Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# Protecting Students in the Public School Environment

Today's network security issues not only involve the protection of the vital data of commerce, but also, whether by law, policy or common sense, the people and the parts of their lives that may be included in that data. It does not matter if your organization is a major corporation, a small business or a home user, parts of a user's life such as Social Security numbers, personal phone numbers, tax/income information, health information, etc, are all possibly available on a network if not properly protected. This paper ...

Copyright SANS Institute
Author Retains Full Rights

AD
Investigate Insider Threats
Protect your company against corporate IP Theft
Learn More
SpectorSoft

# “Protecting Students in the Public School Environment”

**John Decker**

**GSEC Practical**
**Version 1.4b Option1**
**Submitted May 18, 2004**

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

## Abstract

Today's network security issues not only involve the protection of the vital data of commerce, but also, whether by law, policy or common sense, the people and the parts of their lives that may be included in that data. It does not matter if your organization is a major corporation, a small business or a home user, parts of a user's life such as Social Security numbers, personal phone numbers, tax/income information, health information, etc, are all possibly available on a network if not properly protected. This paper will consider the environment and some processes designed to protect our most precious users – our children - when out of our homes and inside the educational environment.

## Introduction

Computing and the Internet have become absolute marvels within our lifetimes. The power to create, entertain, inform and process have grown to become part of our daily lives. The ability to visit with someone across the globe, to collaborate online to complete high level business agreements, create art, share knowledge - and wage war, have become commonplace. Man's ability to figure out problems and achieve is incredible! Alongside these marvelous abilities come the seemingly equal capabilities to create powerful, destructive, and insidious means to disrupt these wonderful technologies and steal from the people that use them. The Internet itself has become a kind of snare for the unwary visitor who is unaccustomed to or uninformed of its possible dangers and how to avoid them. As a result, millions of people have had their privacy abused and their identities stolen.[1] The most vulnerable and innocent users that may be exposed to the shadier side of Internet technology are our children. Within our homes we have the ability to control their playing, learning and surfing habits and monitor their behaviors, but once out of the home, we pass the safety of our kids to principals, teachers, librarians and other staff. This is a large and awesome responsibility for those entrusted with their welfare when they step off the bus and into the school house. Networking professionals working in educational settings have the added responsibility of keeping up with the laws, standards and technology in order to maintain a technologically safe learning environment for the kids.
Some items we will examine as we progress through this topic include:

- The current environment our kids face if not protected
- Threats to today's technologically savvy kids themselves and their growing abilities to work with computer technology
- Laws and legal enforcement of these laws designed to protect the children
- Practical methods of attaining network safety, such as education, network architecture, policy, and software available for filtering and monitoring student Internet usage

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

## A Grim View

As wonderful a thing as life is and can be, in the security professions, we deal mostly in protecting the good from the bad and facing the negative aspects of life. Yearly it seems, the headlines are filled with the horrors of kidnapped and murdered children, sexually abused children and posters are placed in Wal-Mart® of missing children. Our government has had to enact laws such as "Megan's Law" [2] requiring sex offenders to register their residency in every state to protect our neighborhoods. This law is a result of a horrific crime against a 7 year old little girl in New Jersey, who was lured by the promise of seeing a puppy to a pedophile's home.[3] We have also seen pro-active volunteer associations organized into what we now know as the "Amber Alert Plan"[4] which utilizes cooperation between the FCC's "Emergency Alert System" and law enforcement agencies nationwide to alert the national community about kidnapped children so that they can react quickly before tragedy strikes. This plan came about after another tragic crime was committed against a 9 year old little girl in Texas who was just riding her bicycle. The names go on – such as Polly Klaas [5], Carlie Brucia [6]and many others, who are faceless victims not featured in the media. But how do these cases tie in with networking professionals? After all, we just deal with the programs, colorful graphics and technologies which drive today's E-society. The answer: Into the computing/Internet environment enters a large factor that encourages many behaviors in individuals that may not be considered normal –anonymity.

