Global Information Assurance Certification Paper

TEENAGERS AND INTERNET SAFETY

Marilyn Miller
July 26, 2002
GIAC Security Essentials Certification (GSEC) Version 1.4, Option 1

Abstract

A concern of every parent of teenagers should be Internet Safety. The Internet provides access to a vast amount of knowledge but poses three major dangers for teens: personal danger; exposure to inappropriate material; and invasion of privacy (Gralla, 204-205).

The first step in protecting teens is in understanding how they use the Internet. An integral part of their lives, they use it for communicating with their friends; homework; finding information and entertainment. Parents need to learn how to use the software that teens use and learn about the safety issues in order to provide their children with the knowledge and skills required for safe Internet usage. Good parenting skills are the most important thing that parents can use to keep their teenagers safe. There are software tools available that parents can use when necessary. These include activity monitors; cache explorers; site filtering software; spyware removal software; and personal firewalls.

Internet Safety

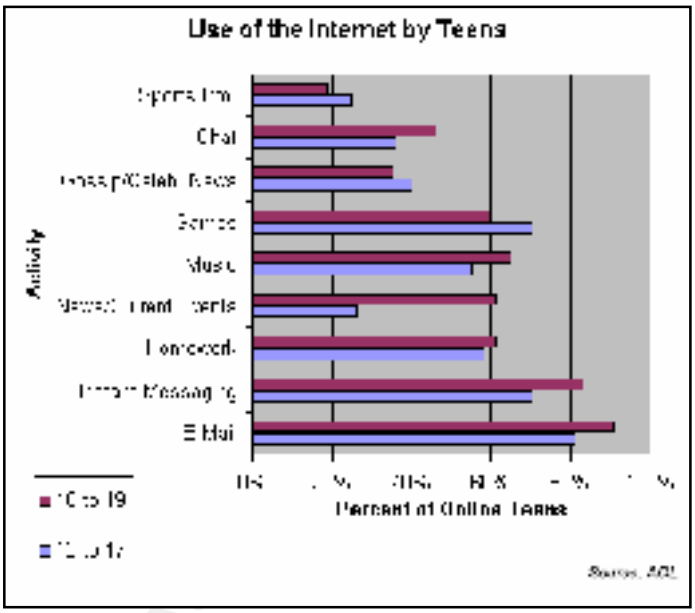
There is much in the news today about Internet Security and Safety. While Internet Security is primarily about protecting your computer and data, Internet Safety is about protecting yourself and your family from dangers posed by the Internet. Teens pose a particular challenge when it comes to Internet Safety. American teenagers are often adventuresome, knowledgeable about computers, and independent but their lack of wariness and life experiences can make them easy targets for various Internet hazards. The Internet poses three major dangers for teens: personal danger; exposure to inappropriate material; and invasion of privacy (Gralla, 204-205). This paper explores these dangers and provides parents with information on how to protect their teenagers.

Teenagers and the Internet

Today's teenagers have grown up with home computers. They have learned about computers at school and have sufficient experience so that in many cases they are move savvy users than their parents. The Internet is an integral part of their lives. In 2001, the PEW Internet and American Life Project estimated that over 17 million American teenagers, ages 12 through 17, use the Internet, representing 73% of this age bracket (Lenhart, Rainie and Lewis 3). Even teens who do not have a home computer have access to the Internet at school, at a

friend's house or at the library. With large number of users and easy access, Internet Safety should be every parent's concern.

