virtual relationship/friendship where in reality they can eventually gain the child's trust.

Many of these offenders ultimately seek to sexually exploit the children they encounter online. These individuals are referred to as 'online' pedophiles. "The pedophile is an adult who has either heterosexual or homosexual preferences for young boys or girls in a specific, limited age range" [4]. Online pedophiles fall into two categories: the dabbler or the preferential offender. The dabbler is essentially "a typical adolescent searching for pornography, a curious adult with a newly found access to pornography; or a profit-motivated criminal. The preferential offender is “usually a sexually indiscriminate individual with a wide variety of deviant sexual interests or a pedophile with a definite preference for children” [4]. When characterizing high tech pedophiles that have been arrested, Special Agent and Chief Spokesman Pete Gulotta of the FBI’s ‘Innocent Images’ Unit, says “they’re almost all white males between the ages of 25 and 45. “We’ve had military officers with high clearances, pediatricians, lawyers, school principals, and tech executives” [5].

It would be of no surprise that most preferential offenders are involved in child pornography. This type of activity online or offline is illegal in the United States. In fact, “The Child Protection Act of 1984 prohibits child pornography and greatly increases the penalties for adults who engage in it” [4]. Recently, “low cost technology has proved a boon to those who sexually victimize children. Readily available scanning equipment converts photos into computer graphics, while electronic mail transmits digital images anywhere in the world” [6]. The Internet has become a primary medium by which pedophiles exchange images and experiences with one another. Many of these pedophiles belong to international organizations and ‘web rings’, which are known to distribute pornographic images of children as well as other related material [7].

Sexual exploitation of children who are online can take on different forms. The online pedophile may chose to engage in explicit sexual conversation or even expose their vulnerable targets to pornographic images, material or information. The motivation behind all of their efforts may be to eventually talk on the phone or meet face to face with the children they encounter and possibly develop real-life relationships with their ‘online’ buddies. These individuals may also seek to obtain sexual gratification through their encounters or fantasies they have with/for the children they target [3].

Many children, generally in there teenage years, may be very curious or interested in sexual material or information. Often, they look to cyberspace to find answers to questions they may be too embarrassed to discuss with their parents or other family members. Adolescents tend to be attracted to individuals who engage in sexual conversation and the exchange of sexual material online. Many online pedophiles that target youngsters in this age group are aware of these needs and desires and use their knowledge of this to exploit the youth through seduction or manipulation [3].

There are signals that can help determine whether a child has become a victim of or is vulnerable to online exploitation. A child who spends a lot of time online, in ‘chat rooms’, specifically at night, may have a greater chance of being a victim of exploitation. Evidence of sexually explicit material such as pornographic images on a computer hard drive or removable media may suggest that a child has become a victim. Children who make/receive calls to/from unknown callers or numbers should also signal a red flag. Parcels being sent to or received by a child should also be deemed suspicious. If a child seems to be withdrawn from normal activities or a change in attitude towards family or friends is noticeable, it is possible that exploitation by an online pedophile is to blame [3].

If any of the characteristic signs of online child exploitation are noted and it is believed that a child has been victimized or may be vulnerable, there are several measures that can be taken. The first step is for the child’s parents or other loved ones to ask questions relating to the child’s activities online. Find out where the child likes to spend his or her time. If a considerable amount of time is spent in ‘chat rooms’ ask the child what is usually discussed in there and with whom. The next step is for the parent or loved one to examine the computer system. A computer’s hard drive may contain log files or conversations, downloaded images or other documents or files that may give clues as to whether the child has become a victim of child exploitation. If it is suspected that the child is getting phone calls from unknown callers or older individuals, caller identification feature from a local telephone company can be added to the household phone line to help screen calls or determine the origin of the incoming calls [3]. If a parent suspects that their child is a victim of online sexual exploitation they should contact one of the following: their local police department or law enforcement agency, United States Customs, the Federal Bureau of Investigation's Baltimore office, the National Center for Missing and Exploited Children or Safeguarding Our Children – United Mothers [8].

Parents who are concerned about their child's online activity in general, should make it a habit to monitor their child while on the computer. Keeping a computer with Internet access in a child's room is highly discouraged. Computers should be placed in a room that is accessible at all times and not secluded. Parents should also be able to access the child's account and e-mail through a master password. Usually, content filtering as well as age restrictions on various online services that may be available for the master account from the Internet Service Provider (ISP). Most ISPs alert their users as to the privacy and child safety options they have available for use by their members. These options and services are often provided free of charge. In the rare case of the ISP offering no such services, the re are software packages that are available for downloading on the Internet or purchasing through a local software retailer. Recently, many new products have hit the market, which feature the ability to filter e-mail from unknown sources and censor web sites that contain adult oriented material [3].

Parents should teach their children how to 'surf safe'. They should convey to their children that the virtual world, as in reality, has a lot of strangers. Often, children tend to trust people that are nice to them. This is no different in cyberspace. "Things like name, address, phone number, school, alma mater, grade, age, sex, likes, dislikes, hobbies, clothes, schedules, and so on are easily collected from children" [5]. It is important to tell children never to give out personal information such as their name or phone number as well any other information pertaining to their identity or location. If someone online asks them questions that they don't feel comfortable answering, children must understand they have a right to say no; even online [3].

Cyberspace, in a sense, provides the pedophile with the ability to lure in vulnerable children without having to leave their home. Most pedophiles are attracted to the fact that there are many dark corners of the Internet that are not being regulated. Essentially, with little effort, the online pedophile can disguise his identity while searches for his next target in what he/she refers to as their 'virtual playgrounds'. This fact, along with the abundance of online 'hangouts' or 'hot spots' makes the Internet the perfect medium for those looking to exploit children.

Despite the attempts to conceal their identities, online pedophiles should be aware that their presence on the 'information superhighway' is known and measures are being taken to identify and bring them to justice [4].

The issue of online child exploitation has caused some concern amongst many lawmakers. As a result, certain acts and laws have been passed to deal with the issue. On October 30, 1998, members of the Senate and House of Representatives of America in Congress enacted the "Protection of Children From Sexual Predators Act of 1998". This act contains many provisions. Under Title I., "Protection of Children From Predators", Sections 101-106 discusses the ways in which sexual predators attempt to gain information about, and ways in which to transport minors for the purposes of engaging in criminal sexual activity. Title II Discusses protections of children against child pornography. Title IV Of the act concerns itself with the prohibition on transfer of obscene materials to Minors. Title V discusses the increased penalties for persons who utilize computers for the purpose of exploiting children. Penalties can range from life in prison to even death based on the severity of the offense. Title X describes the proper procedure for ISPs to follow with regard to reporting any instances of child pornography on their member accessible servers to designated law enforcement agencies [9].

Besides, members of Congress, many state officials throughout the United States are addressing the issue of online child exploitation and child pornography. In November 13, 1997, New York State Attorney General Dennis Vacco formed a nationwide taskforce on 'kiddie porn'. This task force is made up of Attorney Generals from every state. Through the corporation of law enforcement agencies throughout the country, this undercover taskforce has been able to successfully identify and convict online pedophiles that distribute child pornography and other related material over the Internet [8].

Recently, the federal government has stepped up to members of the online pedophile community to let them know they are serious in their commitment to bring all those involved in utilizing the Internet for purposes of exchanging and distributing child pornography to justice. On March 18, 2002, The FBI publicly announced the arrest of 89 people throughout the United States for engaging in activities associated with the distribution and exchange of child pornography over the Internet. The FBI's Houston Child Exploitation Task Force and the United States Attorney's Office of the Southern District of Texas, under the direction of the FBI headquarters, headed the undercover sting, known as Operation Candyman. Essentially, an online medium, known as Egroups, which is affiliated with Yahoo, was utilized to set up the sting. Egroups allows individuals interested in a specific topic or issue to communicate and exchange information, experiences and data with one another. The FBI suspects that many

Egroups of a similar sort exist and they are definitely prepared to take these groups as well as their members offline [10].

The FBI has been no stranger in this war to help clean up cyberspace. In fact, the FBI ranks online pornography and sex exploitation as its number one focus with respect to crimes against children. In 1995, the FBI launched a national initiative known as 'Innocent Images'. The primary focus of this initiative is to: "identity, investigate and prosecute sexual predators who use the Internet and online services to sexually exploit children; establish a law enforcement presence on the Internet as a deterrent to subjects that use it to exploit children; and identify and rescue witting and unwitting child victims" [11]. Although crimes against children have gradually increased and will continue to increase over time, the FBI hopes that this national initiative will help to bring many of the online pedophiles who are still wandering about cyberspace to justice [11].

As technology advances, so do the tools these online pedophiles use in their efforts to avoid being detected or caught. It is known that many pedophiles spend their time in chat rooms. When initially entering a chat room, the user is asked for an alias or nickname. The user's actual identity is therefore disguised. As a result, it is difficult to reveal an online pedophile or any chat room participant's true identity for that matter. Monitoring of these chat rooms by law enforcement agencies can also cause some legal concern. The issue of entrapment can come into play with respect to how law enforcement personnel go about trying to figure out if a chat room user is in fact an online pedophile. Many online pedophiles can simply say that they didn't know that the person whom they suspected to be an adolescent or such was in actuality a law enforcement officer [12].

There are also tools on the Internet that allow online pedophiles to anonymously ‘surf ‘ the net or compose electronic mail. These programs are available free of charge and essentially allow the user to mask their true identity while exploring the many dark corners of the Internet or trying to send vulnerable targets messages. Another thing that online pedophiles do is that they tend to encrypt their data. This is often a big challenge to law enforcement because without knowing the encryption keys, it is often difficult, and in some cases impossible to decrypt if the offender does not cooperate [4]. “Pedophiles have always been ahead of the power curve, and law enforcement has trailed, sometimes far behind, in apprehending them. The Internet is merely the latest area in which the pedophiles have captured a huge lead because of their networking and technical expertise” [7].