Anonymity is a two-edged sword. In countries where freedom is suppressed and free speech is punished, anonymity is a good weapon. Freedom writers using the Web can anonymously post their writings. Underground newsletters can be published and information from free countries can be disseminated. With anonymity people can express personal problems in forums without being embarrassed. But there's a dark side to this anonymity. Spam can be sent out - the "enhancement" type ads that fill up your inbox - and your child's inbox. Darker yet, a person can become whoever they want to be. A man can impersonate a woman, an elderly person can become young, a married person can become single – and a pedophile can become a child. Let's look at some child oriented crime directly related to Internet usage:

- In August of 2001, a 15 year old Massachusetts girl was abducted and sexually abused for a week after chatting with a couple in a chat room about problems with her parents.[7]
- May of 2002 in Connecticut, a 13 year old girl who regularly had provocative chats and sex with those she met, was strangled and dumped.[8]
- According to the FBI, "Online child pornography/child sexual exploitation is the most significant cyber crime problem confronting the FBI that involves crimes against children."[9]

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The Internet has also become a world-wide meeting ground for pedophiles: "Many factors of Internet technology have proven to be very attractive to child sexual abusers, pornographers and pedophiles. They flock to the Internet to share images and information about children and to make contact with children. They are major contributors to children's chat rooms, frequently pretending to be children themselves."[10]
The FBI has set up a branch of their Cyber Crimes unit called the "Innocent Images National Initiative"[11] and its purpose, according to the FBI's Crimes against Children site:
"The Innocent Images National Initiative (IINI), a component of the FBI's Cyber Crimes Program, is an intelligence-driven, proactive, multi-agency investigative initiative to combat the proliferation of child pornography/child sexual exploitation facilitated by an *online computer*." [12] [Italics mine]

And on this same site," Throughout the FBI, there was a 1,997% increase in the number of IINI cases opened between fiscal years 1996 and 2002 from 113 to 2,370. It is anticipated that the number of cases opened and the resources utilized to address the crime problem will continue to rise during the next several years."[13]

These are very disturbing statistics to ponder. A 1,997% increase! If the problem was not a prolific one, would the FBI need such a unit? To finish out this section, let's look at how the "Internet Crimes Against Children Task Force" based in Delaware Pennsylvania, lists the common activities of how children are exploited via the Internet:[14]

1) Online arrangements for the exchange, sale or purchase of child pornography. The actual exchange or delivery occurs through the mail or in hand-to-hand exchanges, e-mail, FTP, and other electronic means.
2) Arrangements between adults seeking sexual access to children, and adults willing to provide and/or trade children for sexual purposes.
3) Adults seeking sexual contact with children by establishing "friendships" with children online. Having "befriended" a child online, the pedophile then attempts to arrange a face-to-face meeting and, ultimately, the sexual exploitation of the child.

As shown, between the exposure of unwanted and mature types of Email in our kid's inbox, and not knowing if the person on the other end is who they really are, our technologically unprotected children are at risk from very damaging and possibly life threatening situations. Our next aspect looks at the reverse of the dangers from the Internet - the child/teen users themselves.

**The Flip Side**

Have you ever come home after a long day's work and your child grabs your hand and shows you the cool new Desktop they downloaded and installed on your computer? How about getting your butt kicked by an eight year old in a computer game? Or as my 11 year old said one day, "Daddy, I just clicked on

