KIDS ONLINE SAFETY GUIDE 101

Hari Pendyala
GSEC Practical Assignment Version 1.4b
May 12, 2004

Table of Contents

Summary

This research paper will present ways to protect children against the dangers of the Internet by using "Defense-in-Depth" principle. I will be explaining about Internet dangers, how and where to report if there is a problem, and early signs of problem. Also, I will focus on providing an extensive list of websites for further reading and software tools comparison.

Why I chose the topic

Recently, one of my friends asked me why when her 10 year old son tried to go to Yahoo's website (http://www.yahoo.com) he got redirected to an "Adult website" and it happened on both of her home computers. Fortunately, my friend's son is a good kid and has open communication with his parents and he went to his mom for help.

I did a little bit of searching and found that there was malware called "surebar" along with some other plethora of junk that was installed on the computer and they were causing URL redirection. After removing all the malware and junk from the computers, browsers started working fine.

To avoid problems like this in future, I had suggested to her, to install web filter software on her computer and she asked me which one. Till that moment, I had never tried to find out about software that protects from dangers of Internet. I had spent about 15 minutes searching the web for a good application and found out there is a lot of variety of software available, but couldn't recommend any particular software as couldn't figure which features were needed and which was the best software available.

So, that's when I decided to do some extra work on figuring out which software is good and what kind of features they offer and wanted to test the effectiveness of the available software.

Some of the facts and figures that support the importance of protecting children from dangers of Internet

From http://www.cyberangels.org

- Approximately 45 million children and teens have access to the Internet. By the year 2005 the growth of children and teens will exceed 77 million. Out of all these millions of children and teens only 1/3 of the households that have Internet access are proactively protecting their children and teens by using filtering or blocking software.

- An alarming 75% of children share personal information about themselves willingly over the Internet in exchange for goods and services.
- Only 25% of our children will tell a parent about an encounter with a predator who approached or solicited sex while on the Internet.
- In the United States, one out of five teens that regularly log on to the Internet have received unwanted sexual material through the web. This material includes requests to have sex or to have sexual talk and to give personal sexual information.
- One out of 33 youths will receive insistent sexual material.
- Online predators will contact 77% of youths by the age of 14, and 22% of children ages 10 to 13 will be approached

From http://www.protectkids.com

- "Dangerous Access, 2000 Edition" by librarian David Burt. 452 public libraries reported 2,062 incidents of Internet pornography accessed at libraries:
    - 41 cases of child porn being accessed
    - 472 incidents of children accessing pornography
    - 962 incidents of adults accessing porn
    - 106 incidents of adults exposing children to porn
    - 5 attempts to molest children in libraries

- The pedophile monitoring group, PedoWatch, has confirmed that online pedophiles are telling each other to use public libraries to download child pornography. PedoWatch is "one of the oldest organizations on the Internet that is working with law enforcement worldwide to remove child pornography and child luring activity," and currently works with "over 125 law enforcement officers" to monitor the activities of online pedophiles. (Dangerous Access, 2001 Edition, David Burt.)

- Public libraries have become a breeding ground for the sexual exploitation of children. (Donna Rice Hughes, Senate Hearing Testimony, 3/28/00)

For more facts and figures on Cyber Porn, Child Porn, Online-Predators, Pornography in public libraries, go to http://www.protectkids.com/dangers/stats.htm

As I progressed on the work, I found out installing software is NOT a panacea for the problem but just part of the solution. Solution should be based SANS principle mantra "Defense-in-Depth"

As mentioned in http://www.cyberangels.org/homefront/facts.html

- First line of defense is Parent's **knowledge** of Internet dangers
- Second line of defense is **Communicating** with children regarding dangers

- Third line of defense is Use of **software**

First line of defense – Knowledge of Internet dangers

Even though some families don't own a computer at home, chances are very high that the kid will be using one at school. So all parents should learn about Internet dangers and talk about them to their kids.

Some of the Internet Dangers are

- Adult Websites
- Loss of Privacy
- Identity Theft
- Online/Chat room Predators
- Viruses
- Malware/Browser Hijack
- Sites that contain bomb making, weapon usage,
- Sites that encourage usage of drugs
- Gambling Sites
- Sites that contain Racist or Hate messages

Adult Websites

These are websites that have pornographic content not suitable for children under 18. Following are some of the examples of how pornography harms children (Source http://www.protectkids.com/effects/harms.htm)

- *Exposure to Pornography Threatens to Make Children Victims of Sexual Violence*
- *Exposure to Pornography Frequently Results in Sexual Illnesses, Unplanned Pregnancies, and Sexual Addiction*
- *Exposure to Pornography May Incite Children to Act Out Sexually against Other Children*
- *Exposure to Pornography Shapes Attitudes and Values*
- *Exposure to Pornography Interferes with a Child's Development and Identity*

Facts mentioned below, shows that parents, educators have an uphill task of protecting kids from these adult sites (Source http://www.protectkids.com/dangers/stats.htm)

- There are 1.3 million porn websites (N2H2, 9/23/03).

