DISCOVERING THE MEANING OF INTERNET SAFETY

A Master's Thesis
Presented to

Information Design and Technology

In Partial Fulfillment
of the Requirements for the

Master of Science Degree

State University of New York
Institute of Technology
Utica, New York

By

Kathleen Palinski

December 2005

SUNYIT

DEPARTMENT OF INFORMATION DESIGN AND TECHNOLOGY
CERTIFICATE OF APPROVAL

Approved and recommended for acceptance as a thesis in partial fulfillment of the requirements for the degree of Master of Science in Information Design and Technology

____

DATE

____

Russell Kahn
Director, M.S. in Information Design and Technology

____

Keith Kempney
Subject Matter Expert

Abstract

An in-depth analysis was conducted with the purpose of discovering the meaning of Internet safety. A case study was used to derive themes from multiple sources of data (documents, interviews, observations, artifacts). Data collected during the study includes interviews from elementary teachers, parents, students, and district-level administrators. It also includes a literature review, documents, and the application of Karl Weick's Organizational Theory.

Internet safety problems were studied at a small school district of approximately 2,500 students in central New York State where the case study was conducted. The current software the district uses is a highly restrictive server level program. A dynamic definition of Internet safety is proposed as a result of the case study.

Acknowledgements

I would like to thank Dr. Russell L. Kahn for all of the time and guidance he has provided throughout this experience. He has been very helpful and always available for advice and encouragement. He has been a great inspiration since I began working toward this degree.

Zoe Hicks has been a tremendous help. Her expertise on Internet safety has guided this project. She has helped in every aspect, from being interviewed to proofreading. Her suggestions, feedback, and support are greatly appreciated.

My study would not have been complete without the expert advice from my subject matter expert, Keith Kempney. I am grateful for the time and energy he put into this project. His guidance, input, and support have been invaluable.

Without the help and support of these wonderful people, the completion of my thesis would not have been possible. For this I am grateful and extremely indebted.

Table of Contents

List of Figures

Section 1: Entry Vignette

Mrs. Kempney was walking through the park with her two toddler sons when all of a sudden the loud sound of helicopters was all they could hear. She couldn't imagine why there were so many helicopters circling her otherwise quiet, uneventful neighborhood. She was anxious to turn on the news to find out what was going on. As soon as she turned on the television, an emergency news flash appeared on the screen. She listened with shock and quickly became scared. Tears welled up in her eyes when she heard, "***A twelve year old girl, Sara Ann Woods, was riding home from her father's church when she was abducted…***" After hearing that news, Mrs. Kempney was never the same. Having two small children in a nearby neighborhood, she vowed to never leave them unattended again.

When her boys were a little older and had started school, society was infiltrated with the term, "Stranger Danger." Her boys learned what was being taught to all children in the community since the Sara Ann Woods tragedy. They were taught:

- never talk to strangers
- never let a stranger get too close to you
- never take candy, a present, or anything from a stranger
- never tell a stranger your name, address or phone number
- never get into a stranger's car
- never go into deserted places alone
- always try to walk with friends or an adult
- if a stranger grabs you, yell as loud as you can saying things like, Help! Call the police! This isn't my parent!

Mrs. Kempney was somewhat comforted by the Stranger Danger phenomenon. She thought, *"This is great. If a stranger approaches my children, they will know what to do."* She watched her boys grow up over the next few years. She could rest easy knowing her children were armed with knowledge and good sense to protect themselves from predators.

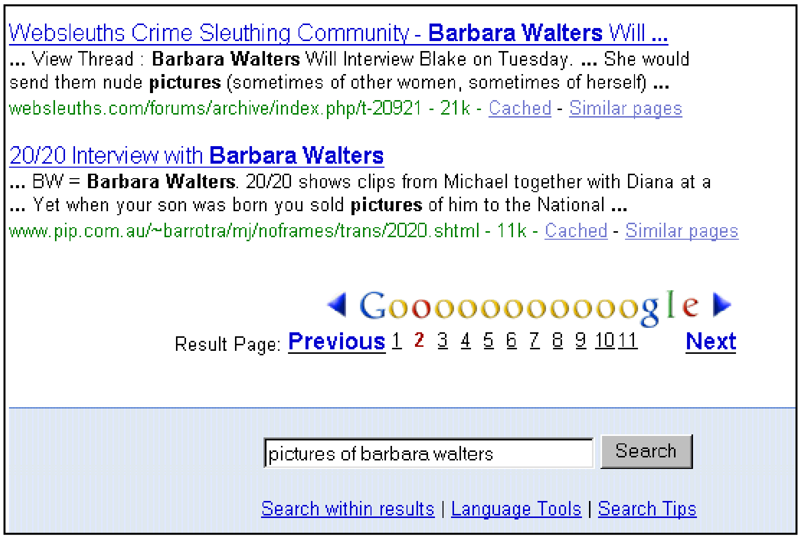
While her boys were in high school, she returned to school to become a librarian. There she learned about the advancements of technology in schools, New York State's drive to integrate technology into education, and above all, the Internet. She learned that the Internet is a new reference tool with which to conduct research. It makes things that are not readily available, easily accessible. However, she also learned that the Internet is a portal to the world accessible to anyone. She quickly learned that people on the Internet do not know if you are a child or an adult. She also learned about the number of sick people who are allowed to put anything (examples: pornography, viruses, hate sites) on the Internet. She recognized that using the Internet as a resource was much different from using print materials in the library. For example, if a child were to find an inappropriate, adult level book from the library, the librarian could contact the parents or refuse to let the child sign the book out. There is no one to tell a child that what they are looking at is inappropriate when they are on the Internet.

She pictured her children sitting in front of a computer screen with the potential for them to be exposed to the dark side of modern culture. After coping with ways of monitoring her own children's Internet use (utilizing password access, parental presence), she began to think about how this was going to affect her newly chosen career. *"If kids are supposed to be using technology and learning about the Internet, how am I going to monitor websites they visit? How will teachers keep them safe from all the dangers lurking on the World Wide Web?"*

Mrs. Kempney found her first year as a librarian insightful. At that time there was no mention of how to keep kids safe from the pornography, hate sites and chat rooms on the Internet. It was her responsibility to develop ways that would effectively keep children safe from dangerous material. She had learned about filtering software while studying to be a librarian. However, the district that hired her did not have any such software. Without any filtering software, Mrs. Kempney felt anxious and worried whenever her students signed onto the World Wide Web.

One day Mrs. Kempney was teaching a lesson about how to find information online. Her objective was to teach students how to use kid-friendly search engines such as *Yahooligans*, *Ask Jeeves for Kids* and *KidsClick*. While most of her students were searching for information via the kid-friendly search engines she taught them to use, eleven-year-old Charles decided to use Google as his search engine. After he typed in what he was looking for, the sites that appeared on the screen contained inappropriate words (nude pictures) for any student, especially Charles, a sixth grader (see Figure 1, page 4). Just as he was moving his mouse to one of the inappropriate websites (Websleuths.com), Mrs. Kempney happened to be watching quietly nearby. When the cursor was on the website link, before Charles could click, Mrs. Kempney asked, *"How is your research coming, Charles?"* After Charles recovered from being startled, face still red with embarrassment, he said defensively, *"My parents let me use Google to search at home."* Mrs. Kempney responded, *"Whatever your parents allow you to do at home is their business. Unfortunately Charles, at school there are rules we must follow. Using Google to search* for information is not allowed in school. This is your warning. If you are caught using Google again in school, we will call your parents in for a conference."

Figure 1 – Google Search



Websleuths Crime Sleuthing Community - **Barbara Walters** Will ...
... View Thread : **Barbara Walters** Will Interview Blake on Tuesday. ... She would send them nude **pictures** (sometimes of other women, sometimes of herself) ...
websleuths.com/forums/archive/index.php/t-20921 - 21k - Cached - Similar pages

20/20 Interview with **Barbara Walters**
... BW = **Barbara Walters**. 20/20 shows clips from Michael together with Diana at a ... Yet when your son was born you sold **pictures** of him to the National ...
www.pip.com.au/~barrotra/mj/noframes/trans/2020.shtml - 11k - Cached - Similar pages

pictures of barbara walters

Result Page: Previous 1 2 3 4 5 6 7 8 9 10 11 Next
Search
Search within results | Language Tools | Search Tips

After searching Google for pictures of Barbara Walters, an inappropriate site appeared.

Mrs. Kempney continued to struggle with Internet safety because she felt it was such a huge responsibility. She had heard that the district might eventually invest in some filtering software. She wondered if the Internet would become more problematic without filtering software.

This study will address a district's and teacher's responsibility and awareness of children's access to Internet sites. Children's safety is always an issue. As shown in this example, a child using the Internet is potentially dangerous. What is the best way to teach Internet safety? This study will consider this issue in depth.