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

this picture and now the Internet looks different and this thing keeps popping up!" (Hmmmm…New browser and search tool installed, eh?) Do you wonder, "How do they know how to do THAT?!" Welcome to the world of today's technologically literate children. The ease with which children seem to absorb computer skills and make it work for them is amazing. They are being taught at school, by their peers and by their natural curiosity as children, to make a computer work for them, and to entertain them. They are beginning to accept computers as just a regular part of life. And no wonder. At "Internet World Stats"[15], a website that tabulates Internet trends and statistics based on Nielsen/ Net ratings and International Telecommunications Union data, shows that between the years 2000 and 2004, Internet usage in North America alone increased by 109.5% ! [16] Within the 2000 Census Bureau reports, demographics showed that 51% of American households owned computers and in those homes, 65% of children between the ages of 3 and 17 had access to the computers! [17] So with the increased exposure to computing and the Internet, from home and school, the kids are becoming proficient in computer usage. In an extremely interesting experiment in 1999-2000, a physicist in India, Dr. Sugata Mitra, installed computers in poor neighborhoods in New Delhi, India. He installed the computers into walls exposed to a street with a high speed Internet connection and left them on. He also watched from video cameras to see what would happen. He found that children between the ages of 6-12 used the computers the most and within days, without any instruction, the children had figured out how to draw with the computer and surf the Internet, among other things.[18] As children become more proficient we need to understand that their increased computer usage, particularly Internet usage, opens them up to the dangers posited in the previous section. Gaining computer skills at a young age is not all bad. As our world becomes more and more technologically advanced, our children should develop these skills. They will have to be proficient to be competitive in future job markets. But with these increasing skills come increasing dangers. It is not only danger from the Internet that needs to concern us, but danger arising from the aspect of being a child at all, and using the Internet.

It can be dangerous to be a user and be a child. A child tends to trust whatever comes from older people and whatever technology dishes out. For example, believing monsters are real and being scared after seeing a movie, or trusting that a web site is safe because it has cartoon-like graphics that are very colorful, are childlike traits. As a personal example, my young daughter had addressed an e-mail to a cartoon character on a website and signed it, "Your Girlfriend" and her name! While Mommy and Daddy were home! She did it innocently, thinking she was talking to a cartoon character, not understanding to what it could lead. The characters talked to other children and joked with them, and there were rainbows and animals. This did not appear threatening to her and led her to misjudge what an appropriate dialogue should be. This was a very enlightening experience! Innocence without intervention and protection can be exploited.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

As children get older and more mature, the variety of topics they become interested in gets broader. Whether it is a homework assignment or plain curiosity, the teen gets more exposure to greater areas of the Internet than just kid's game sites. This means possible exposure, either accidentally or purposefully to pornography, hacker sites, inappropriate blogging sites or chat rooms. All of these areas have that two-edged sword of anonymity working for them as well. The teen can be who they want to be - no pimples, skinny, bold, tall, older, etc. Through these exposures, again, comes the risk of coming across a predator or other unsavory types of individuals on the Internet, as well as addictive behaviors becoming entrenched in the teenager's life. Rather than posting more statistics, please refer to an excellent resource released by the "National Center for Missing and Exploited Children" titled "Online Victimization: A Report on the Nation's Youth".[19] This report clearly lays out many statistics and summaries on unwanted exposures to porn and how kids react to it, online seductions, unsolicited sexual requests, age ranges and many other facts relating to child Internet usage. This is highly recommended reading.

We also see in the news the bad side of teen computer usage:

- In 1998, two boys 15 and 16 years old broke into the Pentagon computers and planted backdoors.[20]
- Henrico County, Va., 2001, Students using issued laptops were hacking grades and downloading porn to share [21]
- A teenager in the UK broke into the Fermi lab and triggered a nuclear alert. [22]
- The year 2001- Remember 16 yr. old 'Mafiaboy' starting DDOS attacks against giant sites like Amazon.com and E-bay? [23]

Face it; some of today's youth are brilliant when using a computer and unfortunately, some turn their abilities to abusing their talents to gain attention or to be "31337". The majority of teen computer abusers though, are what is termed a "script kiddie". They are usually above average computer users, but not in that brilliant category. They enjoy community with the other so called "hackerz", who use other folks' programs and viruses to cause havoc. They seem to want to do this to fit in or gain some power or notoriety with friends, or get freely downloadable movies or software, but they are still a destructive or invasive segment of teens to deal with.

As some of the above paragraphs outline, there is also a danger to the children by the actions of the children themselves. Whether through innocent childhood trust, an immature view of life or active pursuits, perils exist to our children. The need for safeguards to protect them is the next focus. It is not a good topic to ignore. Specific focus will be on protecting the children in the school environment, but educating ourselves and others about child computer usage should be extended into the home as well.

