Global Information Assurance Certification Paper

CyberPorn Tricks and Awareness

By

Stephen Karrick

GSEC Practical Assignment Version 1.4b

CyberPorn Tricks And Awareness

Abstract

Today, parents throughout the world face an everyday challenge to provide the very best protection, education and opportunities for their children. An increasingly difficult and challenging task is protecting their children on the Internet against inappropriate material such as online pornography. Often these parents are unaware of the methods and tricks pornographers facilitate to invade their computers and intrude on their privacy. How can they fight an enemy that may appear at any given time and reappear when least expected? Why does this obscenity appear on their computer when they are not actively searching for it? Who may they call to report such a nuisance? This project is going to answer these questions and provide parents with some insight to what their children (unfortunately) may experience on the Internet.

During this writing I was helping my nine-year-old daughter with a school project. I asked her to go to www.dictionary.com. As she was scrolling down the page she said, "Dad, I went to dictionary.com but this does not look like a dictionary." She had accidentally typed http://www.dicionary.com and missed the "t". This site bounced to http://amaturevideos.nl and then immediately to a porn site called http://hanky-panky-college.com. I started to dig deeper!

WARNING: Some of the material you are about to read is offensive, disgusting, and obtrusive, yet factual. Part of my pedagogical theory is that explaining is insufficient and must be demonstrated with burden of proof in order for readers to appreciate the importance of these issues. To provide a notional situation is informational but displaying the real live exhibition will expand the reality and importance of the subject.

Note: All websites referenced in this paper are active at the time of this writing. There is no guarantee that the sites will remain online.

Methods of Pornography By Deception

> Large percentages of youth Internet users are exposed to sexual material when they are not looking for it. The sex on the Internet is not segregated and signposted like in a bookstore, and is not easy to avoid. *U.S Department of Justice*, *FS 200104*

Deception is the most common technique for tricking innocent Internet users to visit their web site. Due to the large number of pornographic sites and the limited amount of exact names such as sex.com or porn.com, many adult sites revert to alternative methods to attract customers. These methods lead to a variety of pornographic sites that may include child porn, gay men, lesbians, rape, bestiality and other disgusting graphics.

Stealth Sites

Stealth sites are designed to use innocent words to avoid immediate detection. For instance, according to a report from the National Center For Missing and Exploited Children, a fifteen-year-old boy and his friend were searching for information on water sports. Their search led them to www.watersports.com. The watersports.com advertisement slogan is "The Wettest Site on the Net". This site displays graphical exploitations of women urinating and live "streaming video"!

Other similar examples are:

1.) http://www.whitehouse.com/- advertises over 75 million visitors since 1997
2.) http://www.coffebeancatalog.com/ - gay, bondage, leather, interracial gay
3.) http://www.clothingcatalog.com/ - rape fantasies, bestiality, black desires, zoo sex
4.) http://www.boys.com/ - redirects to a gay men site
5.) http://www.crimetop.com/ - rape pictures, movies, stories

Misspelling

> In October 2001, the FTC charged that the defendant, John Zuccarini, was registering Internet domain names that were misspellings of legitimate domain names or that incorporated transposed or inverted words or phrases. For example, Zuccarini registered 15 variations of the popular children's cartoon site, www.cartoonnetwork.com, and 41 variations on the name of teen pop star, Britney Spears (britnayspears.org). *Federal Trade Commission, May 24, 2002*

Nobody ever types a word incorrectly or misspells a word by accident…do they? It is possible to do both and be directed to an adult site preying upon these mistakes. A perfect example is mentioned in the introduction of this paper. A typographical error of entering *dicionary.com* rather than *dictionary.co***m** leads to www.hanky-panky-college.com.

In this instance, the pornographer tricks you into entering the www.hanky-panky-college.com web site and then immediately attempts to capitalize on the fact that the site is “As Seen On The Howard Stern Show”. As soon as a link on this home page is clicked, the Internet user is bombarded with a plethora of pop-up windows offering assorted types of porn. The pornographer is hoping to display a capturing graphic to entice a future customer. A theory is that some people get so tired of clicking and closing the pop-ups that they eventually submit their credit card.

Among the array of pop-ups is an opportunity select an easy method of payment for immediate access. *Figure 1* is a screen shot that provides the instructions to access a porn site without a credit card. The user dials the phone number listed, receives a code and enters it into the web site. The user is then allowed access for the remainder of the call. Some phone calls may charge as much as $8.00 per minute! This may appeal to those hesitant to use a credit card online or those worried about it appearing on their credit card bill.