Filtering software has recently been purchased by Mrs. Kempney's district and has become a part of students' and teachers' daily lives. The decision to purchase and utilize filtering software was driven by the federal government funding policy. The federal government will not fund schools that do not have filtering software.

Questions Raised:

- How is Internet safety being taught in schools?
- Is there a written curriculum for teaching Internet safety and if not, why?

Section 2: Introduction

Literature Review

Several journal articles, which discussed Internet safety and children, were reviewed. They indicated that the issue of Internet safety was being examined in schools across the country. According to the literature, a push in educating children, parents, and communities would help children make decisions while on the Internet that would keep them safe. Most articles examined agree with Michael J. Berson, Ph.D. that, "Educational strategies which focus on helping children and youth to develop autonomous and responsible skills online require education. This approach complements existing filters and security systems which can never guarantee total protection" (57).

Journal Article Summaries

'Internet safety in emerging educational contexts' by Jocelyn Wishart (200) notes the government or "Internet safety organizations reported children's Net literacy as their single most important Internet safety concern." Therefore, educating children to utilize the Internet effectively would be one way to make the Internet a safer place for children. Wishart (203) does report, however, that a "vast majority of schools are teaching Internet safety" but does not include what students should do if they encounter negative situations.

Authors Muhammet Demirbilek, Sebnem Cilesiz, and Dogan Tozoglu present ways for parents and teachers to protect students when they surf the Net in 'Safety strategies while surfing online in the classroom.' They recommend explaining how to use Internet browser software and teaching ethical behavior to children as ways to protect children. As a way for teachers and parents to communicate and work together to ensure safety, the authors suggest teachers inform parents of the procedures and guidelines students are taught as well as be available if parents have questions.

One of the key issues that continually arises while researching Internet safety is appropriate use. Patricia M. Greenfield addresses this concern in ‘Development considerations for determining appropriate Internet use guidelines for children and adolescents.’ Greenfield is concerned with unattended children surfing the web because they could be subjected to unwarranted commercialism. She also discusses the difference between supervised and unsupervised teens in chat rooms and examines the “disturbing instant messages that teens exchange” (760). Greenfield sees the need for more monitoring of children. According to her (760), the “developmental issues raised were not unique to the Internet,” suggesting that parents need to be more involved in all of their children’s activities.

‘Lessons learned about schools and their responsibility to foster safety online’ by Michael J. Berson, Ph.D. proposes that parents and educators be trained more appropriately for preventing Internet errors. Berson strongly advocates the need for better prevention programs. The article discusses the need for communities, parents, and schools to work together to provide the safest Internet environment for children. Ultimately, “ a comprehensive educational program, which is part of a dynamic and interactive experience involving teachers, parents and youth in the development and training process” is necessary for keeping children safe online (Berson 57).

David M. Quinn examines cyberlaw in schools in ‘Legal issues in educational technology: Implications for school leaders.’ Quinn (190) notes that the “…emergence of the Internet has prompted the legislature to compose new statutory laws to address what many believe to be material harmful to minors." He recognizes that some people are against the "Child Online Protection Act" (COPA) (see Appendix A) and the "Children's Internet Protection Act" (CIPA) (see Appendix A) because they think these acts violate free speech. Regardless of the controversies among the laws, Quinn firmly (193) believes that, "…formal Internet safety policies" are necessary in schools.

More specifically, Dick Thornburgh and Herbert Lin address some of the dangers that lurk on the Internet in, 'Youth, pornography, and the Internet.' The article begins, "The Internet is both a source of promise for our children and a source of concern" (Thornburgh and Lin 43). Thornburgh and Lin recognize the positive potential the Internet possesses while addressing the concern of material "harmful to minors" (43). The definition states

> material that if taken as a whole and with respect to minors, appeals to prurient interest in nudity, sex, or excretion; depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals, and taken as a whole, lacks serious literary, artistic, political, or scientific value to minors (Thornburgh and Lin 43).

After a brief description of the Children's Internet Protection Act, Thornburgh and Lin (44) recommend three elements that form "a balanced framework for protecting children online." These include public policy/law enforcement, technology, and education.

'Internet safety' by Anne Reeks (146) is a similar article because it also recognizes that "Porn, questionable characters, hate groups, and misinformation flourish online." Reeks presents several ways to protect children online. She recommends that parents "get involved," set house rules, teach them to protect their privacy (avoid revealing personal information online), "keep the computer in a central spot," use parental controls provided by Internet service providers, implement software, as well as others (Reeks 146, 147). Reeks provides information about six different software programs available for parents. She includes cost and websites to find out more.

Susanne Nadeau introduces readers to a product called the i-STIK, which is a computer key to safe Internet chat rooms. In ‘Students get “key” to Internet safety,’ Nadeau (1) describes the key as “a token that can be carried on a key chain and used at school, home or any computer with a USB port.” According to the article, “Students have a username and a personal identification number unique to them with the i-STIK (1). The key allows students to enter “child-safe chat rooms” (1) where adult predators are not allowed without a key. It also “blocks children from accessing Web sites they shouldn’t access” (1). The article mentions that the key is only one tool to keep children safe. Other ways include, “…setting house rules, teaching [children] to protect their privacy, and using free parental controls provided by Internet Service Providers” (Reeks 146). Parents are encouraged to also help keep their children safe.

Danger

According to Nadeau’s article (1), the Internet is “the greatest technology for those who want to prey on children.” The article also recognizes that “There’s no way to keep children 100 percent safe while using the Internet” (1). Thornburgh and Lin (43) describe the inappropriate material on the Internet as being a “small fraction [that] is highly visible and controversial.” They also note “some people believe that certain sexually explicit material is so dangerous to children that even one exposure to it will have lasting harmful effects” (46).

Another aspect that contributes to the danger of the Internet is the inability of children to use gestures, tone of voice and age to judge another person’s intent. These things are present during face-to-face interactions. Berson (52) recognizes “risks to safety and emotional well being” as the most significant among the difficulties online. Unfortunately, Berson (56) states “teachers typically do not feel equipped to address their evolving role in safeguarding the emotional and physical well-being of children.” Berson (57) does recommend “a comprehensive educational program…involving teachers, parents, and youth.”

Responsibility

Although Berson (52) recommends the involvement of teachers, parents, and youth, he thinks “educators have an important role to play in addressing the lapse in preventative intervention to create and maintain awareness and safety for young people online.” One school where Berson (54) observed, however, allowed the “emphasis on the student, rather than the teacher assuming the responsibility for the daily use of the computer.” Ultimately, Berson (56) notes, “Even among the more progressive districts where Internet safety has been integrated into instruction, prevention programs for parents and educators are less common.”

Thornburgh and Lin posit that everyone is responsible for Internet safety. They mention several ways to improve the Internet environment. For example, “promote media literacy and Internet safety education…develop curricula…professional development materials for teachers…educate parents, teachers, librarians, and other adults about Internet safety education issues” (44). They recognize that some strategies are expensive and time consuming. However, they also think that if students learn about the dangers that exist on the Internet and are taught how to use the Internet effectively, then students will be better able to research appropriate content and avoid “searching for inappropriate material or engaging in unsafe activities” (45). They indicate it is everyone’s responsibility to educate students in using the Internet appropriately and also to educate students about dangers that they may encounter.

According to Reeks (2) it is the parent’s responsibility to “decide how much time you’re comfortable with your child being online and which sites they may go to.” She recommends posting a list of sites they may visit next to the computer so kids know where they can go and those places are easily accessible. Reeks suggests setting house rules, monitoring children closely, and using free parental controls from Internet service providers as ways parents can be responsible for keeping their children safe online.

The literature reviewed provides relevant suggestions for teaching children Internet safety. The articles illustrate the need for more Internet safety awareness. They also support the beginning of a definition of Internet safety.

Problem Questions

The purpose of this study was to examine the meaning of Internet safety. The main question is the focus of the entire study. The sub questions give structure and insight, which ultimately aid in answering the main question.

Main Research Question

- What is Internet safety?

Issue Sub questions

- What is the goal of Internet safety?
- What is considered a “safe” website or an unsafe website?
- What has been the impact of web safety in the school environment?
- What changes (if any) should be made in the schools as regards Internet safety?

The Case Study

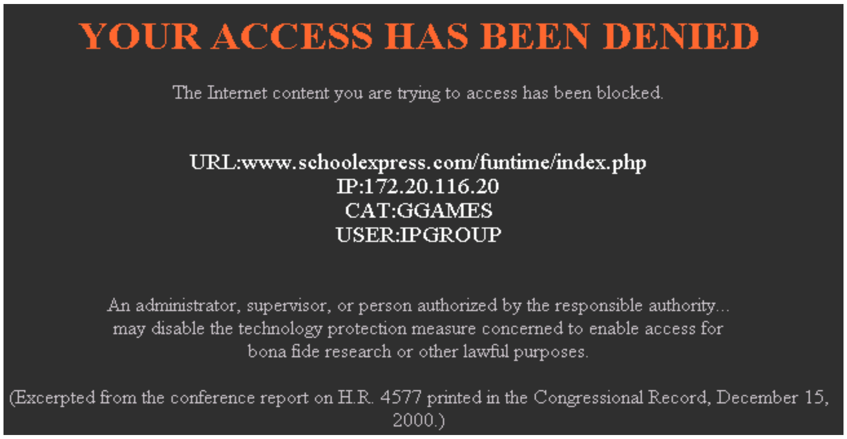
An in-depth analysis was conducted with the purpose of discovering the meaning of Internet safety. A case study was used in order to derive themes from the multiple sources of data (documents, interviews, observations, artifacts). Although the study has phenomenological qualities, a case study seemed to be the most appropriate tradition of qualitative research because it allowed for a more in-depth look at the situation.

The data collection of the case study "is extensive, drawing on multiple sources of information such as observations, interviews, documents, and audio-visual materials" (Cresswell 63). A phenomenological study differs from a case study in that it requires "exhaustive description of a phenomenon" (Cresswell 67). Although discovering the meaning of Internet safety is, in fact, a phenomenon, the timeframe in which data was collected and the current trends in technology lend themselves to a case study.

According to Quinn (187), "Educational technology promises to transform the classroom experience for students, teachers, and parents." In the school district studied, students are expected to know how to use Microsoft Word, PowerPoint, and Excel by the time they leave elementary school. Upon learning these applications, students are also learning how to navigate the World Wide Web, find information, and complete research projects, according to teachers. "While students learn how to use the Internet effectively, teachers are responsible for implementing safe practices," the Library Media Specialist and a classroom teacher agreed. This case study was conducted in order to understand Internet safety.

Internet safety problems were studied at a small school district of approximately 2,500 students in central New York State where the case study was conducted. Educators in the district rely upon filtering software (X-Stop) that is district-wide. Filtering software controlled by the administration filters what a web browser will display. The current software is a server level program that is highly restrictive, according to the district's technology administrator. When sites are blocked, a Denied Access screen (see Figure 2) appears and requires teachers to continue searching for another, more "appropriate" website. According to one classroom teacher, the software does give some peace of mind. Unfortunately, the teacher said, "the software also filters out websites that would be useful for students and teachers." In this case, she noted, it creates more work for educators because "we need to find alternative websites or alternative sources to obtain the necessary information."

Figure 2 – Denied Access Screen



YOUR ACCESS HAS BEEN DENIED

The Internet content you are trying to access has been blocked.

URL:www.schoolexpress.com/funtime/index.php
IP:172.20.116.20
CAT:GGAMES
USER:IPGROUP

An administrator, supervisor, or person authorized by the responsible authority...
may disable the technology protection measure concerned to enable access for
bona fide research or other lawful purposes.

(Excerpted from the conference report on H.R. 4577 printed in the Congressional Record, December 15, 2000.)

The 'Denied Access screen' appeared when the filtering software blocked users' access.

The study made it clear that advancement of technology in education does not come without risk. Several teachers said they feared accidental visits by students to inappropriate websites. Other teachers said they are very careful before even letting students sign on to the World Wide Web. Teachers, librarians, and administrators said they work together to ensure safe computer practices. Teachers explained that they have guidelines in place and teach lessons about using the Internet in hopes of avoiding potentially dangerous websites.

Data Collection

Multiple sources of information were used while collecting data. Interviews and observations were carefully conducted and documents and websites were examined. A data collection matrix illustrating the information sources is presented in Figure 3 on page 15.

The first step in collecting the data involved reviewing journal articles to get a sense of the literature that existed on Internet safety. While examining the articles it became clear that no comprehensive definition of Internet safety existed. However, several articles emphasized a concern for students and their Internet knowledge. The articles served as a starting point for this research.

The author then developed an initial interview protocol (see Appendix B) and set up an interview with a fourth grade teacher. The interview served as a means of gaining insight into how the teacher approached Internet safety with her students. After reviewing the protocol and the responses from the teacher, the questions were revised (see Appendix C) to fit more accurately the specific topic of Internet safety as opposed to the broader topic of filtering software and its effectiveness.

After the revision, formal interviews were set up with a technology administrator and a school librarian. Informal interviews were conducted with a parent and a high school technology teacher. The respondents varied in age and their relationship to the

Internet. Each participant was interviewed in a natural setting, the location in which he or she typically used the Internet, such as the home, office, or school.

Figure 3 – Data Collection Matrix

Information Source	*Interviews*	*Observations*	*Documents*
Teachers	2	1	-
Administrators	1	-	-
Librarian	1	-	-
Parent	1	-	-
Student	2	-	-
Journal articles	-	-	8
Websites	-	15	-
Emails	-	-	1
District policy	-	-	1
Safety poster	-	-	1
Personal journal	-	-	1 (several dates)

Data in the forms of interviews, observations, and documents was collected.

Prior to each interview, subjects were asked to sign and date an ethics permission form (see Appendix D). Each participant was interviewed once, except the fourth grade teacher. She was interviewed with the original interview protocol as well as the revised interview protocol. Interviews were tape-recorded with the consent of the subjects. The interviews were then transcribed and notes taken. The transcriptions also served as a place to search for themes in the study.

The goal of the interviews was to gain insight on what people think is the definition of Internet safety and what might be done to promote Internet safety in schools. Questions were asked regarding their relationship with Internet safety and what they think are safe websites. Each participant was asked what they would like to see with regard to Internet safety as well as characteristics of a safe website. They were also asked what the impact of web safety has been in their school environment. Finally, subjects were asked about unsafe Internet events that they may have encountered.

Upon careful examination of the interviews and the other means of data collection, themes emerged: danger, responsibility, and opportunity costs. These themes are explained in-depth at the end of this section.

Analysis of Data

Generally, participants' responses were similar. Each question with a summary of the key responses given is listed and will be discussed here.

What is Internet safety?

Most respondents mentioned that Internet safety is keeping kids away from people and things that could harm them. They felt that it was the responsibility of teachers and administrators to ensure Internet safety. The Library Media Specialist compared Internet safety with Stranger Danger (see Appendix E). However, she said, "it entails a bigger job than Stranger Danger because there's a whole emotional and psychological safety issue that comes with the Internet, where kids are exposed to graphic images that could do long range damage…"

What is the purpose of Internet safety?

The participants I interviewed answered that the purpose of Internet safety is to make sure students do not visit unsafe websites but also for students to know what to do in case they encounter an unsafe site. According to the Library Media Specialist, the purpose of Internet safety is "understanding that when you sit in front of that computer, you are face to face with the entire world." According to respondents, teachers, administrators, parents and even children are responsible for keeping students away from unsafe websites.

What is your role with regard to Internet safety?

The respondents answered that everyone is involved with Internet safety. The technology administrator's response was, "I think everybody that works in a district is responsible for Internet safety." The teachers' role is to educate students about navigating the Web and how to access safe websites. They are also responsible for making sure students are following the acceptable-use policy in the district (see Appendix F). Technology administrators have the role of making sure the filtering programs are working, blocking any inappropriate sites that may come up, and unblocking useful sites that teachers need for educational purposes. Some respondents think that the role of the parents is to monitor their children while they are on the Internet at home.

What would you like to see done with regard to Internet safety?

Answers to this question varied greatly. A classroom teacher answered, “I’d like our district to set up some policy and procedure or if there is one to communicate it better…I would like to be trained…I would like to see what other people do.” The Library Media Specialist said, “I would like parents to pick up a piece.” She also mentioned that she would like to see larger programs hitting kids and parents. She said, for example, “an organized program…that includes literature and storybooks” to demonstrate the importance of online safety. The district’s technology administrator, “wish[es] all the garbage (pornography, violence, ugly stuff that dares invade our schools) would just go away.”

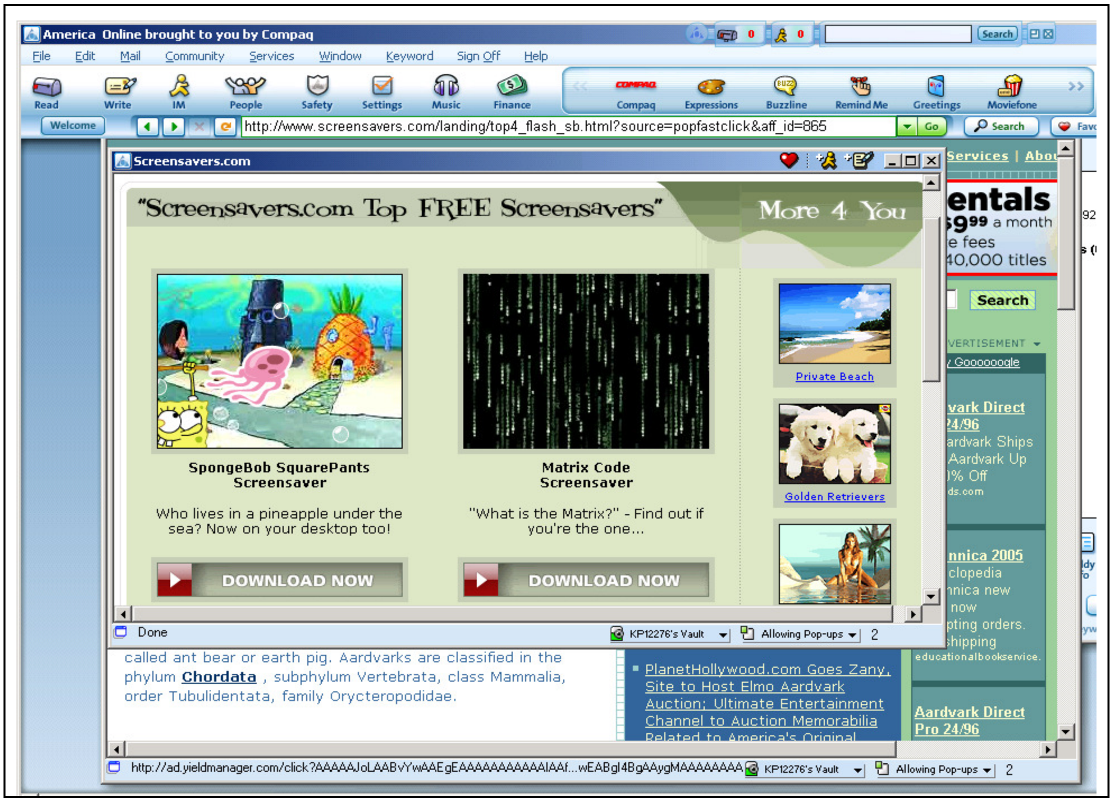
What do you consider a safe website? (What makes a website safe?)

Four of the five respondents described a safe website as one that provides “useful and kid-friendly information. A safe site would have links to other safe sites.” An educator as well as a district technology administrator answered, “a safe website is one that has credible information and is appropriate for all ages.” Other respondents said safe websites are ones that do “not encourage risky behaviors.” The Library Media Specialist explained, “risky behaviors would be…putting in the name and address; clicking on ads, pop-ups, links that lead to things that are not safe, downloads; typing in web addresses (one keystroke and you’re somewhere where you don’t belong).” An example of an unsafe website is shown in Figure 4. Screensavers.com is a potentially dangerous website because it could pop up on a monitor where a student is working and may contain viruses if someone chose to download a free screensaver.

What has been the impact of web safety in our school environment?

As helpful and resourceful as the Internet is (one respondent answered, “the web has definitely improved the amount of material that can be found for every subject being researched”) several participants commented on the inconvenience the web has caused. According to one respondent, “a lot of money is spent on filtering software and human resources.” In addition to the money, the inconvenience aspect also applies to the amount of time teachers have to commit to incorporating the Internet into their classroom instruction. One reason is that because of filtering software, “not everything on the

Figure 4 – Dangerous Website


America Online brought to you by Compaq
File Edit Mail Community Services Window Keyword Sign Off Help
Read Write IM People Safety Settings Music Finance
Compaq Expressions Buzzline Remind Me Greetings Moviefone
Welcome
Go
Search
Screensavers.com
"Screensavers.com Top FREE Screensavers"
More 4 You
SpongeBob SquarePants Screensaver
Matrix Code Screensaver
DOWNLOAD NOW
DOWNLOAD NOW
Private Beach
Golden Retrievers
Done
KP12276's Vault
Allowing Pop-ups
2
Services | Abo
entals
$9.99 a month
e fees
40,000 titles
Search
VERTISEMENT
Goooooogle
vark Direct
24/96
nnica 2005
educationalbookservice.
Aardvark Direct Pro 24/96

http://www.screensavers.com/landing/top4_flash_sb.html?source=popfastclick&aff_id=865

Who lives in a pineapple under the sea? Now on your desktop too!

"What is the Matrix?" - Find out if you're the one...

ardvark Ships
Aardvark Up
0% Off
ds.com

clopedia
nnica new
now
pting orders.
shipping

called ant bear or earth pig. Aardvarks are classified in the phylum **Chordata** , subphylum Vertebrata, class Mammalia, order Tubulidentata, family Orycteropodidae.

- PlanetHollywood.com Goes Zany, Site to Host Elmo Aardvark Auction; Ultimate Entertainment Channel to Auction Memorabilia Related to America's Original

http://ad.yieldmanager.com/click?AAAAAJoLAABvYwAAEgEAAAAAAAAAAIAAf...wEABgl4BgAAygMAAAAAAAA

An example of a dangerous pop-up that was clicked on; tempting viewers to download screensavers.

Internet is available at school." When educational sites are blocked and teachers have to find alternative sites the Internet becomes inconvenient. Teachers are expected to search the subject matter first and find credible sites for students. One respondent compared this activity to a science teacher testing out a chemical experiment before showing it to students for safety purposes.

Have there been any events that were unsafe?

Two of the five people interviewed mentioned chat rooms as an unsafe occurrence. The respondents in this study generally do not support chat rooms for children. A parent responded by saying, "Children get into chat rooms and sometimes have no idea who they're chatting with." Other responses that are related to unsafe events include downloading (it causes computers to crash), inappropriate descriptions under a Google search, gaming sites (appropriate use issue), and identity theft. The amount of unsafe events is fairly small and decreasing with the filtering software. Teachers have been able to prevent unsafe occurrences by teaching students how to use the computer appropriately.

Outcomes/Development of Themes

As the data from the interviews and observations was analyzed, three main themes emerged relating to Internet safety: *danger, responsibility, and opportunity costs*. These will be defined and described.

<u>Danger</u>

The Internet can be a dangerous place. While trying to define Internet safety, the concept of danger arose consistently throughout the data collection. Several examples of dangerous situations came out of the interviews.

Downloading Issues

- Clicking links that could cause viruses
- Downloading programs that could contain viruses

Viewing Issues

- Dramatically increased chances of children seeing graphic images
- Pornography & violence
- Predators & hate sites

Privacy Issues

- Children registering for things over the Internet (in particular, giving out information without parental consent)
- Companies targeting kids for commercial purposes

Miscellaneous Issues

- Inappropriate descriptions (of websites from searching Google; see Figure 1)
- Typing dangerous incorrect addresses in URL box

In order to combat these situations, participants offered ways to keep students out of danger while on the computer. Some of those ways include:

Education

- avoiding chat rooms
- never giving out personal information
- teaching kids to click off the screen and tell an adult if they see something that makes them uncomfortable

Preparation

- using kid safe search engines (*Yahooligans*, *Askjeevesforkids.com*, *kidsclick.com*, etc.)
- filtering software
- creating links prior to students using computers

While analyzing the data, comparisons between the Internet and ‘real life’ emerged. For example, walking up to someone in the mall and giving them your name and address is the same thing as giving someone online that you do not know your name and address. Another example the librarian gave, “Would you want to get on an airplane right now by yourself and get off in Australia alone and wander around the airport there trying to figure out what to do next?" She said that students "consider what's on the screen safe because there's no physical body there." The librarian also said, "I wouldn't buy pornography to put on the shelves so I don't necessarily want it on the machines…"

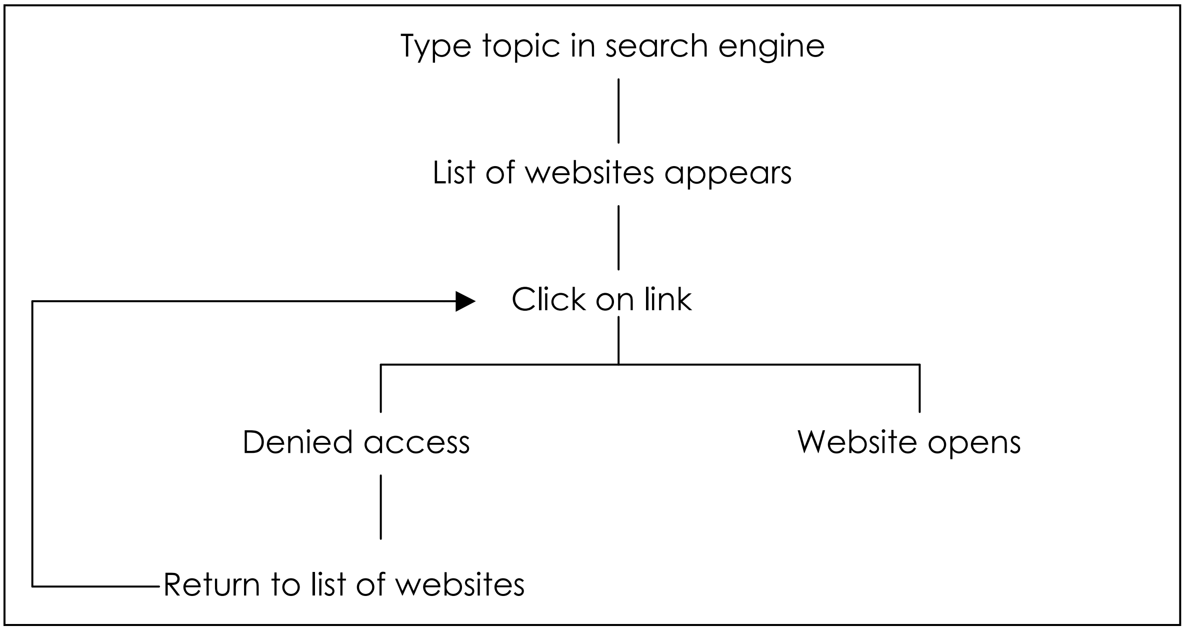
Responsibility

Data analysis indicated a consistent pattern that Internet safety was the responsibility of teachers, administrators, students, and parents. According to the district's technology administrator, Internet safety is similar to the "Stranger Danger" phenomenon: it affects everyone, and everyone has a role in protecting children and themselves from online dangers. Both the Library Media Specialist and the classroom teacher said, while students are in school, teachers have the most responsibility because they are working directly with the students. One part of that responsibility they said was making sure students followed the school district's acceptable-use policy (see Appendix F). Quinn (203) defines acceptable-use polices as, "an essential element of any school district's technology program. These policies establish clear standards of practice for students and staff regarding technology use." Another part is educating students on how to use the Internet as a learning tool. Also, the classroom teacher noted, teachers took responsibility for teaching their students what to do if they see anything they think is inappropriate. Administrators said they have the responsibility of implementing filtering software, communicating with teachers about the effectiveness of software, updating software, and monitoring teacher use of the Internet. The administrators also said they need to learn the best ways to navigate the Internet and be responsible enough to make teachers aware of any problems they encounter. Parents have a growing responsibility, said the Library Media Specialist. They are responsible for what their children are exposed to at home. It is their responsibility, according to the Library Media Specialist and classroom teacher, to make sure students are using the Internet appropriately outside of school.

Opportunity Costs

The filtering software allows teachers to let students search the Internet more independently. Unfortunately, according to the district's technology administrator, the latest software is more restrictive than previous versions. Because it is more restrictive, it is more likely that the Denied Access screen (see Figure 2) will appear on the monitor. In this case, "not everything on the Internet is available at school and [students] have to find alternative websites," said the Library Media Specialist. The filtering software she said, censors a lot of websites, causing students and teachers frustration. The following student observation is an example of the opportunity costs: a student was given 45 minutes to research a topic. The student began searching and was blocked from sites he tried to access. It was then necessary for him to search for alternative websites in order to complete his research (see Figure 5). By the time he found an appropriate website, his

Figure 5 – Search Flow Chart



Flowchart showing the possible processes of searching for websites.

45 minutes were over. Therefore, time spent seeking alternative websites could be time spent completing important research. This also affects teachers because their computers have the same software as the students. According to the classroom teacher, "if teachers prepare lessons at home the night before and find useful websites, there is no guarantee that they will be able to access the same sites at school."

Internet safety has another component that illustrates an opportunity cost. The Library Media Specialist and classroom teacher agreed, "it is necessary for teachers to be prepared in the event that a student does encounter an inappropriate website." If this happened, teachers would have to stop class and use the opportunity to teach students what to do in this situation. The classroom teacher explained that this could interfere with curriculum and testing, forcing teachers to find time in their schedule to make up lost instructional time. She said, "this situation could also prolong projects, making it difficult for teachers to complete their required curriculum." Ultimately, teachers could spend time implementing safe Internet practices instead of instructing and preparing students for required state tests.

Finally, the district's technology administrator said, "Internet safety becomes inconvenient when time and money are considered." The classroom teacher said, "the time spent on learning about the Internet and how to implement it safely in classrooms could be time spent learning how to create classroom websites." She said, "money spent on filtering software could be used for educational software." All informants agreed, "the Internet is an excellent resource for both students and teachers." In addition, they think the benefits of the Internet balance the danger and inconvenience it creates.

Section 3: Description of the Case and Its Context

According to Thornburgh and Lin (47), "…efforts to protect children have focused mostly on technology-based tools such as filters. But technology, especially today's technology, cannot provide a complete or even a nearly complete solution." They also state that children need to develop "an ethic of responsible choice and the skills to implement these choices and cope with exposure…" (Thornburgh and Lin 48). It is necessary to understand what Internet safety is in order to provide students with appropriate Internet safety education.

Journal articles indicated that people who are not familiar with the Internet fear using it as an educational tool. According to Berson (56), "educators often find themselves inadequately prepared to assist children [on the Internet] in the classroom." Several of the articles mentioned the emotional and psychological damage inappropriate exposure may cause. Specifically, Thornburgh and Lin (45) note, "some people believe that certain sexually explicit material is so dangerous to children that even one exposure to it will have lasting harmful effects." Consequently, monitoring children while they navigate the World Wide Web will decrease the likelihood of them accessing risky situations. Berson (55) notes, "direct observation of children online in a public space with periodic interaction and ongoing discussions of their web experiences are the foundations of Internet safety procedures."

The research illustrates, however, that if children are educated on how to use the Internet appropriately and if they know what to do if they encounter something that makes them feel uncomfortable they will be safer. Thornburgh and Lin (44) recommend, "teaching children how sexual predators and hate-group recruiters typically approach young people and how to recognize impending access to inappropriate sexually explicit material." They think if children are educated about these possibilities, "some children [will be] less inclined to spend their time searching for inappropriate material or engaging in unsafe activities."

According to Berson (56), "districts where Internet safety has been integrated into instruction, prevention programs for parents and educators are less common." A fourth grade teacher commented, "I'd like our district to set up some policy and procedure" with regard to Internet safety. She noted, "if there is one, to communicate it to us better" because all of the Internet instruction she provides for her students comes directly from her own experience. She found that filtering software is one way schools can promote Internet safety. It is important, she said, that districts communicate with teachers, students, parents, and communities ways in which they can all contribute to student safety online. It is not just a district's responsibility to ensure Internet safety; it is the responsibility of everyone involved in the lives of the students. Berson (57) suggests a plan for educating and protecting students, "requires a comprehensive educational program… involving teachers, parents and youth…"

Section 4: Description of the Theory

The theory applied to the Internet safety research is Karl Weick's view of Organizational Theory. Organizational Theorist G.L. Kreps believes that communication is the basis for organizing; organizing reduces information uncertainty; human interaction is the central phenomenon of organization (103-121).

Technology is always changing and improving. Therefore, there is no prototype on which to plan an Internet safety curriculum. According to Weick, "Organizations and their environments change so rapidly that it is unrealistic to show what they are like now, because that's not the way they are going to be later" (89). Weick's comment parallels the rapid changes that occur in technology. Perhaps Organizational Theory provides a framework for educators and administrators to utilize. For example, educators and administrators could use the theory as a tool to establish a guideline for teaching online safety in schools.

Weick sees organization as occurring through three major phases. The first one is the enactment or defining of a situation and the beginning process of dealing with information. The second phase is selection. Selection is defined as deciding on what to deal with, what to leave alone, ignore, or disregard. The selection phase also generates answers to 'what's going on here?' The third phase is retention or more simply, "What information will be retained for future use?" (Kreps 114).

The problem with Internet safety, based on observations and interviews, is the lack of curriculum related to Internet safety. With all of the dangers on the Internet, teachers interviewed agreed that they have a responsibility to educate and protect children. The selection phase of Organizational Theory is the act of narrowing equivocality. At the school building level it is important to analyze issues that teachers can spend time improving. Applying this theory permits teachers to answer the question, ‘What are the most important segments of Internet safety?’ Research shows that there are several facets to Internet safety. These include education, communication, filtering software, parental controls, monitoring children and Net literacy as well as concerns over limiting freedom of speech. The third phase of the theory is retention. This phase involves the act of deciding which of the topics from the selection phase will be retained for future use. As a result of extensive research, the most important segments of Internet safety are education and communication.

In essence, Organizational Theory as described by Weick, attempts to answer the question, ‘What is the best way to ensure Internet safety in schools?’ In order to answer the question, a more specific approach to the Organizational Theory must be applied. Internet safety must begin with the act of communicating. The state education department communicates guidelines to school districts and recommends ways to keep the Internet a safe place for children. Second, this communication ultimately ends up at the school district level where administrators or technology teachers/supervisors are required to organize the information given and make decisions regarding software and safety.

After the school district acquires information from the state education department, organizing is done to the extent in which information uncertainty is reduced. The result of this uncertainty reduction is a set of guidelines with which to work. Finally, teachers and students are made aware of the safety protocols in place and would be expected to follow the guidelines and work with administrators in keeping the Internet safe. The human interaction occurs between administrators, teachers, and students, which is the central phenomenon of this type of organization. Ultimately, changes in technology will occur, but the procedure with which to ensure Internet safety will remain the same.

Section 5: Conclusions About Selected Issues

Danger

According to the Library Media Specialist and a classroom teacher, the chances of students encountering dangers on the Internet have decreased significantly because of filtering software. Although the filtering software does provide some peace of mind for some educators, they said other practices need to be in place for students to get the most out of their online experience. In order to ensure the safety of students, educators say they must know the potential online dangers, safe search engines, what to do if students do encounter something dangerous, and they also must monitor student use on the computer.

Responsibility

Teachers accept ultimate responsibility because they are with students when students are online. But they say that responsibility falls on school districts as well as they are responsible for implementing policies, procedures, and guidelines. According to Quinn, “Schools receiving funding [under the Federal Government] must annually certify that they filter from access by children under the age of 17 years…” (191). Parents are another source of responsibility for keeping children safe on the computer. Parents are expected to monitor children, promote safe practices, and support policies that are incorporated in the schools. According to Berson, “Schools cannot address issues of technology use and misuse in isolation” (56). He also believes that “parent and community program components… are necessary for full implementation [of an Internet safety prevention program]” (56).

Opportunity Costs

All informants agree that the Internet is a useful tool. For example, they see the Internet as “access to the whole world”, “a good source for information”, and “an increased amount of available material.” But as useful as it is, the Library Media Specialist said it could also cause inconvenience. A technology administrator said when teachers are educating their students on the dangers of the Internet, they could be spending that time preparing students for a more immediate need, such as a state-mandated test. Similarly, the district’s technology administrator said money spent on updating filtering software could be spent on educational software to better prepare students for those state-mandated tests. Nevertheless, the Library Media Specialist said, “Internet safety has become a necessary part of instruction.” To lessen the amount of time and money spent on Internet safety, the district’s technology administrator said it is relevant for parents and communities to stay involved in the lives of children.

Education and Communication

Based on the data analysis, there does not seem to be an articulated Internet safety curriculum. A classroom teacher said, “I’d like our district to set up some policy and procedure or if there is one to communicate it to us better…most school districts are assuming that people use the Internet and know what’s safe and what isn’t.” According to Berson, “Educational strategies which focus on helping children and youth to develop autonomous and responsible skills online require education” (57). He also says, “The educational process can promote safer use of the Internet through competencies and attitudes targeted toward children in cyberspace” (57).

According to Reeks (146), there are “several ways…to protect one’s child online.” The article recommends that “parents get involved” with their children’s Internet experiences. She thinks parents should, “Instruct [their] child to come straight to [parents] when [they] see anything that makes [them] uncomfortable…” (146). Parents and children need to communicate as well as educators and caregivers. Berson recommends “a comprehensive educational program…involving teachers, parents and youth” (57).

Theory

Karl Weick’s Organizational Theory involves three specific branches in applying it to Internet safety. The first branch, “enactment,” is the act of using the Internet. The second branch, “selection” is represented by the decisions of the New York State Education Department. The final branch of the theory is “retention.” This phase applies to the guidelines that are passed on to teachers by administration.

The potential danger of using chat rooms is an example of how this theory applies to Internet safety. First, anyone can participate in a chat room on the Internet. The enactment is recognizing chat rooms as the situation being defined. Teachers need to understand the potential dangers chat rooms pose for students. If accessible to students, chat rooms allow them to interact with strangers.

The selection phase of the theory requires teachers to decide what they will address. First, teachers must know what to look for if students are gaining access to chat rooms. Students who are typing intermittently for any length of time could be engaged in a chat room. According to one teacher, if a student’s facial expression changes several times within a short period of time, they may be in a chat room.

Finally, the retention phase of the theory includes guidelines and rules the teacher will reinforce as a result of students engaging in chat rooms. This entails learning who to notify (ex. principal, technology administrator) and how to fix the problem. Perhaps the technology administrator should be notified to disengage the ability to access chat rooms.

Section 6: Assertions

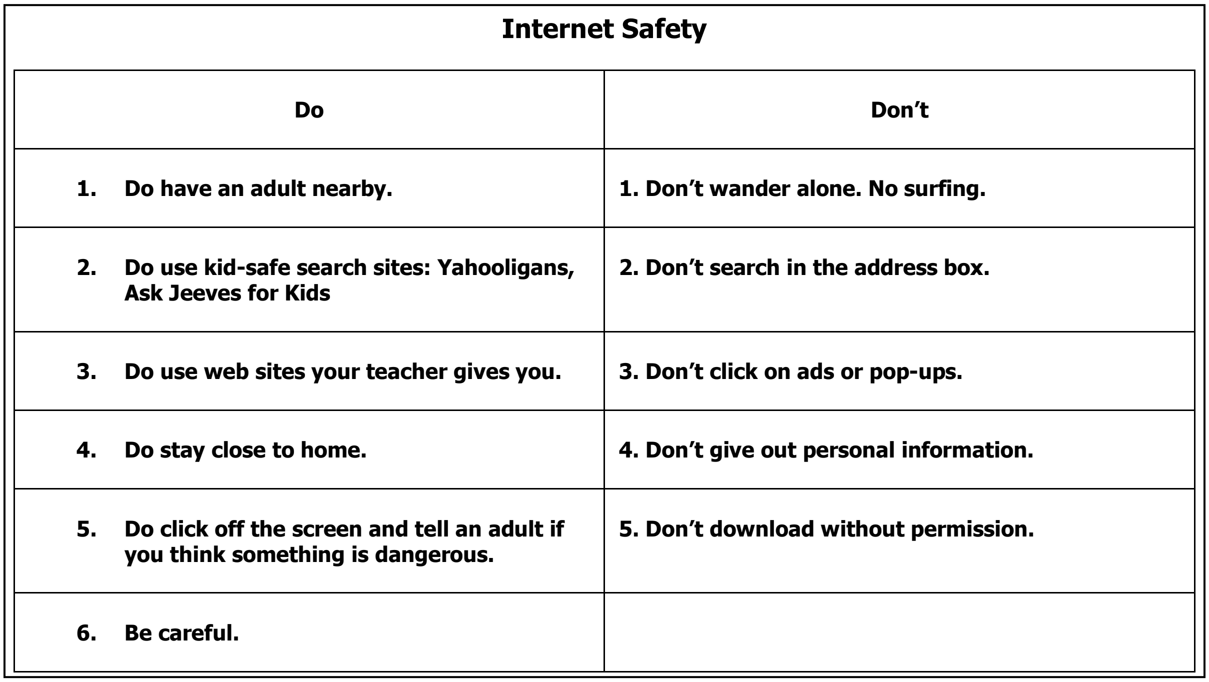
Prevention

One technology administrator believes that promoting Internet safety is preventing dangerous situations from taking place. He suggests districts identify what they regard as "dangerous" and define those dangers. Then they can establish procedures and guidelines based on those dangers. A classroom teacher identifies a need for most districts to train teachers about Internet safety and provide them with guidelines that students need to follow. Teachers can then transfer that knowledge to students, so students can understand why they are not allowed to access those sites. All informants believe that students need to understand the importance of Internet safety and follow the classroom or school guidelines and procedures (see Figure 6, page 35). The Library Media Specialist thinks the most important way to prevent students from gaining access to dangerous situations is to involve parents. According to Berson, there is a need for "prevention programs for both parents and educators…" (56).

Environment

Another way to promote Internet safety according to one technology administrator is to "provide a safe online environment for students." A classroom teacher does this by teaching students how to use kid-friendly search engines, how to use links that are on the school district website, and ways to handle circumstances that may lead students to dangerous situations. For example, teachers can educate students in how to exit a website they think is inappropriate and encourage students to tell teachers if these things happen. One educator had encountered this prior to the installation of the filtering software. She remembers, "I did have [inappropriate material] come up in Google searches with sixth graders where they would tell me about it…I would just say, don't click on it or if that makes you uncomfortable, 'x' out…at that point it was my first year…I hadn't taught anything [about Internet safety]."

Figure 6 – Internet Safety Poster



Internet Safety

Do	Don't
1. Do have an adult nearby.	1. Don't wander alone. No surfing.
2. Do use kid-safe search sites: Yahooligans, Ask Jeeves for Kids	2. Don't search in the address box.
3. Do use web sites your teacher gives you.	3. Don't click on ads or pop-ups.
4. Do stay close to home.	4. Don't give out personal information.
5. Do click off the screen and tell an adult if you think something is dangerous.	5. Don't download without permission.
6. Be careful.	

This poster shows the 'dos' and 'don'ts' of Internet safety.

Knowledge

Perhaps knowledge is the most important factor in Internet safety. Unfortunately, "A general lack of knowledge of online safety combined with an overburdened staff means that many cases of cyberabuse are overlooked" (Berson 56). Certainly, administrators and teachers need to know state regulations and acceptable-use policies (see Appendix F). All informants agree on the importance of students and parents knowing the benefits of the Internet, the dangers on the Internet, ways to decrease unsafe encounters (filtering software, monitoring, parental controls), and what can be done if they encounter something they think is unsafe. According to Thornburgh and Lin, "Adults must learn to teach children how to make good choices on the Internet. They must be willing to engage in sometimes difficult conversations" (45).

Freedom of Speech

According to Quinn (2003), "Legal issues pertinent to this [revolution in educational technology] include the First Amendment, harassment, privacy, special education, plagiarism, and copyright concerns, among others." The Library Media Specialist acknowledged that, "librarians are supposed to [be against] filtering because it's a free speech thing." However, she said, "I'm glad I'm filtered…I have peace of mind with the filtering that I didn't have the first two years, so it has relieved some of the responsibilities…" The district's technology administrator said, "I understand people being worried about censorship and right to information…[but] we need to protect our kids."

Conclusions

Because research indicates the Internet and technology are constantly changing, Internet safety requires a dynamic definition. This study indicates that Internet safety in schools is ultimately keeping students safe from the dangers that lurk online. The research indicates that dangers online include:

- pornography
- hate sites
- chat rooms
- predators
- strangers
- violence
- inaccurate information

Ways to keep students safe from these dangers include:

- using kid-safe search engines
- supplying links for students to access safely
- monitoring students' use
- educating
- communicating/awareness
- teaching students to click off the screen and tell an adult

Further Research

Quantitative data would be useful in learning first, if the conclusions drawn from this small sample apply to other school districts. It would also be useful to learn how many teachers have been trained in Internet safety, how many teachers use the Internet in their classroom, the number of teachers who have generated their own Internet use policies, the number of students who have encountered dangerous websites, and the number of times teachers are denied access to useful websites. In addition, examining a broader area or a larger number of districts would make the research more reliable. Quantitative data would provide insight into the everyday occurrences students and teachers have with the Internet. More research in general would be helpful in learning more about the effectiveness of filtering software.

Limitations

This case study was bounded in several ways. One limitation in this study was time. Studying the use of the Internet in schools over a five-month period is a short amount of time to obtain data. Unfortunately, time throughout the day was limited as well. In a small school, teachers have a lot of duties in addition to teaching, making it difficult to schedule interviews. The small sample size of this study was also a limitation. In order to make assertions that could apply to a larger population of schools, more schools would need to be studied and more time would be needed to conduct interviews. More teachers, parents, and students would need to be interviewed in order to make generalizations.

Section 7: Closing Vignette

The district installed filtering software in all of the schools shortly after Mrs. Kempney and Charles discussed kid-friendly search engines. Along with the new software, sixth grade teachers gave lectures to their students regarding acceptable use on the Internet. With all of this education, Mrs. Kempney was more at ease while her students were accessing the Internet.

Several months after Charles was reprimanded for using Google as his search engine, a new student enrolled at the school. The new student, unaware of school procedures, tried to access an inappropriate website (www.fireworks.com). The Denied Access screen (see Figure 2) appeared on his monitor, which was next to Charles. Charles noticed and said, “Derek, what are you trying to do?”

“I heard about this new site where you can buy fireworks and firecrackers. Why can’t I get there?” Derek responded.

“Well, the school district has filtering software installed on all the computers. If a website has things on it that kids shouldn’t see, the filter blocks it out and this screen pops up,” said Charles while pointing to Derek’s monitor.

“Oh, that stinks. I guess I’ll just wait until I get home to order the fireworks,” Derek said in a disappointed voice.

Charles said to Derek, “By the way, don’t use Google to search. We are only allowed to use Kidsclick.com, askjeevesforkids.com, or yahooligans.com. I got in trouble a few months ago, and it’s really not worth it.”

Mrs. Kempney was standing quietly nearby. She smiled to herself and was grateful that Charles had learned his lesson and that educating students in conjunction with the use of filtering software was, at least in this case, effective.

Appendix A: Excerpts from the Child Online Protection Act and the Children's Internet Protection Act

TITLE XIV--CHILD ONLINE PROTECTION

SEC. 1401. SHORT TITLE.

This title may be cited as the ``Child Online Protection Act''.

SEC. 1402. CONGRESSIONAL FINDINGS.

The Congress finds that—
(1) while custody, care, and nurture of the child resides first with the parent, the widespread availability of the Internet presents opportunities for minors to access materials through the World Wide Web in a manner that can frustrate parental supervision or control;

(2) the protection of the physical and psychological well-being of minors by shielding them from materials that are harmful to them is a compelling governmental interest;

(3) to date, while the industry has developed innovative ways to help parents and educators restrict material that is harmful to minors through parental control protections and self-regulation, such efforts have not provided a national solution to the problem of minors accessing harmful material on the World Wide Web;

(4) a prohibition on the distribution of material harmful to minors, combined with legitimate defenses, is currently the most effective and least restrictive means by which to satisfy the compelling government interest; and

(5) notwithstanding the existence of protections that limit the distribution over the World Wide Web of material that is harmful to minors, parents, educators, and industry must continue efforts to find ways to protect children from being exposed to harmful material found on the Internet.

SEC. 1403. REQUIREMENT TO RESTRICT ACCESS BY MINORS TO MATERIALS COMMERCIALLY DISTRIBUTED BY MEANS OF THE WORLD WIDE WEB THAT ARE HARMFUL TO MINORS.

Part I of title II of the Communications Act of 1934 (47 U.S.C. 201 et seq.) is amended by adding at the end the following new section:

``SEC. 231. RESTRICTION OF ACCESS BY MINORS TO MATERIALS COMMERCIALLY DISTRIBUTED BY MEANS OF WORLD WIDE WEB THAT ARE HARMFUL TO MINORS.

``(a) Requirement To Restrict Access.--
``(1) Prohibited conduct.--Whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined…

CHILDREN’S INTERNET PROTECTION ACT (Pub. L. 106-554)

TITLE XVII--CHILDREN'S INTERNET PROTECTION

SEC. 1701. SHORT TITLE.

This title may be cited as the ``Children's Internet Protection Act''.

SEC. 1702. DISCLAIMERS.

DISCLAIMER REGARDING CONTENT.--Nothing in this title or the amendments made by this title shall be construed to prohibit a local educational agency, elementary or secondary school, or library from blocking access on the Internet on computers owned or operated by that agency, school, or library to any content other than content covered by this title or the amendments made by this title.

(b) **DISCLAIMER REGARDING PRIVACY.--**Nothing in this title or the amendments made by this title shall be construed to require the tracking of Internet use by any identifiable minor or adult user.

SEC. 1703. STUDY OF TECHNOLOGY PROTECTION MEASURES.

IN GENERAL.--Not later than 18 months after the date of the enactment of this Act, the National Telecommunications and Information Administration shall initiate a notice and comment proceeding for purposes of;

(1) evaluating whether or not currently available technology protection measures, including commercial Internet blocking and filtering software, adequately addresses the needs of educational institutions;

(2) making recommendations on how to foster the development of measures that meet such needs; and

(3) evaluating the development and effectiveness of local Internet safety policies that are currently in operation after community input.

DEFINITIONS.--In this section:

TECHNOLOGY PROTECTION MEASURE.--The term ``technology protection measure'' means a specific technology that blocks or filters Internet access to visual depictions that are;

(A) obscene, as that term is defined in section 1460 of title 18, United States Code;

(B) child pornography, as that term is defined in section 2256 of title 18, United States Code; or

(C) harmful to minors.

(2) **HARMFUL TO MINORS.--**The term ``harmful to minors'' means any picture, image, graphic image file, or other visual depiction that--

(A) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

(B) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

(C) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

(3) **SEXUAL ACT; SEXUAL CONTACT.--**The terms ``sexual act'' and ``sexual contact'' have the meanings given such terms in section 2246 of title 18, United States Code.

Subtitle A--Federal Funding for Educational Institution Computers

SEC. 1711. LIMITATION ON AVAILABILITY OF CERTAIN FUNDS FOR SCHOOLS.

Title III of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 6801 et seq.) is amended by adding at the end the following:

``PART F--LIMITATION ON AVAILABILITY OF CERTAIN FUNDS FOR SCHOOLS

``SEC. 3601. LIMITATION ON AVAILABILITY OF CERTAIN FUNDS FOR SCHOOLS…

Appendix B: Original Interview Protocol

Interview Protocol
Project:
Time of Interview:
Date:
Place:
Interviewer:
Interviewee:
Position of Interviewee:

(The purpose of this case study is to describe and understand the Internet restrictions (for the purpose of safety) and the effectiveness of these restrictions in schools.)

Questions:

1. **What role does Internet Safety play in our school?**

2. **How does Internet Safety influence/impact teaching?**

3. **How does Internet Safety affect student computer use?**

4. **How are Internet Safety guidelines implemented in the classroom?**

5. **How effective are Internet Safety guidelines?**

6. **What about state guidelines and curriculum regarding the Internet?**

7. **Who else should I talk to about Internet Safety?**

Appendix C: Revised Interview Protocol

Interview Protocol
Project:
Time of Interview:
Date:
Place:
Interviewer:
Interviewee:
Position of Interviewee:

(The purpose of this case study is to discover the meaning of Internet safety.)

Questions:

1. **What is Internet Safety?**

2. **What is the purpose of Internet safety?**

3. **What is your role with regard to Internet safety?**

4. **What would you like to see with regard to Internet safety?**

5. **What do you consider a safe website? (What makes a website safe?)**

6. **What has been the impact of web safety in our school environment?**

7. **Have there been any events that were unsafe?**

8. **Who else should I talk to about Internet Safety?**

Appendix D: Ethics Permission Form

Ethics Protocol for Case Study Research

Kathleen Palinski

This authorization is being requested in part to fulfill requirements of the State University of NY Institute of Technology's Human Subjects Research Review Board as well as state and federal regulations regarding the use of human subjects in research. The project involves a case study that may be used in my master's research at the SUNYIT Information Design and Technology Master's program. Excerpts or rewritten versions may also be submitted to professional journals for publication. The case study involves the examination of Internet safety software and restrictions in grades five and six. The work involves participant and non-participant observations, one-on-one and group interviews, and scheduled visits.

I can be reached at *315-339-0959.* I would be happy to answer any questions about the project.

I would like to reassure you that as a participant in this project you have several rights.

- Your participation in these studies is entirely voluntary.
- You are free to decline to answer any question at any time.
- You are free to withdraw from the study at any time.

My notes from meetings, interviews, and observations will be kept strictly confidential. Excerpts from these notes may be made part of the final thesis.

Copies of the final publications will be supplied whenever possible and as requested.

I would be grateful if you would sign this form to show that you have read its contents.

____ signed
____ printed
____ dated

Appendix E: Stranger Danger Definition

This definition comes from the Keller, Texas police department website: http://www.kellerpd.com/childsafe.htm.

Child Safety

STRANGER AWARENESS

Definition of a "stranger": Any person who your parents/guardians have not given you permission to be or go with.

Safety Rules to Protect Yourself from Stranger Danger

1. **Never talk to strangers**
2. **Never let a stranger get too close to you**
3. **Never take candy, a present or anything from a stranger**
4. **Never tell a stranger your name, address or phone number**
5. **Never get into a stranger's car**
6. **Never go into deserted places alone**
7. **Always try to walk with friends or an adult**
8. **If a stranger grabs you, yell as loud as you can saying things like, "Help!!" "Call the Police," "This isn't my parent!"**

If a Stranger Follows You

1. **Run to a place where there are people, like a store or a restaurant and call for assistance from a person that works there such as a cashier**
2. **Don't run any place that is dark or deserted like a movie theatre or a park or an alley**

If You Are Home Alone

1. **Never open the door to anyone knocking or ringing the bell**
2. **Never tell anyone calling on the phone that you are home alone**

Your Private Parts

1. **Never let anyone touch your private parts**
2. **If someone touches your private parts, tell your parents or someone you trust (adult) like a teacher**

Appendix F: Acceptable-Use Policy/District Internet Safety Policy

POLICY

INSTRUCTIONAL **8069**

INTERNET SAFETY POLICY

I. A. Although the District recognizes the value of the Internet as an educational tool, it also understands that information with no redeeming social value is accessible through the Internet.

B. 1. The District has developed and will enforce this Internet Safety Policy in compliance with the Children's Internet Protection Act (CIPA) and the Neighborhood Children's Internet Protection Act (NCIPA).

2. In addition, the District maintains its "Access to Networked Information Resources Policy" which governs the acceptable use of the Internet by students and employees.

II. Access to the Internet using the District's computer equipment is subject to the following restrictions:

A. **Filtering**. Filtering software will be used to block minors' access to:

1. visual depictions that are (a) obscene, (b) child pornography, or (c) harmful to minors;[1] and
2. Internet sites which, in the Board's determination, contain material which is "inappropriate for minors." (See item B. below.)

Adult access to visual depictions that are obscene and/or child pornography will also be blocked. However, the Superintendent or his/her designee may disable the software to enable access to blocked sites for bona fide research or other lawful purposes.

B. **Matter Inappropriate for Minors**. The Board will determine by resolution what Internet material is "inappropriate for minors" in the District. This determination will be based on community standards.

[1] The terms "obscene", "child pornography", "harmful to minors," and "matter inappropriate for minors," used throughout the policy, are defined in the Children's Internet Protection Act and the Neighborhood Children's Internet Protection Act (Public Law 106-554). See Appendix A.

References

Berson, Michael J. "Lessons Learned About Schools and Their Responsibility to Foster Safety Online." Journal of School Violence 2 (2003): 105-117.

"Child Online Protection Act." Electronic Privacy Information Center. 2004. 10 April 2005. http://www.epic.org/free_speech/censorship/copa.html.

"Children's Internet Protection Act." Internet Free Expression Alliance. 2001. Miscellaneous Appropriations Act, 10 April 2005. http://www.ifea.net/cipa.html.

"Child Safety." Keller Police Department. 2005. TexWeb, 10 April 2005. http://www.kellerpd.com/childsafe.htm.

Creswell, John W. Qualitative Inquiry and Research Design: Choosing Among Five Traditions. Thousand Oaks, CA: Sage Publications, Inc., 1998.

Demirbilek, Muhammet, Sebnem Cilesiz, and Dogan Tozoglu. "Safety Strategies While Surfing Online in the Classroom." Annual Proceedings of Selected Research and Development (2001).

Greenfield, Patricia M. "Developmental Considerations for Determining Appropriate Internet Use Guidelines for Children and Adolescents." Applied Developmental Psychology 25 (2004): 751-762.

Kreps, G.L. Organizational communication (2nd ed.). New York: Longman, 1990.

Nadeau, Susanne. "Students Get 'Key' to Internet Safety." Knight Ridder Tribune Business News 31 March 2005: 1.

Quinn, David M. "Legal Issues in Educational Technology: Implications for School Leaders." Educational Administration Quarterly 39 (2003): 187-207.

Reeks, Anne. "Internet Safety." Parenting March 2005: 146-149.

Thornburgh, Dick, and Herbert Lin. "Youth, Pornography, and the Internet." Issues in Science and Technology 20 (2004): 43-48.

"Top Free Screensavers." Screensavers.com. 2005. Screensavers.com, 10 April 2005. http://www.screensavers.com/landing/top4_flash_sb.html?source=popfastclick&aff_id=865.

Weick, K.E. The social psychology of organizing (2nd ed.). Reading, MA: Addison-Wesley Publishing Company, 1969.

Wishart, Jocelyn. "Internet Safety in Emerging Educational Contexts." Computers & Education 43 (2004): 193-204.

Kathleen Anne Palinski
22 January 1976
Rome, New York 13440

704 West Embargo Street
Rome, New York 13440
(315) 339-0959
kat_palinski@yahoo.com

Education

State University of New York Institute of Technology
Pursuing a Master of Science Degree in Information Design and Technology
Marcy, New York
Current; Expected date of graduation: December 2005

University of New Hampshire
M.A., Elementary Education, Reading Concentration
Durham, New Hampshire
September, 1999

State University of New York College at Geneseo
B.S., Elementary Education, Art History Concentration
Geneseo, New York
May, 1998

Work Experience

Oneida City School District; Sylvan-Verona Beach Elementary;
Verona Beach, New York: 2002-2005
Remedial reading teacher/Academic Intervention Services Provider
Worked closely with K-6 teachers in planning and implementing curriculum
Taught English Language Arts to students in whole groups and small groups in grades K-6
Member of Student Assistant Team

Oppenheim-Ephratah Central School;
St. Johnsville, New York: 2000-2002
Remedial reading teacher/fifth and sixth grade ELA teacher
Worked closely with grades 3-6 team

Williford Elementary School;
Rocky Mount, North Carolina: 1999-2000
Fourth Grade Teacher
Instructed group of twenty students as part of the fourth grade team
Conducted reading and writing workshops on a daily basis

Relevant Skills

Comprehensive knowledge of InDesign 2.0
Vast knowledge of computer applications including Microsoft Word, Excel, PowerPoint, MacIntosh, Lotus, Internet, Photoshop
Skilled in desktop publishing
Extensive research ability
Skilled in written communication

Awards

SUNYIT Writing/Design Contest, second place in design category
Rome Daily Sentinel, first place winner in city logo contest