**The Law and Students**

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Laws are enacted to fulfill a purpose. Laws protect citizens from crime, protect inventions or ideas, keep businesses above board and fair, etc. The fascinating thing about law is that a single law can create a boundary for both an offender and the responsibilities of the protected at the same time. Without laws defining responsibilities and protections, our great country would be a shambles. Imagine the crime rates if laws were even a little less slack! We have already examined a portion of society that needs protection from growing threats, resulting from a growing technology. As computing technology has grown, the Federal government has had to react and pass legislation alongside that technology to protect the public from its abuse. Federal and State governments have both legislated initiatives to install computers in schools and have passed laws designed to protect the users of those computers. Let's look at some of the Federal level legislation designed to protect students in our educational systems.

The first Federal law we'll look at is "CIPA", the "Children's Internet Protection Act".[24] This bill was introduced by Senator's McCain and Hollings in 1999 and passed in 2000, and requires schools and libraries to enact measures to protect minor's access to the Internet, as well as protecting any release of information about a student on the Internet. The law requires the following:

"Under CIPA, schools and libraries subject to CIPA do not receive the discounts offered by the "E-Rate" program (discounts that make access to the Internet affordable to schools and libraries) unless they certify that they have certain Internet safety measures in place. These include measures to block or filter pictures that: (a) are obscene, (b) contain child pornography, or (c) when computers with Internet access are used by minors, are harmful to minors:

1. Schools subject to CIPA are required to adopt a policy to monitor online activities of minors; and
2. Schools and libraries subject to CIPA are required to adopt a policy addressing: (a) access by minors to inappropriate matter on the Internet and World Wide Web; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) restricting minors' access to materials harmful to them. CIPA does not require the tracking of Internet use by minors or adults." [25]

As outlined, this law requires schools and libraries to conform to keeping the students safe or lose Federal discounts/funding.

Secondly a law was passed in 2003 called the "Protect Act"[26], which set up the "Amber Alert" program nationwide, increased severity of child pornography criminal penalties, eliminated statutes of limitations for sexual crimes against

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

children and allowed more law enforcement tools to prosecute these crimes. Though this law is not directly aimed at schools, it has implied responsibilities, as President Bush stated at the law's signing:

"This law carries forward a fundamental responsibility of public officials at every level of government to do everything we can to protect the most vulnerable citizens from dangerous offenders who prey on them." [27]

–President George W. Bush

We've looked at some Federal Legislation; now let's look at some State level law. Through the mandating of CIPA, every State in the nation has to enforce the protection of students in their education systems. (Laws exhibited as examples here are from the state of Virginia, though all states have similar laws and regulations in place.) Virginia has included protective regulations into two sections of the Code of Virginia:

- 22.1-70.2. Acceptable Internet use policies for public and private schools.[28]

  This section mandates each superintendent of every state school division to enforce acceptable use policies, Internet access regulations and filtering policies. Further, this section requires the superintendents to submit reports of compliance biennially.

- 42.1-36.1. Power and duty of library boards and certain governing bodies regarding acceptable Internet use policies. [29]

  This section is similar to the regulations for schools, but it is for libraries in every town and city and has provisions for juvenile protections as well. The reporting requirements are also biennial.

Further, the Virginia Department of Education has mandated that every school division develop and publish an Acceptable Use Policy (AUP) [30] establishing guidelines for responsible computer network and Internet usage. Usually the student and the students' parents are required to review and sign the policy, which ensures acknowledgement of responsibilities.

As we see, from the high levels of the Federal government to the local school down the road, child exploitation crimes have forced laws to be passed to protect our children. It is a travesty that we have to protect against such crime, but the harsh reality is there. Again, even though we in the Information Technology professions usually don't think about this topic much, it is a serious matter- especially for those networking professionals working in the educational systems around the country.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

## The Practicals of Protection

The completion of the process of protecting our students now moves from the abstracts of law to some practical means of protection at the school and individual student level. This can be accomplished in a number of effective ways, including educating our youth on proper network usage, structuring our networks to isolate and protect the student population and using protective software products, such as Internet filtering programs.