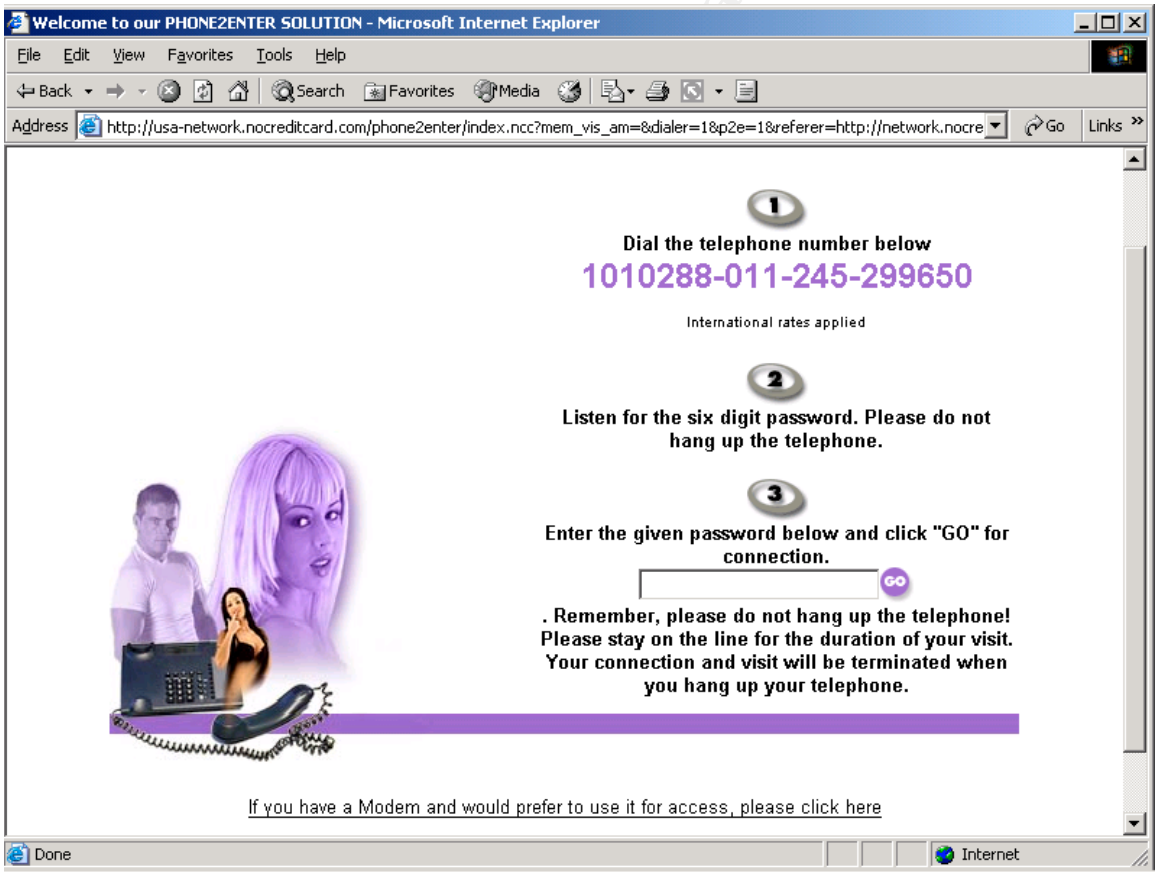

Figure 1: Instant Porn Access Via a Phone Call Without using a Credit Card

That’s it! Any person that can read, follow directions, and make a phone call can have instant porn. Setup is effortless and no credit card authorization is needed.
.

Misspellings are commonly tracked on Google and other search engines. If you mistype or misspell a word such as "*hurricane*" and spell it "*huricane*" with one "r", the search engine will make an attempt to help you by asking you something similar to " Did you mean *hurricane*?" and offer a link to correct your entry. An adult web site developer accessing the historical data of commonly mistyped or misspelled words can use this information to register a new domain name or trick Internet surfers into visiting other porn sites. These are specifically constructed to take advantage of these mistakes.

A search for "Britney Spears" is currently very popular in search engines. *Figure 2* illustrates a three-month historical record of Google's spelling correction system for variations of "britney spears". The first entry is the correct spelling and corresponding queries for "britney spears". The subsequent entries are various spellings used by at least two unique Internet users during a three-month period. The mistakes were corrected to "britney spears" by Google's spelling correction system. Right away a site named brittanyspears.com may have received a portion of the 40,134 queries.

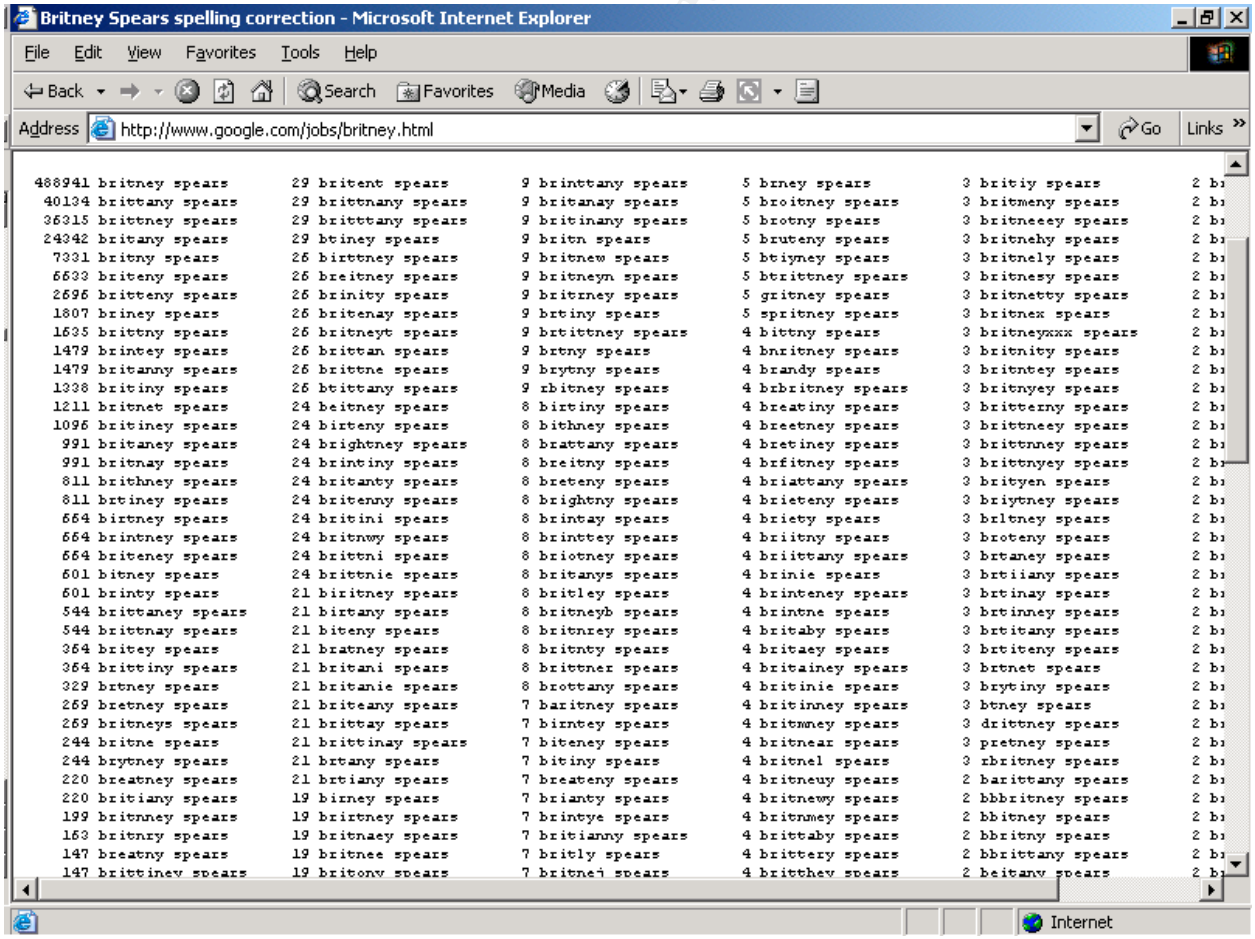

Figure 2. Google's Data of Misspellings for Britney Spears

A couple of other examples intentionally designed to take advantage of a typographical error or misspellings are:

1. http://www.teeen.com/ vs. www.teen.com
2. http://www.amaturevideos.com vs. www.amateurvideos.com
3. http://www.freeacrade.com vs. www.freearcade.com. This link will also redirect you to www.hanky-panky-college.com

Porn Napping

> An educational Web site run by Ernst & Young has been replaced by a XXX porn site featuring "165,000 Barely Legal Teen Movies", the global professional services company admitted yesterday. *The Register, October 2001*

Porn Napping is a phenomenon that involves expired domain names (like your business.com or yourchurch.org). It is a relative of Cyber Squatting where someone purchases an expired domain name with the intention of selling it to someone at an inflated price. Porn napping is somewhat similar. A person purchases the domain name and reconstructs the homepage into a porn site with the intention that the original owner will quickly pay a price to resume ownership of the domain.

> One result of "porn-napping" is that in the last 19 months, the number of web pages with adult content has grown four times as fast as the overall number of web pages, according to Rule Space, a web-filtering company in Portland, Oregon.
> *Agape Press*, *Ministries, Churches Susceptible to 'Porn-Napping' 2002*

According to the Online Internet Institute, the following are a couple of the latest examples of porn napping:

Baggett Investigations	http://www.baggettinvestigations.com/ 02/13/03	
Michigan Techlit Grants	http://www.mi-techlit.org/	04/12/03

> The United States Congress last week passed legislation criminalizing pornographers who deliberately mask web sites behind innocuous-sounding domain names. *Recycled-Traffic.com, April 20, 2003*

False Advertising

Most legitimate businesses refrain from selling advertising space to pornographers and most banner exchange programs forbid pornography. So how do they get around this? Many pornographers create a fake web site equipped linking banners, graphics, and/or logos to place on other web sites that

have a link back to their fake web site. Once approved from the linking web site, they then replace the original fake page with their real pornographic website.

Developers also create false error messages or warnings designed to trick you into clicking the OK button. This is often a link to one of their adult web sites. An example is shown in a form of Mouse Trapping explained later in this document.

Doorway Scams

Keywords are the most popular methods to find related web sites. Web sites owners purchase keywords to have their ads pop-up on a search engine and direct increased traffic to their web site. Keywords like sex, anal and blowjob can sell for six figures. Adult web developers tailor their sites to popular keywords.

A version of a Doorway scam is to create a porn site that will get listed in the search engines whenever selected non-porn keywords are entered. For example, a search for "zoo farm" displays a bestiality porn site listed as one of the top ten web sites as seen in *Figure 3*.

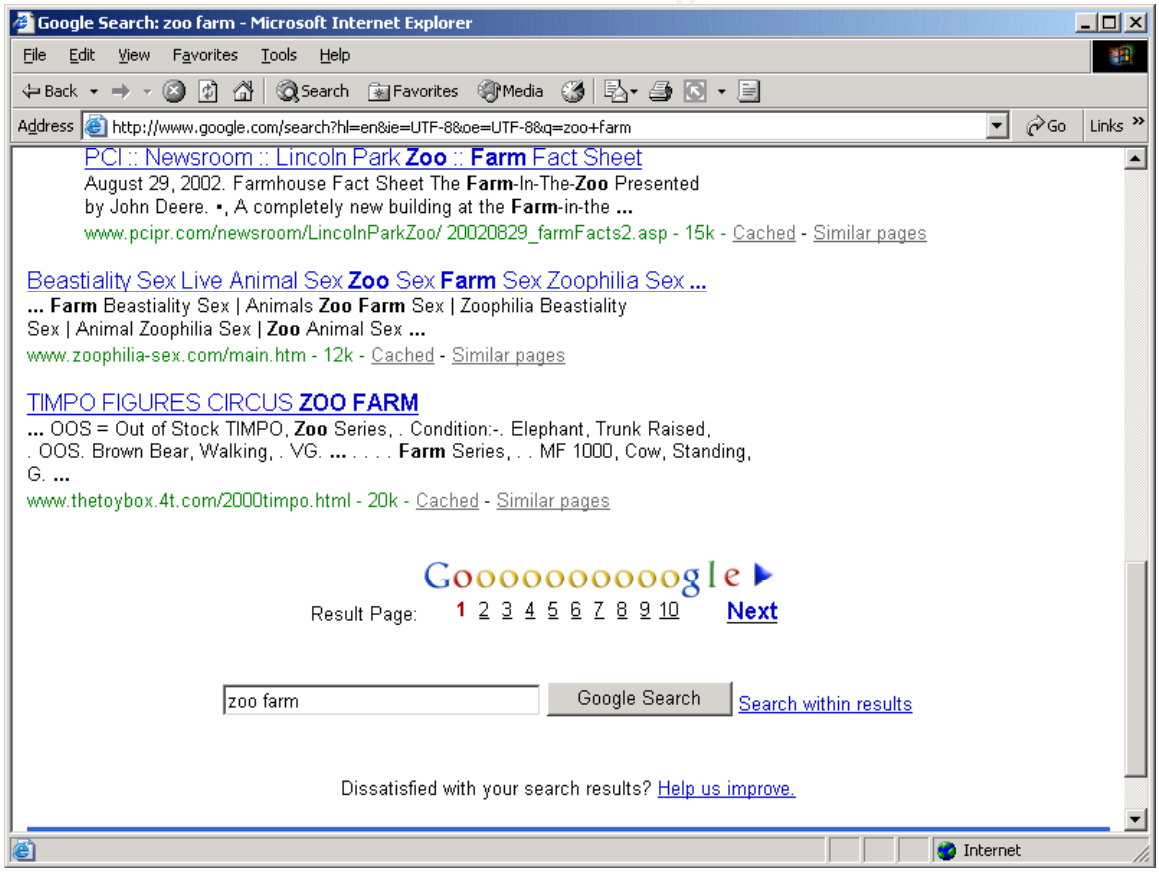

Figure 3. Google search of "zoo farm"

Another popular Doorway scam is to take advantage of celebrity names such as Halle Barry, Cameron Diaz, Anna Kournikova or Jennifer Lopez. The web

designer will design the porn site using these names in places like the site title, description, and metatags. The search engines seek out this information and display the results when these names are actively searched.

Once you enter the name you might think you are intended for a legitimate web site but in all reality you are directed to a pornography site. This trickery also pertains to searches like Pokeman and Action Man or brand names like Disney, Barbie and Nintendo. It is also estimated that twenty-five percent of porn sites use this type of scheme.

Entrapment

> "If you are lucky enough to get a surfer from the AVS' [Adult Verification Service] link list (or anywhere else for that matter), you should do everything that you can to keep him within your own network – unless of course you can send him off to a sponsor and make some money from him – you don't want him returning back to the AVS' link list (or wherever else he came from). You can do this by using internal links to keep him within your own family of sites. This can be as simple as adding "next gallery" links, or as complex as building your own link list, top list, or even your own private web ring." *[advice from AVS Sites for Profit]*

Pornographers want to keep you trapped in their world for profit. The more clicks, the more dollars, the more time, the more dollars, the more credit cards, the more dollars. Contractors known as “script jockeys” are often hired to create all manner of annoying consoles, phony link tricks, pop-up windows and other in-your face sales tools. Entrapment is one of the best-known methods to capture and hold Internet users.

Mouse Trapping

> Clicks on the "close" or "back" buttons caused new windows to open." After one FTC staff member closed out of 32 separate windows, leaving just two windows on the task bar, he selected the "back" button, only to watch the same seven windows that initiated the blitz erupt on his screen, and the cybertrap began anew," *FTC v. John Zuccarini, Federal Trade Commission, May 24, 2002*

Mouse trapping, or disabling a Web surfer's browser controls is used almost exclusively at pornographic sites now although modified versions can be found throughout the Internet. Many times they will disable the Close button, Back button and/or the X on the upper right hand corner of Microsoft Internet Explorer.

Mouse trapping involves two separate actions: changing, or disabling your browser's functions and using a programming language such as JavaScript to present new windows that pop up, seemingly at random but

are actually planned in a script. *Figures 3-7* demonstrate a series of consecutive Alert boxes. These Alert boxes force a user to click either OK or the X to close the box in order to continue. This is the simplest and least effective form of mouse trapping. A sample script to create an Alert Box is included in Appendix A.

Figure 3. Popup #1, once clicked, popup #2 appears

Figure 4. Popup #2, once clicked, popup #3 appears

Figure 5. Popup #3, once clicked, popup #4 appears

Figure 6. Popup #4, once clicked, popup #5 appears

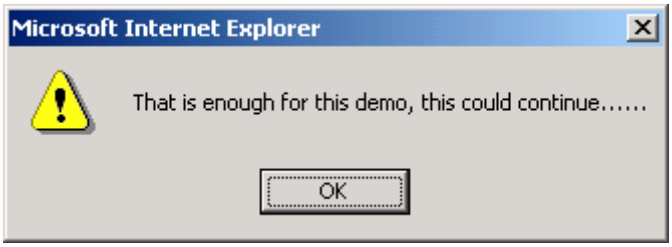

Figure 7. Popup #5, once again it can take you anywhere

Looping

Porn looping involves a Web surfer trapped in a never-ending loop with new windows appearing one right after another. They use complicated links to keep you within their site or family of sites---a private web ring. You can be kept in an even more complex and labyrinth trap. Your Browser's back button becomes redundant and the only way to escape is to hit <Ctrl><Alt><Del> at the same time. Adult Internet professionals have decried the practice as doing more harm than help to the industry, yet it is still prevalent in the field.

Cookies

Cookies are pieces of information stored in the user's computer. Cookies are embedded in the HTML information flowing back and forth between the user's computer and certain web servers. Usually this goes unnoticed to the web surfer. A cookie may contain such things as surfing history, personal preferences or buying habits. An unprincipled pornographer can use this information to track every move you make and select you for numerous scams and tricks

The process of receiving a cookie takes place in two stages. A typical example is when a user goes to a web site of interest and selects a preferred category. The web server creates a tagged string of text containing the users preference and transmits the cookie to the users computer. If the users computer is setup to allow cookies, the cookie is placed in a cookie list. The next stage covertly and involuntarily transfers the cookie to the web server. A sample redirection Cookie Script can be found in Appendix B.

Dangerous Downloads

> The charges indicated that they had called the number several times, for long periods of time. Each time they were billed anywhere from $2.00 to $10.00 a minute! All of the calls were to a company on a small island nation in the South Pacific called Vanuatu. How is it that all of these people were suddenly billed for calls to this island … when they swore they never made those calls? *Tom Martino, Troubleshooter Network*

A vicious download can mean hours of rebuilding a computer, continuous havoc, unforeseen pop-ups, privacy problems and many other problems. These programs can come in the form of screen savers, calendars, dialers, games, e-cards and more. Sometimes they even alter your start programs, replace your home page or automatically add themselves to your favorites lists.

Trojans

> The program, dubbed "Cytron" by the bureau's National Infrastructure Protection Center (NIPC) and some anti-virus vendors, is a covert browser plug-in that gives Internet Explorer users something they probably don't want: more pop-up ads, promoting a slew of adult websites. *Computer Cops, 21 October 2002*

Trojan Horses are imposters that claim to be of a desirable nature but in fact are malicious. Trojans are often called backdoors. For a Trojan Horse to spread, they must be placed onto your computer. Most often this is done by opening an email or downloading and running a file from the Internet.
An example of a Trojan program dubbed “Cytron” is distributed in the form of an electronic greeting card. The recipient receives the greeting card with a cute smiley face background and the text “You have received an e-card” in squiggly block letters. This takes the recipient to surprise.net where they must accept the download of an “e-card viewer plug-in” in order to read the card. Internet Explorer will then feed them numerous pop-ups for adult sites.

Dialers

> The vast majority of your sites visitors either don't own or aren't prepared to use a credit card to buy adult services online. This means that most of your visitors aren't going to be paying ones! By signing up and simply installing our dialer you're enabling your site to catch these surfers that would normally disappear at the site of a credit card form. This results in a substantial increase in the revenue your web site creates. *Porn Site Dialers.com, 2003*

Dialers come in many forms. They can be a Nintendo advertisement, a 1-900 dialer, an attachment or an email. In any form, once it is downloaded it will disconnect you from your Internet Service Provider (ISP) and dial out to 900 numbers, an overseas number or an international number. Amazing as it may seem, if you have calls to international numbers blocked on your phone, some dialer viruses will call 10-10-XXX and connect….yikes! For those of you connected via DSL or cable and still have a modem connected, you can sometimes hear the modem trying to connect.

Dialers also create simple business opportunities that provide all of the details to get started in pornography. There are companies that provide everything you need to get started quickly including graphics, links, marketing tips and online

statistics. They automatically deposit your payments into your bank account and relinquish the need for merchant accounts for the business opportunists. The program they provide may be as small as 20kb, which downloads to your computer in a matter of seconds.

Figure 8 is an example of a logo offered by Porn Site Dialers you may select to use for advertisements. *Table 1* shows the rates the business will pay you per minute. The companies also allow you to customize and rename the graphics and links.

Figure 8. One of nine logos available From Porn Site Dialers

Country	Rate US$/minute
United Kingdom	$0.51
United States	$0.51
Australia	$0.45
Switzerland	$0.39
Germany	$0.33
Japan	$0.29
Austria	$0.23
Ireland	$0.18
Finland	$0.16
Mexico	$0.11
Italy	$0.10
Hungary	$0.11
Poland	$0.10
Russia	$0.10
Czech Republic	$0.10
Canada	$0.07
Greece	$0.06
Hong Kong	$0.06
Spain	$0.06
Morocco	$0.05
Venezuela	$0.05
India	$0.05

Table 1. Pay Chart from Porn Site Dialers

Spyware

"Spyware" is Internet lingo for Advertising Supported Software (Adware). It is any technology that assists in compiling information about an organization or person without their knowledge or explicit permission. Spyware received its name because some advertising companies installed additional tracking software that is constantly calling back to "home base" providing statistical data, like your surfing habits, to a remote location.

Internet Filters

One of the most frequently asked questions by parents is "What Internet Filter is the best to use?" The answer is more complicated than it seems. There are many different types of software that do different things. Do you want to block Internet sites? Do you want to block chat rooms? Email? News Groups? Usenet? What age group are you blocking? What about pop-ups? Are you attempting to block spam? Do you use America Online? Do you have DSL or cable? Do you have a Hotmail or Yahoo email account?

Filters can provide a reasonable amount of protection but every situation is a little bit different. There is no one-stop shop solution. A lot of porn sites provide filtering software links at the bottom of their web site and many of these software companies allow you to evaluate their software for a trial period.

There are several downfalls to filtering software. One of the downfalls are web sites that describe how to disable them. Any Internet savvy person can search and find a solution to disable the filter. Peacefire.org is one of the sites that promote this information. Peacefire.org is an organization that *claims* to represent the interests of people under 18 in the debate over freedom of speech on the Internet. Among their ongoing projects is to list how to disable many of the popular filters.

If your child could disable the software, what good does the filter do? What if the software is stealth and does not show up on the Task Bar or in the processes? Stealth is an answer we will see in the Monitoring section. Although it is not designed to be a filter, it sure can helpful. Before we do that, *Appendix C* is a sample contract that parents may review and *Table 2* is a list of filters rated by internetfilterreview.com:

Software	Rating	Web Site
ContentProtect 1.2	Excellent	http://www.content-watch.com
Cybersitter 2002	Excellent	http://www.cybersitter.com/
CyberPatrol 6.0	Very Good	http://www.cyberpatrol.com/
FilterPak 7.1	Good	http://s4f.com/

CyberSentinel	Good	http://www.securitysoft.com/new601/cs_home.htm
Mcafee Parental Controls 1.0	Good	http://www.mcafee.com/myapps/pc/
NetNanny 5.0	Good	http://www.netnanny.com/
Norton Parental Controls	Good	http://www.symantec.com/
CyberSnoop 4.0	Fair	http://www.cyber-snoop.com/index.html
ChildSafe 3.0	Fair	http://www.webroot.com/wb/products/childsafe/index.php

Table 2. Popular Internet Filters For Review

Monitoring

Monitoring can be as simple as reviewing reports generated from a software filter or having a computer in a centralized room that is physically monitored. The ability to physically monitor the computer twenty-four hours a day is simply impracticable. Especially, if the Internet is used for hours at a time and only a short period of that time is utilized viewing inappropriate material.

Filtering software can be used as a monitoring device and overall does a pretty good job. Most show up in Program Files, Desktop and /or the Task Bar by default. You can even go to Add/Remove Programs and see that it is installed. This is obvious to the user who may find a method to disable, trick or circumvent the software. This is where a stealth-monitoring program such as Spectorsoft Pro steps in.

SpectorSoft

Spectorsoft Professional is a powerful surveillance and monitoring solution that will record email, Web Sites, Chat/Instant Messaging logs, and Keyboard strokes. It captures Internet based email services such as Hotmail, Yahoo Mail and AOL Mail, which many filters do not. It can also be setup to record specific users or certain Windows applications. The beauty of this software is the triple layer of security that makes this software invisible to the user and resides on a hidden location on your computer. The three layers are:

1. Stealth Mode - Stealth technology ensures that it will not appear in the Windows System Tray, Desktop, Task Manager or Add/Remove Programs Menu. Unless you are an authorized user and know it is installed, you probably will be unaware that you are being monitored.

2. Hot Key Access – The authorized user must know a combination of Hot Keys and a password. For instance <Ctrl> <Alt> <1><2> followed by the password.

3. Password Protection - The authorized user must enter a password once the Hot
   Key Access is entered.

A fantastic feature is the keyword detection and reporting. This feature generates a report only when an “alert” word or phrase is encountered, therefore eliminating extraneous data and wasting system resources. This can be setup so that whenever someone enters a chat room and types “meet me’, “skip school”, “send picture”, etc or enters a web site with one of your keywords enabled, the program will start recording and send an email immediately to a specified account such as a parent.

Another advantage is that it can be installed in an unattended silent mode. You can send it as an email attachment, through a Microsoft Network Logon Script or a URL that once clicked it will install automatically.

Child Pornography and Peer-to-Peer

Searching for words such as "preteen," "underage" and "incest" on the Kazaa network resulted in a slew of images that qualify as child pornography. *CNET, News.com, March 12,2003*

Child pornography is also known as pedophile pornography or Kid Porn (KP) and is defined as photographic, film, video or other visual representation that shows a person who is under the age of eighteen years old engaged in or depicted in explicit sexual activity. Antichildporn.org claims that:

- Child pornography is produced at the suffering of children who are sexually abused
- Child pornography renews feelings of guilt, shame, fear and self-hate in the victims of childhood sexual assault
- Child pornography fuels the deviant sexual desires of adults who would sexually abuse children and also is used in the commission of sexual abuse as a tool to groom the victim

Child pornography is an enormous problem on the Internet according to a report by the General Accounting Office (GAO). A second report from the House Government Reform Committee conceded that current filtering technology has "…no, or limited, ability to block access to pornography via file-sharing programs or peer-to-peer networks." The US Justice Department estimates the child pornographic market to be a 2 to 3 billion dollar-a-year industry, making it one of the largest cottage industries with Peer-to-Peer networks contributing to this remarkable growth.

Peer-to-Peer networks are a community of computers that directly communicate with each other as opposed to a server at some company. You can share multiple files on your computer, share one file, or share your entire hard drive. Your hard drive may be shared without you even knowing it. This technology does not use websites or browsers and most filters will not block the content.

Napster popularized the phenomenon and claimed as many as 70 million users at its peak. The difference now is that the new file sharing programs can be used to download any type of file including photographs, video files, and software. Napster supported only sharing of MP3 music files and operated on a central server.

These types of networks are gaining speed and provide free access to thousands of pornographic videos and images that do not require a credit card. On a given day, six of the top ten searches were for "porn", "sex", and "XXX", and other terms intended for elicit pornography. Child pornographers are taking advantage of these networks because it is harder for the FBI to track, locate and contain.

There are a number of file-sharing programs out there like Morpheus, Bearshare, Kazaa, Nutella, Limeware, Gnucleus, MyNapster, Direct Connect, eDonkey2000, Bodtella, Mactella, Newtella, Aimster, Imesh and more. If you see any of these programs on your computer, you may want to start asking a few questions.

Reporting Suspicious or Inappropriate Activity

There are numerous activities that are annoying, inappropriate and illegal. Below are just a few contacts, phone numbers and web sites that may be useful at some time.

The National Center for Missing and Exploited Children maintain a Child Pornography Tip Line at 1-800-843-5678 or visit them online at:

http://www.cybertipline.com/

The FBI Crimes Against Children Program can be reached at 202-324-3666

The FTC can be reached at 877-FTC-HELP.

To report Porn Napping visit:

http://oii.org/html/report.html

To report Cyberstalking & Harassment visit

https://www.wiredsafety.org/forms/stalking.html?menu

To report online child pornography visit:

http://www.antichildporn.org/reportcp.htm
https://www.wiredsafety.org/forms/report_kp.html

Conclusion

Pornographers continue to find new avenues to trickle into our lives using the Internet as one of their prime resources. Cyberporn is a multi-billion dollar industry that continues to grow at a phenomenal rate and will not deteriorate anytime soon. Most parents want to instill in their children their own personal values about relationships, sex, intimacy, love, and marriage but Cyberporn goes against these values by depicting things like rape, bestiality and the dehumanization of females in sexual scenes. Hopefully with continued awareness, improved software and legislation we can get together and find some sort of solution.

Appendix A

HTML Code For Alert Boxes

```
<html>

<head>
<title>Popup Test</title>
<SCRIPT language=JAVASCRIPT>
<!--
function AlertBox(){
    alert('This is the first Alert Box!');
    alert('This can be used to warn you about a virus!!!');
    alert('You tried to click out but it did not work, did it?');
    alert('You may have been infected with a virus, click OK to check your system');
    alert('That is enough for this demo, this could continue.....');
}
 -->
</SCRIPT>
</head>
<body onload='AlertBox()'>
</head>
</body>
</html>
```


Appendix B

Redirection Cookie Script

```
<script>
```

```
<!--
/* Copyright http://www.perlscriptsjavascripts.com
   Free and commercial Perl and JavaScripts     */

// page to go to if cookie exists
go_to = "http://www.perlscriptsjavascripts.com";

// number of days cookie lives for
num_days = 60;
function ged(noDays){
    var today = new Date();
    var expr = new Date(today.getTime() + noDays*24*60*60*1000);
    return  expr.toGMTString();
}

function readCookie(cookieName){
    var start = document.cookie.indexOf(cookieName);
    if (start == -1){
        document.cookie = "seenit=yes; expires=" + ged(num_days);
    } else {
        window.location = go_to;
    }
}

readCookie("seenit");
// -->
</script>
```


Appendix C

ACPO'S Be Smart, Be Safe Online Contract

By signing this contract I agree:

- Never to reveal my name, where I go to school, my home or e-mail address or my phone number to anyone I meet online.
- Never to give out passwords to anyone that asks. Ever.
- To use an alias and user name that does not reveal school, gender, age, street address, city, or real name.
- Never to meet a chat friend in person without a parent or adult along with me.
- Never to open or respond to e-mail messages unless I know who sent them.
- Never to open or download a file from someone I don't know.
- Never to send a picture of myself, or to accept one from someone online without my parent or guardian's permission.
- Never to install and/or use a web cam while online without parent or guardian permission.
- To report to a parent or guardian immediately if someone online says something or asks me something that makes me feel uncomfortable, or that I don't understand.
- To only be online during the time that has been agreed upon between me and my parent or guardian.

My Signature:

_____

Date: _____

Parent/Guardian Signature:

_____

Date: _____

ACPO ©2003, Non-Profit Organization

Resources

Jerry Ropelato, “Tricks Pornographers Play”, CTO ContentWatch Inc., 2002
URL: http://www.dirtcycles.com/tricks-p-play.htm

Rice, Donna, “ How Children Access Pornography on the Internet”, Protecting Children in Cyberspace, 2001
URL: http://www.protectkids.com/dangers/childaccess.htm

Declan McCullagh, “Congress Cracks Down on P2P Porn”. CNET, Networks, Inc, March12, 2003
URL: http://news.com.com/2100-1028-992371.html?tag=nl

Office of the Press Secretary, “Increasing Safety for America’s Children”, 23 Oct 2003
URL: http://www.whitehouse.gov/news/releases/2002/10/20021023.html

U.S Department of Justice, Office of Juvenile Justice and Delinquency Programs, March 2001 #04, Fact Sheet FS 200104
URL: http://www.missingkids.com/en_US/documents/internetsafety_surv.pdf

Online Internet Institute, “Porn Napping”, March 2003
URL: http://oii.org/html/porn-napping.html

Porn Site Dialers, May 2003
URL: http://www.pornsitedialers.com/

FTC, “Court Shuts Down Cyberscam Permanently”, Federal Trade Commission, May 24,2002
URL: http://www.ftc.gov/opa/2002/05/cupcake.htm

Tom Martino, “Mysterious Phone Charges Exposed”, Troucbleshooter.com. May 2003
URL:
http://www.troubleshooter.com/data/columns/mysteriousphonecharges.htm

Agape Press, Christian News Service, “Ministries, Churches Susceptible to Porn-Napping”, 2 Apr 2002
URL: http://headlines.agapepress.org/archive/4/22002d.asp

Electronic Group Interactive, May 2003
URL: http://usa-network.nocreditcard.com/

Philo Levin, “Arizona Cybercrime Bill Targets Porn Loops, Other Offenses” AVN Media Network, April 2000
URL: http://www.avnonline.com/issues/200004/bitsbytes/bb0400_04.shtml

Perlscripts Javascripts, May 2003
URL: http://www.perlscriptsjavascripts.com/js/cookie_redirect.html

Online Internet Institute, “Report Porn Napping”, March 2003
URL: http://oii.org/html/report.html

Computer Cops, “E-card Sneakware Delivers Web Porn” October 2002
URL: http://www.computercops.biz/article1635.html

Jerry Ropelato, “Cyber Secrets 2003”, CyberPorn and Internet Safety, February 18,2003
URL: http://byubroadcasting.org/secrets/transcript/ropelato_transcript_2003.htm

Pest Control, “Spyware Cookies”, May 2003
URL: http://www.safersite.com/Support/About/About_Spyware_Cookies.asp

Recycled-Traffic.Com US congress criminalizes “porn-napping”, April 20, 2003
URL: http://www.recycled-traffic.com/news.jsp?newsid=23

Bennett Haselton, “Instructions For Setting Up A Simple Circumventor”, Peacefire, Open Access For The Next Generation, April 7, 2003
URL: http://www.peacefire.org/circumventor/simple-circumventor-instructions.html

CyberTipLine, National Center For Missing and Exploited Children
URL:
http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=169

Anti-Child Porn Organization, “Anonymous Submission”, May 2003
URL: http://www.antichildporn.org/reportcp.htm

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event