- More than 32 million unique individuals visited a porn site in Sept. of 2003. Nearly 22.8 million of them were male (71 percent), while 9.4 million adult site visitors were female (29 percent) (Nielsen/Net Ratings, Sept. 2003).

- More than 20,000 images of child pornography are posted on the Internet every week (National Society for the Prevention of Cruelty to Children, 10/8/03).

- 140,000 child pornography images were posted to the Internet according to researchers who monitored the Internet over six weeks. Twenty children were estimated to have been abused for the first time and more than 1,000 images of each child created (National Society for the Prevention of Cruelty to Children, 10/8/03).

- More than half of all illegal sites reported to the Internet Watch Foundation are hosted in the United States. Illegal sites in Russia have more than doubled from 286 to 706 in 2002 (National Criminal Intelligence Service, 8/21/03).

Loss of Privacy

Giving your address, phone number, or even your full name to a stranger can put you or your family members in danger. It is very important to tell your children not to give out any information that could harm family and friends. Lot of websites collect this information about children for use in marketing, fundraising, and other activities by luring them to register for contest or in exchange for prizes. Children should never reveal any information about themselves without first checking with their parents.

Since U.S.Government feels that protecting the privacy of children is very important and to prevent abuse of personal information while you are shopping or just browsing the internet, The Federal Trade Commission has passed new rules for website operators to make sure kids' privacy is protected. These new rules are part of 1998 Children's Online Privacy Protection Act (COPPA). This rule applies to all commercial website operators, Operators of general audience sites, Operators of general audience sites that have a separate children's area, whose services are directed towards children under 13 and collect information from children under 13.

There are some tools available on the Internet that analyze your computer and tell you what information is collected from your computer without your knowledge when you visit a website. One such tool is available at http://www.privacy.net/analyze/.

Online/Chat room Predators

Predators/Pedophiles use chat rooms, instant messaging and email to lure children who are susceptible. They target a potential victim and seduce the victim in stages, first with words and then physically. Some facts regarding online predators -

- Internet pedophiles are increasingly adopting counter-intelligence techniques to protect themselves from being traced (National Criminal Intelligence Service, 8/21/03).
- Forty percent of people charged with child pornography also sexually abuse children, police say. But finding the predators and identifying the victims are daunting tasks (Reuters, 2003).

For more information on how Online Predators seduce children, go to http://www.cyberangels.org/homefront/predator.html

Identity Theft

This is one of the fastest growing crimes today. According to Visa.com approximately about 700,000 individuals fall victims to this crime every year and once thieves get details about your identity, they can

- Open new bank accounts and write bad checks.
- Establish new credit card accounts and not pay the bills.
- Obtain personal or car loans.
- Get cash advances.
- Set up a cellular phone or utility service and run up bills.
- Change your credit card mailing address and charge on your existing accounts.
- Obtain employment
- Rent an apartment, but avoid the rent payments and get evicted

If you had given credit card to your children, tell them not use credit card either on-line or off-line without your permission.

Dumpster Diving, Mail Theft, Purse or Wallet Theft, Inside Sources, Imposters, Online Data, Documents in the home are some of the ways thieves steal your identity.

To prevent Identity theft (http://www.usa.visa.com/personal/secure_with_visa/identity_theft_prevention.html)

Do

- Shred all personal and financial information-such as bills, bank statements, ATM receipts, and credit card offers-before you throw it away.
- Keep your personal documentation (e.g., birth certificate, Social Security card, etc.) and your bank and credit card records in a secure place.
- Be aware of your surroundings when entering your Personal Identification Number (PIN) at an ATM.
- Limit the number of credit cards and other personal information that you carry in your wallet or purse.
- Report lost or stolen credit cards immediately.
- Cancel all inactive credit card accounts. Even when not being used, these accounts appear on your credit report, which is accessible to thieves.
- If you have applied for a credit card and have not received the card in a timely manner, immediately notify the appropriate financial institution.
- Closely monitor the expiration dates on your credit cards. Contact the credit issuer if the replacement card is not received prior to your credit card's expiration date.
- Sign all new credit cards upon receipt.
- Review your credit reports annually.
- Use passwords on your credit cards, bank accounts, and phone cards. Avoid using the obvious passwords-your mother's maiden name, your birth date, and the last four digits of your Social Security or phone number.
- Match your credit card receipts against monthly bills to make sure there are no unauthorized charges.