A major challenge to the law enforcement community is investigation of online crimes against children. Often law enforcement personnel do not know how to properly deal with these types of crimes because they are complex. Many law enforcement agencies that have to investigate these types of crimes usually are faced with following problems: jurisdiction, expertise, equipment, time/personnel and follow-up [13].

The jurisdiction issue related to the fact that online crimes can extend to other towns, counties, cities, states or even countries. It may sometimes be uncertain as to whether such an investigation should be handled by the local agency that initially took the complaint, which eventually led to an investigation. The issue with respect to expertise deals with the issue as to whether the law enforcement agency that is performing the investigation is knowledgeable enough and properly trained in this type of crime. Sure, there may be a technology or computer guru on staff but when it comes to criminal matters, training and expertise is a must. There is also the equipment issue. In order to investigate these types of crimes it is absolutely necessary for the law enforcement agency to know how to properly examine digital evidence. Digital evidence is extremely fragile and can improper examination can result in the evidence being deemed inadmissible in court. There are several software packages that are available to law enforcement agencies and personnel that allow for the forensic analysis of computer data. However, these programs are often too costly to purchase. As a result, an agency that is not properly equipped to handle these types of crimes may be faced with knowing who to call or what to do next. Another problem relating to this type of investigation is that fact that such crimes require much time, effort and personnel. Many law enforcement agencies are already understaffed. Due to the complexity involved in the investigation in these types of crimes, a given law enforcement agency may not have the time or personnel that is needed. With respect to the follow-up that is needed when investigating these types of crimes, this is often a challenge because many law enforcement agencies may not have the resources available to develop leads and interview possible victims, witnesses or suspects [13].

Despite the challenges involved, law enforcement agencies must begin to realize that more and more computers are being used to commit crimes. In order to thoroughly investigate crimes involving computers or other digital evidence, proper training is necessary. There is no real way to rid the Internet of online pedophiles. However, to protect the future, our children, it is necessary to work together in order to get as many of these pedophiles offline and bring them to justice.

References

[1]. Paynter, Ronnie L. "Riding the Cyber Wave." Law Enforcement Technology, Vol. 26, No. 11, November 1999, pp. 52-55.

[2]. Kopelev, Sergio D. "Cyber Sex Offenders: How to Proactively Investigate Internet Crimes against Children." *Law Enforcement Technology*, Vol. 26, No. 11, November 1999, pp. 46-50.

[3]. U.S. Department of Justice: Federal Bureau of Investigation Publications: "A Parent's Guide to Internet Safety." http://www.fbi.gov/publications/pguide/pguidee.htm

[4]. Bennett, Wayne W and Karen M. Hess. "Crimes Against Children." *Criminal Investigation*. California: Wadsworth, 2001. 289-313.

[5]. Cohen, Fred. "How To Keep Your Children Safe on the Internet." http://all.net

[6]. McCauley, Dennis. "Hi-Tech Crooks." *Police*, Volume 20, No. 12 December 1996, pp. 32-49.

[7]. Lesce, Tony. "Pedophiles on the Internet: Law Enforcement Investigates Abuse." Law and Order, Vol. 47, No. 5, May 1999, pp. 74-78.

[8]. "Internet Crimes Against Children: The Secrecy of Child Sexual Abuse." http://www.prevent-abuse-now.com/law3a.htm

[9]. Protection of Children From Sexual Predators: Public Law 105-314. http://www.child-law-watch.net/protection_from_predators.htm

References (continued)

[10]. Operation Candyman, FBI Press Release: March 18, 2002.
http://www.fbi.gov/pressrel/pressrel02/cm031802.htm

[11]. FBI: Crimes Against Children: Online Child Pornography: Innocent Images Initiative.
http://www.fbi.gov/hq/cid/cac/innocent.htm

[12]. Quart, Alissa. “The Sex Avengers”. Time Digital: September 2000, Vol. 5 No. 5.
http://www.time.com/time/digital/magazine/articles/0,4753,57290,00.html

[13]. Armagh, Daniel S.; Battaglia, Nick L.; and Lanning, Kenneth V. *Use of Computers in the Sexual Exploitation of Children*. Washington DC: Office of Juvenile Justice and Delinquency Prevention, June 1999. [NCJ-170021).

About the Author

Robert Fried holds a B.S. and an M.S. in Forensic Science with a concentration in Advanced Investigation. He also holds Certificates in Law Enforcement Science, Forensic Computer Investigation, and Information Protection and Security from the University of New Haven and SEARCH. Fried has extensive knowledge of forensic science, however, most recently he has worked extensively in the developing field of "digital forensics" and has published in this area by organizations such as the SANS Institute. He is also a member of the NorthEast chapter of the High Technology Crime Investigation Association (HTCIA).