Right from the start, the firm belief in programs educating our students concerning the proper usage, etiquette and possible dangers faced from computer/Internet usage, tops this authors list. Beginning at home, parents can start the education process by surfing the 'Net with their kids, explaining terms, letting the child know what advertisements are versus the good content, and going through an online safety briefing with their child. There are many excellent websites on the Internet to help with online safety to aid the parent. Parents don't need to be wizards to explain and model good surfing habits and how not to just "click" away at the multitudes of links a website may contain. This is also a good time for the parent to set up the guidelines for what the child is allowed to do when at the computer and to review the sites the child may already be using. Send some e-mail with the child and let them know about not giving out personal information about themselves or their family. Parents should regularly check on what the older children are interested in on the 'Net and monitor which sites they may be going to.

At school, a properly structured program taught at the beginning of each school year in our computer labs or classrooms would go far in helping to inform students that the Internet and computers are wonderful tools, and not to be feared if they are aware of their downfalls. There are even CIPA compliant workshops such as one made available to school districts by the "Consortium for School Networking" (COSN)[31] organization, the "Safeguarding the Wired Schoolhouse" project. This workshop is to aid districts by instructing them about CIPA and how to become CIPA compliant. The COSN website offers many links to guides and organizations that aid in educating parents, teachers and children, not only about online safety, but legislation, how to choose proper products, write good Acceptable Use Policies, etc. Properly trained staff and student instruction go hand-in-hand to protect our children.

Moving into the network infrastructure side of student protections we will look at some possible networking solutions and implementations to physically and logically protect the students. As a disclaimer, this sub-section will not be exhaustive as many papers could be and have been written, on the topic of network infrastructure/security and how to deploy it. The ideas that are put forward result from experience working in a medium sized university environment as well as a public school environment and the ideas are designed to aid in demonstrating possible methods of protecting our students.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

One of the most successful means of student protection comes from actually creating an entire student network, separate from any administrative network. This can be accomplished by putting all student network servers and workstations on separately addressed network segments and utilizing VLAN's. Depending on which network operating system (NOS) is installed and the size of your network, the creation of separate student domains, workgroups, trees or OU's can be utilized extremely well for maintaining user and desktop policies. Within the Microsoft Windows environment the usage of Active Directory's Group Policy management can be setup to effectively "lockdown" a student's ability to do much other than what the schools AUP allows or what the student's classroom work requires them to do (but the students try anyway!). Group Policy/User management can restrict student logon hours, maintain a defined desktop on each workstation, and restrict what files and directories can be viewed on the workstation itself. Installation of any software other than by Administrators can also be prevented. These types of separations and tight management policies serve a few purposes:

1. If any students do want to try "hacking" or to try changing network equipment, the vital information on the administrative network will be isolated and make these efforts harder.
2. Monitoring the student Internet/network traffic and filtering usage are easier to implement.
3. Managing and changing just the student environment, such as installed applications, is a little easier.
4. Implementing the Defense-in-Depth principle in general.

Schools are required by the "Children's Internet Protection Act" to actively filter and monitor students activity. At each point of student network isolation some type of software or filtering appliance must be in place to filter and monitor all student Internet traffic. One enterprise application, for example is Symantec's "Web Security"[32]product. This content filtering proxy server not only filters and blocks inappropriate material and website access, but also provides reporting features, logging and inbound\outbound anti-virus protection as well. The state of Virginia has a list of approved products, so check your own state's regulations concerning approved product lists. Another possibility, depending on your current infrastructure, is to implement interior network firewalls before the student network in order to further manage what student traffic is allowed in or out. Also, it would be a good idea to examine whether or not to allow high school students to have e-mail accounts at school. This is a good thing/bad thing issue. As we know many viruses and worms are introduced via e-mail attachments. Student e-mail abuse could present problems, but on the other hand, some curricula, such as virtual businesses for example, may need e-mail accounts for interschool communications – a problem for the administration to iron out!

Finally, maintaining general security practices on the student network is essential:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Monitor security event logs on your student network servers
- Regularly monitor your firewall/proxy server logs and set up the proper notifications (Some school districts have security personnel who do just this.)
- Ensure you have a proper means of communications with your teaching staff for them to inform you of "weird" or out of place events on the student network (or strange student computer usage)
- Keep all antivirus protection updated
- Possibly setup an Intrusion Detection System
- Know your school regulations and policies

Setting up protections on a student network is a must, but with a properly setup environment, managing security becomes an easier task.

**Summary**

Our children are precious. They are our future. Watching parents whose children have become victims to sexual predators or exploited by other means is heart wrenching. The growth of anonymous technologies such as the Internet, have become an explosive phenomenon that drives our world's economies and have infiltrated throughout our society. Along with advantages, many disadvantages are apparent as the Internet has grown. Disastrous results of unsupervised usage have led to terrible consequences. Professionals in the IT world need to be vigilant and parents need to be educated and informed. Our children spend a good part of their lives attending school out of parental care and this time should be a time of learning, childhood experiences and joy. The children should not have to use these technologies fearfully. Networking professionals in the public schools need to remember the responsibility entrusted to them and help maintain a healthy learning environment. We have examined the negative side of the internet to which our kids may be exposed, laws designed to protect the children and practical ways to secure their computer use while spending a large portion of their lives in the public schools.

---

[1] http://www.usdoj.gov/criminal/fraud/idtheft.html#What%20Are%20Identity%20Theft%20and%20Identity

[2] http://www.megannicolekankafoundation.org/ctc.htm

[3] http://www.cnn.com/US/9705/30/megan.kanka/

[4] http://www.amberalertnow.org/aboutamber.html

[5] http://www.cnn.com/US/9609/26/davis.klass/

[6] http://www.foxnews.com/story/0,2933,110622,00.html

[7] http://abcnews.go.com/sections/us/DailyNews/sexslave010814.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

[8] http://www.cbsnews.com/stories/2002/05/31/national/main510739.shtml

[9] http://www.fbi.gov/hq/cid/cac/innocent.htm

[10] http://www.delcoicac.com/problem.html

[11] http://www.fbi.gov/hq/cid/cac/innocent.htm

[12] http://www.fbi.gov/hq/cid/cac/innocent.htm

[13] http://www.fbi.gov/hq/cid/cac/innocent.htm

[14] http://www.delcoicac.com/problem.html

[15] http://www.internetworldstats.com/stats2.htm

[16] http://www.internetworldstats.com/stats2.htm

[17] http://www.census.gov/prod/2001pubs/p23-207.pdf

[18] http://www.businessweek.com/bwdaily/dnflash/mar2000/nf00302b.htm

[19] http://www.missingkids.org/en_US/publications/NC62.pdf

[20] http://www.wired.com/news/politics/0,1283,14119,00.html

[21] http://www.edweek.org/ew/newstory.cfm?slug=20laptop.h21

[22] http://www.smh.com.au/articles/2004/02/03/1075776065349.html

[23] http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,56555,00.html

[24] http://www.fcc.gov/cgb/consumerfacts/cipa.html

[25] http://www.fcc.gov/cgb/consumerfacts/cipa.html

[26] http://www.usdoj.gov/opa/pr/2003/April/03_ag_266.htm

[27] http://www.whitehouse.gov/news/releases/2003/04/20030430-6.html

[28] http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+22.1-70.2

[29] http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+42.1-36.1

[30] http://www.pen.k12.va.us/go/VDOE/Technology/AUP/home.shtml#intro

[31] http://safewiredschools.cosn.org/workshops/index.html

**Reference:**

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

1. United States Department of Justice. "Identity Theft and Fraud" 6/5/2000
URL: http://www.usdoj.gov/criminal/fraud/What%20Are%20Identity%20Theft%20and%20Identity