The first step in protecting teenagers from Internet dangers is in understanding how teenagers are using the Internet. Teenagers use the Internet for many reasons including communicating with friends; downloading music; doing homework; and playing games. This chart, taken from an article by Michael Pastore and prepared by America Online, shows how teens are using the Internet.



e-mail

The most popular use of the Internet among teens is e-mail. Teenagers can easily get an e-mail account either through their family's Internet Service Provider (ISP) or from a site offering free Web-based e-mail accounts like Hotmail from Microsoft Network (MSN) or Yahoo!Mail from Yahoo. Web-based e-mail is convenient for teenagers because it requires no special software; it can be accessed from any computer with Internet access; and accounts can be easily obtained by providing some basic information such as name, birthday, and gender. Companies providing free e-mail accounts offset the expense of providing the email accounts with the income generated by advertising on the e-mail web site. Advertising is often geared to the user based on information provided when activating an account (Goodman). Parents can try out a free Web-based e-mail by connecting to http://www.hotmail.com or http://mail.yahoo.com.

Instant Messaging

Another popular use of the Internet is Instant Messaging, the most popular of which is AOL Instant Messenger (AIM). Seventy-four percent of online teens use Instant Messaging while nineteen percent of online teens use Instant Messaging as the primary way of contacting their friends when they are not with them (Lenhart, Rainie and Lewis 3). With Instant Messaging, users maintain a list of contacts and can send messages to them when they are online. Messages are displayed in a special window as soon as it is received. Teens frequently participate in multiple Instant Messaging sessions at one time and often carry on conversations all evening while doing other things such as homework or talking on the phone.

Kids have created a special lingo which is used when communicating through Instant Messenger so that it takes less time when responding. Examples include brb – be right back; gtg – got to go; and pir – parents in room (Holder). The lingo can be very cryptic for parents who are not regular users of Instant Messenger. Parents can download a copy of AIM free of charge at http://www.aim.com/index.adp.

Music

Teens love music and with limited spending money, downloading free music over the Internet is a popular activity. In 2000, 59% of online teens had listened to music online and 53% had downloaded music files from the Internet. These percentages are even higher for older teens. (Lenhart, Rainie and Lewis 41).

Files traded over the Internet are stored in the MP3 format. The MP3 format makes the files small enough to easily move over the Internet. "Napster, which began the Internet craze of trading music files and boasted 60 million users at its height" has effectively been shut down by the music industry (Collins). It was immediately replaced by other similar peer-to-peer file sharing alternatives such as Morpheus and KaZaA. Peer-to-peer means that rather than having files stored and downloaded from a central server, files reside on other user's machines. Users share directories on their machines so that files can be downloaded by other users and likewise users can download files from shared directories on other machines. Teens with CD burners can create music CDs from the files they have downloaded.

One big issue with peer-to-peer file sharing is that most of the songs traded are copyrighted. By trading songs over the Internet instead of buying CDs, the artists and music industry do not get any royalties. Another issue is that teens are allowing people they don't know to access a part of their hard drive. In some cases, if set up incorrectly, they may be giving access to a lot more than they realize.

Copies KaZaA can be downloaded from http://www.KaZaA.com/ en/index.php.

Chat Rooms

More than half of all online teens have visited a chat room (Lenhart, Rainie and Lewis 42). A chat room allows a group of people to type in messages that are seen by everyone in the room. Chat rooms are usually organized around topics so that people with similar interests can talk with each other. There are different types of chat rooms. Some chat rooms are moderated meaning that there is a person leading the discussion; others are monitored so that people behaving inappropriately can be kicked out; and others are entirely open. Since there is no way to know who is really in the room, it is important never to give out any personal information. It is easy for a person to pretend to be someone they are

not. For example a pedophile can pretend to be a teenager and attempt to befriend teenagers in the chat room. For this reason, chat is probably the most dangerous area of the Internet (Magid, “Teen”).

Yahoo.com has a listing of popular teen chat rooms at http://dir.yahoo.com/Society_and_Culture/Cultures_and_Groups/Teenagers/Chats_and_Forums/Chats/.

Homework

The Internet is a great tool for helping teens with their homework. They can find information on any topic. There are even web sites where they can get help with their homework such as the Minneapolis-St. Paul Star Tribune Homework Help site at http://www.startribune.com/homework_help. There are, however, some downsides to using the Internet for homework. Being able to cut and paste text from Internet web pages directly into word processing software makes it very easy and tempting for teens to plagiarize. Some web sites have term papers available for free download and other sites even offer custom term papers. Parents need to be aware of these possibilities so they can discuss with their teens the pitfalls of plagiarism and cheating.