Don't

- Volunteer any personal information when you use your credit card.
- Give your Social Security number, credit card number, or any bank account details over the phone unless you have initiated the call and know that the business that you are dealing with is reputable.
- Leave receipts at ATMs, bank counters, or unattended gasoline pumps.
- Leave envelopes containing your credit card payments or checks in your home mailbox for postal carrier pickup.

- Record your Social Security number or passwords on paper and store them in your wallet or purse. Memorize your numbers and/or passwords.
- Disclose bank account numbers, credit card account numbers, and other personal financial data on any web site or online service location, unless you receive a secured authentication key from your provider.

To learn more about how to prevent Identity Theft, go to http://www.usa.visa.com/personal/secure_with_visa/identity_theft_prevention.html?it=il_/personal/secure_with_visa/identity_theft.html

Viruses

According to http://www.webopedia.com, Virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves.

According to International Computer Security Association (ICSA), so far there are more than 60,000 viruses have been identified and 400 new ones created every month.

If your computer is infected with a virus, it could delete files on your computer, steal your documents by mailing them. If you don't know what kind of damage virus did to your computer, you might need to reformat and reinstall your computer. So, don't let your kids download unknown programs from the Internet and install them on your computer.

You need to purchase and install an Anti-Virus program to protect your computer in real-time. Make sure you keep your virus definition/pattern files up-to date by downloading them automatically or manually. Some of the popular anti-virus software

Trend Micro Inc	(http://www.antivirus.com)
Symantec	(http://www.symantec.com)
Mcafee	(http://www.mcafee.com)
BitDefender	(http://www.bitdefender.com)

There are some free online scanners available, if you need to scan your computer for viruses and they are

Trend Micro's Housecall	(http://housecall.antivirus.com)
PandaSoftware ActiveScan	(http://www.pandasoftware.com)
BitDefender Scan Online	(http://www.bitdefender.com)
Kasperscky Online Scanner	(http://www.kaspersky.com)

Malware

According to Trend Micro, Malware – short for malicious software – refers to any malicious or unexpected program or code such as viruses, Trojans, and droppers. Not all malicious programs or codes are viruses. Viruses, however, occupy a majority of all known malware to date including worms. The other major types of malware are Trojans, droppers, and kits.

Ad-aware, BHODemon, Browser Hijack Blaster, HijackThis are some of the freeware tools available to remove malware from your computer.

Sites that contain Offensive material

(Drug usage, Racist or Hate messages, Gambling sites, Bomb/weapon making)

The Internet doesn't cause kids to use drugs or weapons, but it might be an encouraging factor. The students responsible for Columbine Massacre and De Anza College Bomb Plot, got information about bomb making and using weapons from Internet.

On Feb 1, 2003 there was news about a child in Phoenix, AZ that took a fatal over dose while his Internet pals watched.

Like real Casinos, kids should not be allowed to access any gambling sites whether it is just for fun or for money.

Whom to contact

How and where to report when there is a problem with

Loss of Privacy

Parents and others can submit complaints to the FTC through *www.ftc.gov* or call toll-free number (877) FTC-HELP

Identity Theft

(http://www.usa.visa.com/personal/secure_with_visa/identity_theft_if.html?it=il_/personal/secure_with_visa/identity_theft.html)

- Make a single toll-free call to one of the national credit bureaus
- File a Police Report
- Contact Creditors' Fraud Departments
- File a Complaint with the Federal Trade Commission (FTC)

Online Predators

- If you feel any kid is imminent danger from a predator, call 911 emergency line or local Police

- If you see any child pornography, pl. report it to Child Pornography Tipline 1-800-843-5678 or http://www.cybertipline.com/, http://www.missingkids.com

Early warnings about problems with your kids' online surfing

There are lots of early warnings, if your kid is doing something online, which he/she not supposed to. According to http://www.cyberangels.com, some of the warnings are

- **Screen Switching** If your child quickly changes screens or turns off the monitor when you come into the room, it is likely they are viewing something they don't want you to see.
- **Odd Phone Calls** If your child suddenly begins receiving phone calls from strange adults (or even other children) or if you see unexplained long distance charges or phone numbers on your phone bill, you may have a problem.
- **Odd hours of the night** If your child is up typing away in the wee hours of the night he may be chatting online. This activity should be reserved for times and places that are supervised.
- **Sudden influx of cash** If your child suddenly has more cash than can be accounted for, or shows up in unfamiliar clothing or with gifts that you can't explain - pedophiles often spend a great deal of money cultivating a relationship with a child.
- **Unusually upset at an Internet interruption** It is not normal to cry to be overly upset when the Internet goes down for an hour or two.
- **Withdrawal** from family or friends. Pedophiles work very hard to drive a wedge between children and the people who support and care for them. The larger the gap between the child and his family, the easier it is for a predator to create a relationship.