2. Megan Nicole Kanka Foundation, Inc. "Megan's Law Coast to Coast"
URL: http://www.megannicolekankafoundation.org/ctc.htm

3. Cable News Network. "Repeat sex offender guilty in 'Megan's Law' case"
URL: http://www.cnn.com/US/9705/30/megan.kanka/

4. Amber Alert Now! Polly Klaas Foundation. "About the Amber Alert Plan"
URL: http://www.amberalertnow.org/aboutamber.html

5. Cable News Network. "Killer of Polly Klaas sentenced to death" Sept. 26,1996
URL: http://www.cnn.com/US/9609/26/davis.klass/

6. FoxNews. "Carlie Brucia Found Dead" February 06,2004
URL: http://www.foxnews.com/story/0,2933,110622,00.html

7. ABC News. "Teens Horrific Ordeal" August 14,2001
URL: http://abcnews.go.com/sections/us/DailyNews/sexslave010814.html

8. CBS News. "The Two Faces of a 13-Year-Old Girl" May 21,2002
URL: http://www.cbsnews.com/stories/2002/05/31/national/main510739.shtml

9. Federal Bureau of Investigation. Investigative Programs – Crimes against Children website.
URL: http://www.fbi.gov/hq/cid/cac/innocent.htm

10. Internet Crimes Against Children, Operation Triad Delaware, Pennsylvania "The Problem"
URL: http://www.delcoicac.com/problem.html

11. Federal Bureau of Investigation. Investigative Programs – Crimes against Children website.
URL: http://www.fbi.gov/hq/cid/cac/innocent.htm

12. Federal Bureau of Investigation. Investigative Programs – Crimes against Children website.
URL: http://www.fbi.gov/hq/cid/cac/innocent.htm

13. Federal Bureau of Investigation. Investigative Programs – Crimes against Children website.
URL: http://www.fbi.gov/hq/cid/cac/innocent.htm

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

14. Internet Crimes Against Children, Operation Triad Delaware, Pennsylvania
"The Problem"
URL: http://www.delcoicac.com/problem.html

15. www.InternetWorldStats.com website subsection "Internet Usage in North America"
updated February 29,2004
URL: http://www.internetworldstats.com/stats2.htm

16. www.InternetWorldStats.com website subsection "Internet Usage in North America"
updated February 29,2004
URL: http://www.internetworldstats.com/stats2.htm

17. U.S. Department of Commerce, Bureau of the Census publication
"Home Computers and Internet Use in the United States: August 2000"
Issued September 2001
URL: http://www.census.gov/prod/2001pubs/p23-207.pdf

18. Business Week online article. Edited by Judge,Paul.
"A Lesson in Computer Literacy from India's Poorest Kids" March 2,2000
URL: http://www.businessweek.com/bwdaily/dnflash/mar2000/nf00302b.htm

19. Finklehor, David , Mitchell, Kimberly J. , Wolak,Janis
"Online Victimization: A Report on the Nation's Youth"
by the Crimes Against Children Resource Center June 2000
URL: http://www.missingkids.org/en_US/publications/NC62.pdf

20. Wired News/Reuters "Teen Hackers to be Grounded" July 30, 1998
URL: http://www.wired.com/news/politics/0,1283,14119,00.html

21. Borja, Rhea R. "Student Misuse of School Laptops Forces District to Tighten Access"
January 30,2002 Education Week website.
URL: http://www.edweek.org/ew/newstory.cfm?slug=20laptop.h21

22. Sydney Morning Herald. "Teen hacker triggered nuclear terrorism alert"
February 4,2004
URL: http://www.smh.com.au/articles/2004/02/03/1075776065349.html

23. Verton, Dan "Teen Hacker 'Mafiaboy' Pleads Guilty to 55 Charges"
January 18,2001 Computerworld website
URL:
http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,56555,00.html

24. Federal Communications Commission. "Children's Internet Protection Act"
URL: http://www.fcc.gov/cgb/consumerfacts/cipa.html

25. Federal Communications Commission. "Children's Internet Protection Act"
URL: http://www.fcc.gov/cgb/consumerfacts/cipa.html

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

26. U.S. Department of Justice Release. "Fact Sheet Protect Act" April 30,2003
URL: http://www.usdoj.gov/opa/pr/2003/April/03_ag_266.htm

27. Bush, George W. President of the United States. Statement from White House press release upon the signing of the Protect Act. April 30, 2003
URL: http://www.whitehouse.gov/news/releases/2003/04/20030430-6.html

28. Code of Virginia section 22.1-70.2
URL: http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+22.1-70.2

29. Code of Virginia section 42.1-36.1
URL: http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+42.1-36.1

30. Virginia Department of Education website. "Acceptable Use Policies-A Handbook"
URL: http://www.pen.k12.va.us/go/VDOE/Technology/AUP/home.shtml#intro

31. The Consortium for School Networking website "Workshops" page
URL: http://safewiredschools.cosn.org/workshops/index.html

32. URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=60&EID=0

© SANS Institute 2004, Author retains full rights.

Last Updated: September 5th, 2015

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Crystal City 2015 | Crystal City, VAUS | Sep 08, 2015 - Sep 13, 2015 | Live Event |
| SANS Network Security 2015 | Las Vegas, NVUS | Sep 12, 2015 - Sep 21, 2015 | Live Event |
| SANS Seoul 2015 | Seoul, KR | Sep 14, 2015 - Sep 19, 2015 | Live Event |
| SANS Tallinn 2015 | Tallinn, EE | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Baltimore 2015 | Baltimore, MDUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| Data Breach Investigation Summit & Training | Dallas, TXUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Perth 2015 | Perth, AU | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS ICS Amsterdam 2015 | Amsterdam, NL | Sep 22, 2015 - Sep 28, 2015 | Live Event |
| SANS Bangalore 2015 | Bangalore, IN | Sep 28, 2015 - Oct 17, 2015 | Live Event |
| SANS Seattle 2015 | Seattle, WAUS | Oct 05, 2015 - Oct 10, 2015 | Live Event |
| SANS DFIR Prague 2015 | Prague, CZ | Oct 05, 2015 - Oct 17, 2015 | Live Event |
| SOS: SANS October Singapore 2015 | Singapore, SG | Oct 12, 2015 - Oct 24, 2015 | Live Event |
| SANS Tysons Corner 2015 | Tysons Corner, VAUS | Oct 12, 2015 - Oct 17, 2015 | Live Event |
| SANS Gulf Region 2015 | Dubai, AE | Oct 17, 2015 - Oct 29, 2015 | Live Event |
| SANS Tokyo Autumn 2015 | Tokyo, JP | Oct 19, 2015 - Oct 31, 2015 | Live Event |
| SANS Cyber Defense San Diego 2015 | San Diego, CAUS | Oct 19, 2015 - Oct 24, 2015 | Live Event |
| SANS Sydney 2015 | Sydney, AU | Nov 09, 2015 - Nov 21, 2015 | Live Event |
| SANS South Florida 2015 | Fort Lauderdale, FLUS | Nov 09, 2015 - Nov 14, 2015 | Live Event |
| SANS London 2015 | London, GB | Nov 14, 2015 - Nov 23, 2015 | Live Event |
| Pen Test Hackfest Summit & Training | Alexandria, VAUS | Nov 16, 2015 - Nov 23, 2015 | Live Event |
| SANS Hyderabad 2015 | Hyderabad, IN | Nov 24, 2015 - Dec 04, 2015 | Live Event |
| SANS Cape Town 2015 | Cape Town, ZA | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| SANS San Francisco 2015 | San Francisco, CAUS | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| Security Leadership Summit & Training | Dallas, TXUS | Dec 03, 2015 - Dec 10, 2015 | Live Event |
| SANS Milan 2015 | OnlineIT | Sep 07, 2015 - Sep 12, 2015 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |