Adena Raub
EDUC478
April 27, 2005

Cyber Security and Children

Problem:

We are privileged to live during an age of such tremendous technological advancement, especially concerning the developments in communications that are made on a daily basis. Today's youth can discover information from all corners of the earth with the click of a button, virtually tour the most incredible landmarks on the planet, and interact with people across the street or across an ocean.

However, such ease in communication can allow for predators to reach children easier as well. Without proper protection, even adults can fall into the traps of those that breach cyber security. Children are even more vulnerable. They are meeting strangers in chat rooms. They are distributing their personal information freely. They are downloading viruses. Today's youth is in serious danger.

Youth make up the largest percentage of Internet users in the United States (Bawer p.1). Children are adapting to technology with incredible speed, but unfortunately, many children do not recognize the potential vulnerabilities that they are opening themselves up to when they use the Internet. A report by The National Cyber Security Alliance revealed, "According to research firm eMarketer, 75 percent of children believe it's okay to reveal private family information online in exchange for free gifts" (Bawer p.3). Such a statistic is frightening and should be of critical concern to all parents whose children use the Internet

In order to clear up the misconceptions held by the nation's children concerning their assumed safety while using the Internet, adults must educate children about the potential dangers that arise during Internet use. Clearly, parental supervision is an excellent way to prevent children from misusing the internet, but of course parents can not always be present in every situation in which their children will use a computer. Therefore, if parents first educate themselves to the risks involved, and then teach their children about cyber security through using a computer-based curricula and activities the result will be much more comprehensive.

Parent Resources:

Due to the recent realization that children are exposed to such risks, many organizations and government agencies have compiled guides for parents to monitor the Internet use of their children. The FBI, for instance, has drafted, **"**A Parent's Guide to Internet Safety" which outlines warning signs that children are misusing the Internet such as children spending excessive time on the computer at night or receiving gifts from strangers in the mail (FBI p.3). The guide also provides parents with steps to take if they suspect that their child has been involved in communication with a sexual predator, as well as how to minimize a child's victimization.

Similarly, *GetNetWise* has produced an extremely inclusive guide for families including a breakdown of what children should be permitted to access depending on the child's age as well as the different types of risks that haunt children who use the Internet.

For instance, the section titled, “Meeting someone Online,” points out that most of the children who end up being lured by Internet predators are in fact over the age 15 and female (Internet Education Foundation).

Though created for educators, the guide “Safe and Responsible Use of the Internet” provides information that would be useful for parents who are both tech-savvy and those that may consider themselves technologically challenged. The guide is simple to understand with comparisons like, “Allowing young children to have supervised, open access to the Internet (filtered or not) without close supervision would be the equivalent of leaving a child to play unsupervised in New York City's Central Park” (Willard 3). The guide is comprehensive, examining topics such as protection and empowerment, inappropriate material, and legal issues. Some of the sections are specifically aimed at the use of the Internet and technology in schools which may be useful for parents who are very concerned about their children’s cyber security while they are using school computers.

Parents need to know the risks that their children face when they sign on to use a computer. By familiarizing themselves with material that outlines the risks at hand, parents are taking a first step towards their children’s security. Once parents learn how to prevent their children from being exposed to such risks, parents are moving forward even more to help. However, a well-informed parent is not enough to keep a child safe. The child needs to be equally as informed about how predators use the Internet in order that the children can protect themselves.

Resources for Parents to Teach Children:

Though a new threat, many prominent educational organizations have formed to protect children from breaches of cyber security. Even more organizations have developed curricula to teach children about the dangers that exist on the Internet and how to avoid such dangers. Many of these curricula are easily available online for free. For instance, Cyber Smart has developed a free curriculum for grades K-8 that focuses on the areas of security, manners, advertising, research, and technology. The curriculum includes worksheets, activities and kid-friendly links. “Lessons combine an effective mix of offline and online activities. Offline lessons can be taught without computers or an Internet connection. Online lessons require an Internet connection; however, it is not essential that every student have use of an Internet-ready computer at the same time” (Cybersmart.org).However, Cyber Smart is just one example of one type of Internet tool to educate children.

Aside from entire curricula, many children’s Web sites have adopted sections that are devoted to cyber security. For instance, Disney Online has adopted a set of activities that allow children to watch comics and play games involving their favorite characters, but they also learn about important cyber security techniques. Some of which have a “what would you do?” format. Following the comics, the child is always debriefed by a character about the lesson that was just presented in order to reiterate.

Similar sites are available for older children and teenagers, with the interactive nature, but without the cartoon feel. Besides discussing computer security, Chatdanger.com also discusses the potential dangers in using telephones to go online or to text message. More pertinent to cyber security, however, the site offers information

about the dangers of online chat, instant message, e-mail, and games. The sections about each of the uses of technology include the stories of those who have made mistakes in cyber security in the past. Additionally, the sections contain information about how to remain safe while participating in the discussed activity. For instance, in the information section of the "chat" section, the following advice is offered, "Check your profile and make sure it doesn't include any personal information (name, address, telephone number, mobile number, private email address, picture)" (Chatdanger.com). Each section also has games to emphasize the issues discussed through the personal stories. For instance, the "Back Chat" game emphasizes that people chatting on the Internet are not always who they seem to be.

Another Web site, ThinkUKnow.Com is based in the United Kingdom and offers a mixture of information and interactive activities to educate about the importance of cyber security. The game has a clickable "lounge" scene in which clicking on the various characters and objects in the room results in a different game, personal testimony, or informative tip about security. Again, this site is aimed toward an older group than the Disney games, but it is less wordy, but also less informative than ChatDanger.Com

Different formats work better for different children. Regardless of the characters used or games involved, it is important that children get the chance to experience these types of activities themselves, rather than just being told the information by a parent. "Children must learn to make secure computing choices even when adults are not watching. As children mature, they begin to venture into public places on their own and take more responsibility for their own physical security. Similarly, as children age, they make independent computing decisions based on a foundation of learned skills" (Bawer 14). Many of these activities require the user to apply his or her prior knowledge or make a judgment call about a situation in order to complete the activities. In doing so, the child can take a "hands-on" approach to his or her own cyber security.

Filtering or Nanny Software:

In order to allow children to have more freedom in their Internet use and not always have to depend upon a pair of parental eyes for protection, many parents and schools use filtering software that determines what children can or can not see when using the Internet. Most filtering software allows parents to choose what types of content to block from children. According to ConsumerReports.org, filtering can occur through three main processes: software analysis (in which the software rapidly evaluates the content of a Web site), human analysis (sites are reviewed by staff and then placed on either a blocked list or an allowed list), or site labeling (owners and creators of sites voluntarily submit the level of content on their sites).

All three of the types of filters had flaws in either blocking too many Web sites, (for instance if one word was considered to be explicit) or would not block enough material. Consumer Reports concluded that America Online's Young Teen setting is the best for blocking prohibited material out of the filtering software that was tested (p.2). Results varied about which software blocked sites that seemed appropriate for children.

Besides AOL, Consumer Reports determined that the best filtering software is Cyber Patrol, which allows for a time limit to be placed on users, as well as the parental option to allow or block sex education sites. All of the programs tested offered the ability

to control what personal information is submitted by children to Internet users. However, ConsumerReports.Org also determined that this function was not enough for parents to rely upon in protecting the disclosure of information.

Resources Need to Be Used:

Though there is a plethora of information available both free on the Internet and that can be purchased, if the information and activities are not used, no progress will be made. The motivation for such education must come from the parents, because children do not see their actions as a problem.

Importantly, parents and influential adults must be able to step forward and lead by example. If children watch their parents participate in breaches of cyber security or bad habits while using the Internet, the children will simply follow suit. “But most adults are in no position to lead the way. Commonplace security breaches are widespread among homes with broadband access to the Internet. And when it comes to stealing and cheating online, most are no different than children. Neither group thinks it is wrong” (Bawer p.2).

Additionally, parents must also take the initiative to make their home computers as safe as possible for their children. A variety of “nanny” or “parental control” software is available that filters the web sites that children are able to see. The National Cyber Security Alliance found that, “97 percent of homes in which children have broadband access do not utilize filters or parental controls” (Bawer 2). Parental controls are often provided by ISPs such as America Online and others in order to filter what is seen by little eyes. Settings can be determined to control the amount of chatting and with whom, and timers can be set to limit children from spending excessive hours online. These tools are especially useful for parents who can not supervise their children exploring the Internet. Not using such tools just leaves children more vulnerable.

In order to protect children, parents, teachers, and the community as a whole must make conscious decisions to educate ourselves and the children we care about in order to provide protection from predators that use the Internet as a tool to accomplish their treachery. Children do not fall into the traps of these predators because they are mischievous, but rather they are naïve to the way the Internet works and how it can be used to do harm.

Internet Awareness and Cyber Security Plan:

I. Self Education
    a. Compile Information
        i. Internet Predators
        ii. Inappropriate Internet material
        iii. Filters and Parental Controls
        iv. Sharing Information on the Internet
        v. Chat room Protection
II. Devise a Plan
    a. Educate Children
        i. Discuss information Discovered

ii. Discuss consequences
iii. Create rules for Internet Use

b. Provide Children With Hands-On Cyber Security Activities
i. Choose Age Appropriate Material
ii. Discuss the Material With Children

III. Execute Security Measures
a. Use Filter or Nanny Software if You Choose
b. Monitor Internet Use and Behavior of Child
c. Use secure practices yourself to role model for child

Conclusions:

Though a lack of cyber security is an issue plaguing youth that use the Internet, the threat has been recognized, and parental concerns are being addressed by the creators of Web sites and the makers of software. By writing about cyber security and creating activities to teach children, those who make their living in the Internet industry are empathizing with parents and doing what they can to assist in protecting the children.

Resources about cyber security are abundant on the Internet, and a simple Google search of the terms "cyber security" will result in too many Web sites to visit. However, more than just visiting the sites that hold the information about cyber security, the information from these sites must be absorbed by parents and then transposed to children. Additionally, children need to get the chance to grab the bull by the horns and learn through activities about their own security when using the Internet. Parents also need to step up in action by role modeling positive decisions in using the Internet.

Additionally, as quickly as technology is adapting, children are adapting, and unfortunately, those that prey on children also can adapt. Therefore, to counter those who abuse technology, parents and teachers must also keep a constant watch for new technologies and how they are used, especially in consideration to communication technology.

Works Cited

"About Kids Safety." *GetNetWise*. Internet Education Foundation. Apr 20 2005. < http://kids.getnetwise.org/safetyguide/kids>

Bawer, Mala. "An Action Agenda for Securing the Nation's Digital Resources: Start in Kindergarten!" *The National Cyber Security Alliance*. May 5 2004. Apr 20 2004. < http://www.staysafeonline.info/resources /NCSAEducationWhitePaper.pdf>.

Childnet International. *ChatDanger*. 2004. Apr 19 2005. <www.chatdanger.com>

"Curriculum Scope." *Cybersmart*. 2005. Apr 20 2005. < http://www.cybersmartcurriculum.org/curr_over/>.

"Digital Chaperones for Kids." *ConsumerReports.Org*. March 2001. April 21 2005. <http://www.consumerreports.org/main/content/display_report.jsp?FOLDER%3C%3Efolder_id=348251&bmUID=1114655344405>.

Federal Bureau of Investigation. "A Parent's Guide to Internet Safety." Apr 19 2005. < http://www.fbi.gov/publications/pguide/pguidee.htm>

Willard, Nancy. "Safe and Responsible Use of the Internet: A Guide for Educators." 2003. Apr 20 2005. < http://responsiblenetizen.org/onlinedocs/pdf/srui/sruilisting.html>