To learn more about Internet and Internet dangers, it is good to take some classes in local community college or on-line classes from websites like http://www.cyberangels.com, http://www.wiredsafety.org/

Second Line of Defense – Communicating with children

Just learning about the Internet dangers will not protect the children, Parents must communicate it to them. It is a good idea to talk about the danger of the Internet before the problem occurs.

Both kids and parents should sign the following Internet use Agreement (https://www.safekids.com) and post is it near the computer. If you want you can add more items.

Family Contract for Online Safety

Kids' Pledge

1. I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.
2. I will tell my parents right away if I come across any information that makes me feel uncomfortable.
3. I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.
4. I will never send a person my picture or anything else without first checking with my parents.
5. I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the service provider.
6. I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.
7. I will not give out my Internet password to anyone (even my best friends) other than my parents.
8. I will be a good online citizen and not do anything that hurts other people or is against the law.

I agree to the above

____
Child sign here

I will help my child follow this agreement and will allow reasonable use of the Internet as long as these rules and other family rules are followed.

____
Parent(s) sign here

Family Contract for Online Safety
Parents' Pledge

1. I will get to know the services and Web sites my child uses. If I don't know how to use them, I'll get my child to show me how.
2. I will set reasonable rules and guidelines for computer use by my children and will discuss these rules and post them near the computer as a reminder. I'll remember to monitor their compliance with these rules, especially when it comes to the amount of time they spend on the computer.
3. I will not overreact if my child tells me about a problem he or she is having on the Internet. Instead, we'll work together to try to solve the problem and prevent it from happening again.
4. I promise not to use a PC or the Internet as an electronic babysitter.
5. I will help make the Internet a family activity and ask my child to help plan family events using the Internet.
6. I will try to get to know my child's "online friends" just as I try get to know his or her other friends.

I agree to the above

____
Parent(s) sign here

I understand that my parent(s) has agreed to these rules and agree to help my parent(s) explore the Internet with me.

____
Child sign here

You can make Online Safety teaching fun by going to the following websites

- Online Safety Quiz (http://www.safekids.com/quiz/index.html)
- Fun website about Online safety http://www.netsmartz.org/flash/index.html
- Make your Kids earn a web license by going to http://pbskids.org/bts/license/?next=1
- Another good example of Internet Use agreement http://www.ftc.gov/bcp/conline/pubs/online/kidzbmark.pdf
- Internet Safety game for teens, http://www.kidscom.com/games/isg/isg.html

Third line of defense – Software

The software is broadly classified into the following categories

- Filtering
- Monitoring
- Time Limiting
- ISP based
- Browser based

Filter software

The majority of filtering software blocks all adult content materials including pictures and sexually explicit text, but none of them is 100% fool proof. In the early days of filtering software, the software manufacturer decided which sites, which words, which type of content to block, but not any more. Many of the filtering software have started giving control to the user, so that consumer has better control over what to see and what not to see. Of course, this control is protected by a password and only authorized users (Parents) can change it.

Sample list of companies that provide filtering software (http://kids.getnetwise.org/tools/tool_result.php3?display_start=1&functionality_id_array%5B%5D=931452496.23087)

- AOL Parental Controls
- NetNanny
- CYBERsitter
- SurfPass
- Kiddefender
- CyberPatrol
- Kidsnet
- McAfee Parental Controls 1.0
- Norton Parental Control
- Trend Micro PC-Cillin

Monitoring Software

These tools allow parents to monitor Kids' online activity and they just keep track of applications used, sites visited etc. They don't prevent kids from accessing any of the inappropriate websites.

Sample list (http://kids.getnetwise.org/tools/tool_result.php3?display_start=1&functionality_id_array%5B%5D=931542385.18341)

- AOL Parental Controls
- NetNanny
- CYBERsitter
- SurfPass

Time limiting software

This type of software allows you to set time limit on your Kids Internet usage.

Some of the tools are (http://kids.getnetwise.org/tools/tool_result.php3?display_start=1&functionality_id_array%5B%5D=931452504.82116)

- AOL Parental Controls
- NetNanny
- CYBERsitter
- SurfPass

ISP based

There are lots of National ISP services that provide filtered access to Internet. This list can be obtained by searching using your favorite search engine "Family ISP Listings" or "Filtered Access ISP".

Following is the list from Yahoo

http://dir.yahoo.com/Business_and_Economy/Business_to_Business/Communications_and_Networking/Internet_and_World_Wide_Web/Network_Service_Providers/Internet_Service_Providers__ISPs_/National__U_S__/Filtered_Access/

Browser software

This type of software allows children to browse the internet safely through a web browser.

(http://kids.getnetwise.org/tools/tool_result.php3?display_start=1&functionality_id_array%5B%5D=1049731107.1234)

- AOL Parental Controls
- Crayon Crawler
- Noah's Web

Majority of the software vendors offer free trials. Based on the features offered, try them before purchasing. Majority of the mentioned software are commercial software. Free software tools are also available like http://www.we-blocker.com/
A product guide for Internet utilities is available at http://www.pcmag.com/category2/0,1738,2202,00.asp
An excellent review of Internet filter software is available at http://www.internetfilterreview.com.

Conclusion

Use "Defense-in-Depth" principle. Put your computer in a common room like family room so that you can keep an eye on your kid. Check your computer for any adult content pictures or text; check the browser's history file after your kid done browsing.

Software is not 100% effective and not fool proof. Some can be bypassed by using anonymous browsing websites (http://www.the-cloak.com/anonymous-surfing-home.html), Peer-to-Peer applications like Kazaa, Morpheus. Also it is good practice to scan your computer periodically for any ports that are open with out your knowledge (https://grc.com/x/ne.dll?bh0bkyd2) and for viruses and malware.

References

http://www.ftc.gov/kidzprivacy - FTC's website on Kid's privacy and provides lot of resources for teachers, parents. It also provides lot of information on COPPA.

http://www.fbi.gov/publications/pguide/pguidee.htm - Very good guide for Parents from FBI

Protecting your privacy as you surf the web – by John Batteiger (San Francisco Chronicle July 25, 2001)

http://www.getnetwise.org - Their mission is to be "one click away" from the resources that parents need to make informed decisions about their family's use of the Internet.

http://www.cyberangels.org - Their mission is to be “Virtual 411” for to address the concerns of parents, the needs of children, on-line abuse and cyber crime, while supporting the right of free speech.

http://www.safekids.com - Larry Magid, a broadcaster and syndicated columnist and author of numerous articles about online safety operates SafeKids.Com, SafeTeens.Com and The Online Safety Project

http://www.netsmartz.org - The NetSmartz is an interactive, educational safety resource from the National Center for Missing & Exploited Children® (NCMEC) and Boys & Girls Clubs of America (B&GCA) for children aged 5 to 17, parents, guardians, educators, and law enforcement that uses age-appropriate, 3-D activities to teach children how to stay safer on the Internet.

http://pbskids.org/ - Website operated by pbs.org for kids

http://www.kidscom.com - KidsCom has kids games, chat rooms for kids, video game cheats and other child activities. Our kids' games focus on fun, learning and Internet safety.

http://dev.btcs.org/safety - Website operated by Bristol Tennessee City School System, Tennessee

http://www.epic.org - EPIC is a public interest research center in Washington, D.C. Their mission is to focus public attention on to protect privacy, the First Amendment, and constitutional values.

http://www.epic.org/privacy/tools.html#surf - Provides list of website that allow anonymous browsing

http://www.privacy.org - This web site is a joint project of the Electronic Privacy Information Center (EPIC) and Privacy International.

http://grc.com/default.htm - Gibson Research Corporation is owned and operated by Steve Gibson. This website provides collection of freeware to protect your computer.

http://www.webopedia.com - Webopedia is a free online dictionary for words, phrases and abbreviations that are related to computer and Internet technology. Webopedia provides easy-to-understand definitions in plain language.

http://www.linuxadvisory.com/forums/thread414.html -- Provides list of Malware tools available for windows

http://history1900s.about.com/library/weekly/aa041303a.htm - An article on Columbine massacre

http://www.cnn.com/2001/LAW/02/01/campus.bombs/ - News article on De Anza College, Cupertino, CA student Bomb plot

http://www.the-cloak.com/anonymous-surfing-home.html -- One of the sites that provides anonymous browsing

http://www.visa.com - Provides lot of information of Identity theft

http://www.kazaa.com/us/index.htm - One of popular peer-to-peer software

http://www.morpheus.com/ - Another popular peer-to-peer software