Personal Danger

Description of the Problem

A parent’s biggest fear concerning the Internet is that a predator, who was met on the Internet, could victimize their child. Risks include sexual molestation, abduction, and harassment. In 1999, a survey was conducted for the National Center for Missing & Exploited Children by the University of New Hampshire's Crimes Against Children Research Center. The survey questioned teens and preteens about their online experiences. “According to this report, approximately one in five children, aged 10 to 17, had received a sexual solicitation online. One in 33 youth had received an aggressive sexual solicitation — a solicitor who asked to meet them somewhere; called them on the telephone; or sent them regular mail, money, or gifts. [. . .] One in 17 was threatened or harassed in some way. One of the most distressing things discovered in this study was that less than 10 percent of the sexual solicitations were reported to authorities” (Finkelhor ix).

Chat rooms, instant messaging, and e-mail are the tools of the online victimizer. Chat rooms, especially those used by teenagers, are used by pedophiles to find victims. However, it is often the case that teenagers are the ones soliciting or harassing other teenagers. A study by the National Center for Missing and Exploited Children found that the “vast majority -- 96 percent -- of those who

solicit teens are under 25 and nearly half -- 48 percent -- are themselves children under the age of 18" (Magid, "Study").

Fortunately, the number of teens who are actually "molested, abducted, or leave home as a result of contacts made on the Internet are relatively low, but when it happens the results can be tragic" (Magid, "Teen"). For this reason, parents need to be alert to what their teenagers are doing on the Internet and look for signs that they may be in trouble.

Countermeasures

Parental Guidance

It is important that parents give their teenagers guidance on how to deal with potentially dangerous situations on the Internet. Parents need to be supportive and not overreact if the teenager does something they view as inappropriate. If parents threaten to take the Internet access away from their teen when the teen comes to them for help or advice, the teenager will likely not consult the parents again. Thirty percent of girls responding to a study by the Girl Scouts "reported that they had been sexually harassed in a chat room, but only 7 percent told their mothers or fathers about the harassment, most fearing their parents would overreact and ban computer usage altogether" (Au).

Parents need to establish some basic rules on Internet activity. A few important rules include the following:

- Never reveal any information which could help determine your real identity, this includes name, address, and pictures of yourself.
- Never agree to meet someone who you meet online without consulting with a parent. Never go without an adult.
- Never respond to any instant message, email or chat messages which make you feel uncomfortable.
- Choose an Internet name which is gender neutral and not likely to attract unwanted sexual attention.
- Remember that people on the Internet are not always who they claim to be.
- Always consult with your parent if anything makes you uncomfortable on the Internet.

Activity Monitor

Parents should monitor their teenager's activity on the Internet and watch for signs that they may be engaging in unsafe behavior. This can be very difficult especially when it comes to Instant Messaging, chat rooms and email.

With Instant Messaging, it is very difficult to find out who a teenager is communicating with and what they are saying. Teenagers often minimize windows when the parent walks into the room. Typically everyone uses screen names which are not indicative of whom they are. For example, is "SexyGuy" the

boy next door or a pedophile across town? Finally there is no record of the sessions which parents can view to make sure that communications are innocent. All these problems are the same for chat rooms. If a teenager uses an web-based email account, messages are stored on a remote server instead of the home computer. Teenagers can have one or more e-mail accounts without the parent's knowledge and since the account is password protected, the parent is not easily able to monitor messages sent to and from the teenager.

Because of the difficulty in monitoring, it is very important that the parents keep communications open with the teenager concerning Internet activity. However, when the parent feels that something is wrong and feels that the teenager is hiding it, there are software options that can help identify the problem. These types of software are known as activity monitors. Some of the top rated products include Spector Pro by SpectorSoft Corporation; Spytech SpyAgent by Spytech; iOpus Starr PRO by iOpus Software; and NetObserve by ExploreAnywhere Software (Glass).

Spector Pro, which is PC Magazine Editors' Choice for this type of software, is a descendant from the Netbus Trojan horse. It can capture screen shots; log keystrokes; log SMTP and POP mail sessions; monitor web-based e-mail such as Yahoo, Hotmail, and AOL; record file attachments; monitor instant messaging and chat sessions; and capture every Web site accessed (Glass). Parents can set it up so that they are emailed each time a key word is typed on the computer, on a web site or in an email. The software runs on Windows 98 and above with an approximate cost of $100. (Spector).

The decision to use an activity monitor can be a difficult one, involving issues of the teenager's privacy and trust. It is similar to reading a child's private diary. One option is to inform the teenager that he or she is being monitored and recorded and that activity will be reviewed later. Knowing this, the teenager may behave more responsibly when using the Internet. However, they may just go use a friend's computer when they want to do something their parent has forbidden. Some parents feel that by routinely reviewing chat conversations and e-mails, they can spot potential predators and protect their child before it has a chance to develop into a dangerous situation. Others prefer to respect their teenager's privacy and only use an activity monitor when they suspect that something serious is going on. There is no right or wrong answer and parents must do what they feel is best for their teenager.

Inappropriate Material

Description of the Problem

The Internet is a vast information resource. There are many great sites to visit, but there are also many sites that contain material inappropriate for teenagers.

Teenagers can find materials related to pornography, sex, hate, violence, and cults just as easily as they can find information needed for a school research paper.

In some cases, the teenager doesn't have to be trying to access inappropriate material. According to one study, "one in four young people has had unwanted exposure to pictures of naked people or people having sex. These are not cases where the young person admits to looking for such pictures, but situations where they have come upon them while searching for material, or where links to such material were sent via e-mail" (Magrid). In some cases, teenagers are tricked into visiting a particular site. For example, students mistakenly typing in www.whitehouse.com instead of www.whitehouse.gov will find themselves at a pornographic site instead of a site containing information about the White House.

Teens can also be exposed to pornographic material when using the peer-to-peer file–sharing software typically used for downloading music. Programs such as Morpheus and Aimster can "provide children easy and free access to thousands of explicit pornographic videos and other pornographic materials" (Waxman and Largent)."

Countermeasures

Parental Monitoring

While most experts agree that computers should be placed in a common area of the house and children should be monitored while on the Internet, for several reasons this is often not practical when it comes to teenagers. One reason is lack of time. Teenagers spend a lot of time on the Internet. Computers and the Internet play an important role in the teenager's education often requiring nightly use to complete homework. Parents simply do not have the time to constantly watch over their teens while they are using the computer, especially when it involves multiple children and multiple computers. Since teenagers are often home alone or stay up later than their parents, much of their usage is when the parent is not around. This makes it very difficult for a parent to actively monitor everything that the teen is doing on the computer. Even teenagers, who are well supervised at home, may use the computer inappropriately when they are at a friend's house.

Statistics bear out the difficulty in monitoring teenage Internet usage. A 1999 study by Greenfield Online found that "75 percent of 16-year-old teenagers are allowed to surf the Web freely [. . .] The study found that only 5 percent of parents with children over the age of 16 attempt to monitor their online activities" ("Greenfield").

Checking the Browser History & Cache

One way to monitor which web sites a teenager visits is to check the history list in the browser. In Internet Explorer, the history list may be viewed by clicking on the History button. A pane will open up showing sites visited by date visited (see example to the right). In Netscape Navigator, it may be viewed by selecting Window and then History. In Internet Explorer, the length of time that the history is kept is configurable by selecting Tools, Internet Options, General Tab and then setting the "Days to Keep Pages In History." It should be noted that it is very easy for the teenager to delete the browser history. In Internet Explorer simply by clicking on the Clear History button found on the same screen where the "Days to Keep Pages In History" setting is found.

The Favorites list in Internet Explorer and the Bookmarks list in Netscape Navigator may also give clues as to sites that the teenager likes to frequent. Teens may use these lists to create shortcuts to their favorite sites.

Software products can be bought to help discover what sites have been visited. There are software products that can recreate web pages from the cache where web pages are stored temporarily after they are downloaded to the PC. Two such products are Microsoft Internet Explorer Cache Explorer and Netscape Cache Explorer. Both can be downloaded for a free trial from http://www.pcworld.com/downloads. Cache Explorers are not a foolproof way to know what sites your child is visiting. It is very easy for the teenager to delete the cache. In Internet Explorer, select Tools, Internet Options, and under Temporary Internet Files, click Delete Files. In Netscape Navigator, select Edit, Preferences, click the + sign next to Advanced, choose Cache, and click Clear Disk (Gralla 225).

Checking Cookies

Parents can also determine what sites their teen is visiting by looking at cookie files. "A cookie is a piece of text that a Web server can store on a user's hard disk. Cookies allow a Web site to store information on a user's machine and later retrieve it" (Brain). Not all sites store cookies, but by looking at the cookies, it is possible to determine some of the sites that have been visited from the PC. Cookies contain the name of the web site that stored the cookie. To see cookies stored by Internet Explorer, look in either the Windows\Cookies or Windows\Profiles\UserName\Cookies directory. The name after the @ sign corresponds to the site name. Netscape Navigator cookies are all stored in one

file and can be viewed by opening C:\Program Files\Netscape\Users\Username\ cookies.txt (Gralla 151-153).

Site Filtering Software

Site filtering software is one way to prevent teenagers from reaching inappropriate web content. This type of software attempts to block out objectionable web sites using several methods. Some products use software analysis. In this case, the software determines if the site is objectionable by scanning for the presence of certain phrases or images. The advantage of this method is that it can analyze every site, but the disadvantage is that it blocks some legitimate sites only because they contained a prohibited word. It is very difficult to for software to understand the context in which a word is used. A second method is human analysis. With this method, the software company has a staff which manually reviews sites and creates lists of those which are to be blocked. The advantage of this method is that humans can better interpret appropriateness of sites than a software program, but the disadvantage is that the web contains so many sites that are ever changing that there is no way that all objectionable sites will be placed in the blocked list. The third method is site labeling. Products using labeling incorporate a rating system such as the nonprofit Internet Content Ratings Association (ICRA). With ICRA, web site owners voluntarily label their content. The problem with this method is that many sites are not rated. Choosing to block unrated sites will block numerous legitimate sites, but choosing not to block unrated sites will result in failure to block many of the inappropriate sites (Digital 21).

There are a number of software products sold for Internet filtering. Two of the programs rated best by Consumer Reports in 2001 were Cyber Patrol by Surf Control Inc. and Cybersitter 2000 by Solid Oak Software Inc. Both provide good blocking of objectionable material and Cyber Patrol was rated excellent at not blocking sites containing potentially controversial, but legitimate material. Both products run on Windows and sold for $50 or less. America Online also provides content filtering for its members. Consumer Reports rates their Young Teen control the best of all filters. (Digital 23).

Activity Monitor

Activity Monitors, which were discussed under Personal Danger, are another way to determine if a teenager has accessed inappropriate web content. See that section for more information.

Searching the Hard Drive

To find out if a teenager has been downloading pornographic images from the Internet, a parent can search the hard drive for recent files with endings such as .gif, .jpg, .bmp, .tif or .zip (Digital 22). These images can then be viewed using any number of graphics editing programs, some of which come free with the

computer. Parents should also look for sexually explicit music by looking at recently downloaded files in KaZaA and Morpheus.

Parental Communication

Since there is no fool proof way to prevent teenagers from accessing inappropriate web sites or downloading pornographic images, it is important that parents should talk with their teenagers about their expectations for teenage Internet behavior. Should it is discovered that a teen has accessed inappropriate material, it is important that the parent not overreact. Parents should discuss the problem with the teen to find out the teenager's feeling about the content and explain why the parent finds the site objectionable. It should also be remembered that the teen may have accessed the site in error.

Invasion of Privacy

Description of Problem

The Federal Trade Commission did a study and found that "nearly ninety percent of child-oriented sites it visited collected personal information from children" (Gralla 208). Sites collect names, addresses, phone numbers, email addresses, social security numbers and even information about their parents. Teenagers unwittingly give out information while performing seemingly innocent activities such as completing surveys; playing games; and entering contests.

Another threat to a teenager's privacy is Spyware. "Spyware is a broad software category that covers any program that secretly tracks or records information about you, your computer use or personal information. Often these programs have the ability to report back to a central database computer on the Internet without you knowing it" ("Attacks"). Spyware is sometimes included in share-ware and freeware which teens may download from the Internet and install on the home computer. For an example, KaZaA, the software many teens use to download music, includes Brilliant Digital software which sends statistics back to a web server when a 3D advertisement is played in KaZaA ("So").

Countermeasures

Parental Guidance

Parents need to make sure that their teenagers know not to provide personal information over the Internet. Guidelines should be given as to what is acceptable and what is not. Personal information should never be given out in a chat room since there is no way to know who is listening. Teenagers should think twice before entering any information about themselves for any reason on any web site. If children are in doubt, they should ask their parents.

Investigate Software

Teens should be instructed to check out software for spyware before downloading it and installing it on their computer. Two helpful sites that tell whether a software product contains spyware are SpyChecker (http://www.spychecker.com/) and TomCat Internet Solutions Spyware List (http://www.tom-cat.com/spybase/ spylist.html).

Spyware Removal Software

There are software products available that will remove spyware from a computer. Ad-Aware 5, by Lavasoft, was awarded PC World's Best Software Product of the Year in 2002. Ad-Aware 5 is a "free program that scans your computer for the telltale files that adware plants on your system--and deletes them" ("Spyware"). The software can be downloaded from Lavasoft at http://www.lavasoftusa.com/ index.html.

Personal Firewall

A personal firewall, such as Zone Alarm, can prevent spyware from reporting its findings back to the central server. Since Zone Alarm can block both incoming and outgoing connections, when the spyware tries to connect to the server, Zone Alarm can issue a warning and allow the user to block the connection. Zone Alarm can be downloaded for free from Zone Labs at http://www.zonelabs.com/store/content/home.jsp.

Conclusions

The Internet plays a big role in today's teenagers' lives. There are many great features of the Internet as well as many dangers. Parents must be vigilant in making sure that their teenagers use the Internet appropriately and safely. The first step in accomplishing this is by understanding how teenagers use the Internet. Parents should have teenagers show them how some of their favorite features work and parents should stay current on Internet advancements and safety concerns.

The best way to keep teenagers safe is to have a good relationship with the child and to have frequent non-judgmental discussions about the Internet and safety. There are a number of software tools that can be used to monitor teens and restrict their access, however, the use of these tools has some drawbacks. In one study, "teens made it clear that they had the computer sophistication to get around many of their parents' technology roadblocks and considered it a challenge to do so. Worse, the parents using these technologies are betraying any sense of trust and diminishing the opportunity to build new relational connections with their offspring" (Pollack).

As with most things related to parenting, there is no right or wrong answer. Parents have to understand the issues and decide what is right for their child in the specific situation.

Works Consulted

"Attacks from the Inside: The Spyware Threat." HomeNetHelp.com 26 July 2002. <http://www.homenethelp.com/web/explain/spyware.asp>.

Au, Sara. "New Study Shows Girls Are Driving on the Information Superhighway Without a License." Girl Scouts 13 Feb. 2002. 28 June 2002. <http://www.girlscouts.org/news/archive/2002/net_effect.html>.

Bannan, Karen J. "Watching You, Watching Me." PC Magazine July 2002: 100 - 105.

Brain, Marshall. "How Internet Cookies Work." Marshall Brain's How Stuff Works 26 July 2002. < http://www.howstuffworks.com/cookie.htm>

Collins, Meghan."Napster Files for Bankruptcy." CNNMoney 3 June 2002. 28 June 2002. <http://money.cnn.com/2002/06/03/news/companies/napster_bankrupt/index.htm>.

Finkelhor, David, Kimberly J. Mitchell, and Janis Wolak. Online Victimization: A Report on the Nation's Youth. Alexandria, Virginia: National Center for Missing & Exploited Children, 2000.

Glass, Brett. "Activity Monitoring." PC Magazine July 2002: 106-112.

Goodman, Andrew. "Web-Based E-Mail Frequently Asked Questions (FAQs)". Traffick 2 April 2002. 21 June 2002. <http://www.traffick.com/article.asp?aID=10>.

Gralla, Preston. The Complete Idiot's Guide to Protecting Yourself Online. Indianapolis: Que Corporation, 1999.

"Greenfield Online: Most Teenagers Allowed to Surf Unsupervised." NUA Internet Surveys 28 April 1999. 23 June 2002. < http://www.nua.com/surveys/index.cgi?f=VS&art_id=905354867&rel=true>.

Holder, Allison. '"wassup? brb pir, ttyl". St. Petersburg Times Online 8 Oct. 2001. 21 June 2002. <http://www.sptimes.com/News/100801/Xpress/wassup_brb_pir__ttyl.shtml>.

"How Napster Works." Marshall Brain's How Stuff Works. 23 June 2002. <http://www.howstuffworks.com/napster.htm>.

"Digital chaperones for kids, Which Internet Filters Protect the Best? Which Get In The Way?" ConsumerReports.org March.2001. 25 July 2002. <http://www.consumerreports.org/main/detailv2.jsp?CONTENT%3C%3Ecnt_id=18867&FOLDER%3C%3Efolder_id=18151&bmUID=1027641492678>

Lenhart, Amanda, Lee Rainie, and Oliver Lewis. "Teenage Life Online, The Rise of the Instant-Message Generation and the Internet's Impact on Friendships and Family Relationships." The Pew Internet & American Life Project 30 June 2001. 21 June 2002. <http://www.pewinternet.org/reports/pdfs/PIP_Teens_Report.pdf>.

Magid, Lawrence. "Study Outlines Safety Tips for Kids, Online study finds perpetrators are younger than you'd expect." Safekids.com 11 June 2000. 21 June 2002. <http://www.safekids.com/articles/ft_study.htm>

Magid, Lawrence. "Teen Safety on the Information Highway." Safekids.com 1998. 21 June 2002. <http://www.safekids.com/safeteens/safeteens.htm>.

"Online Risks For Youth." National Center For Missing and Exploited Children. 26 July 2002. <http://www.missingkids.com/>.

Pastore, Michael. "Internet Key to Communication Among Youth". The Big Picture Demographics 25 January 2002. 19 June 2002. <http://cyberatlas.internet.com/big_picture/demographics/article/0,,5901_961881,00.html>.

Pollack, William. "The Parent Trap." CIO.com 15 May 2001. 26 July 2002. <http://www.cio.com/archive/051501/diff.html>

"So, is KaZaA/Brilliant Digital Entertainment ... Spyware?" 26 July 2002. <http://www.imilly.com>

"Spector Professional Edition." Spector Soft . 26 July 2002. <http://www.spectorsoft.com/products/SpectorPro_Windows/index.html>

"Spyware Removal." Spyware Online. 26 July 2002. <http://www.spywareonline.org/spyware_removal.html>

"Users Of File-Swapping Alternatives Increase Nearly 500 Percent In The US, Surpassing Napster." Jupiter Media Metrix 21 Oct. 2001. 21 June 2002. <http://www.jmm.com/xp/jmm/press/2001/pr_101001a.xml>.

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS