THE INTERNET, A SECRET MINEFIELD FOR CHILDREN

by

David Plude

A Capstone Project Submitted to the Faculty of

Utica College

August 2013

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Cybersecurity

Abstract

Numerous changes in technology since the year 2000 have increased the availability of the Internet, increased the amount of Internet activity among children, and expanded the age range of Internet users. Children are in danger while in their own homes like never before. Dangers such as cyberbullying, sexting, identity theft, and terrorist radicalization are hidden dangers in a virtual minefield. Children are also at risk of damaging their online reputation that will prove to be costly in the future, if they do not learn how to avoid these dangers. The purpose of this research was to evaluate the Internet safety education for children in Virginia schools to determine if they are adequately preparing children for the online world. What minefields await children when they go online? What are Virginia schools doing now to educate children about the dangers and the proper usage of the Internet? What challenges may prevent teachers and schools from delivering a comprehensive Internet safety education program? While schools must comply with the Children's Internet Protection Act (CIPA) in order to receive e-funds for Internet access, merely preventing access while on school grounds is not enough. Congress passed the Protecting Children in the 21st Century Act in 2008, identifying public schools as the educator of children to prepare them for Internet life. The act requires public schools to educate their students about cyberbullying, online safety, and sexual predators. Much of how the school system complies with this act remains up to the individual school district; therefore, they may not be giving this the proper attention. Schools have an obligation to provide safety education to students. Keywords: Cybersecurity, Professor Chris Riddell, First Amendment, Cyberethics, Cybersafety, Character Education.

Acknowledgments

My first acknowledgement is to God for providing a clear direction in my life. It was His plan for me to pursue a Master's Degree in Cybersecurity. He has always been faithful to guide me. He carried me through this process. It is because of Him that I am successful. All glory belongs to Him.

Many thanks to my wife, Treasa, for allowing me the time and effort that this program required. She never questioned my pursuit of a Master's Degree because she also saw that God had a plan for me, and she was behind me from the beginning. I could not have done this without your support. To my three children: Britney, Nicolas, and Ashley, who for many nights and weekends wondered where I was; what was I doing in my office for so long; this research is for you. My passion to keep children safe online stems from wanting to protect you three as much as possible. I tried to keep family life in balance with school and work. Sometimes I was successful and sometimes I was not. I hope that one day you will realize that the sacrifices we made now have a lasting effect into the future. Never stop searching for ways to learn new things.

To the staff at Utica College, I express my sincere gratitude for the time and efforts you put in to ensure that each student succeeds. I never felt left alone. Many thanks to my Professor and Capstone chair, Chris Riddell who always had time and advice. He challenged me to consider views that turned this project from good to great. However, my deepest gratitude goes to Cynthia Gonnella, my second reader as well as Capstone advisor. Her passion for protecting children online far surpassed mine. She inspired me to take the extra step when necessary. She challenged me in ways that elevated my research beyond my original intent.

It is my desire that someone will read this research and make changes to their programs to educate children. If this research saves even one child, it was worth my effort and then some.

Table of Contents

List of Illustrative Materials

The Internet, a Secret Minefield for Children

The Internet can be a dangerous place for children, especially for those who have not been taught to protect themselves. Threats to children come in many forms including identity theft, cyberbullying, online grooming, and abduction, to name a few. Children can jeopardize their future reputation if not careful how they use the Internet today. Children can even become weapons used by terrorists against the United States. Equipping children, with knowledge and tools to protect themselves is essential to keeping them safe online and protecting their online identities. This education needs to start in kindergarten and continue through high school (Pruitt-Mentle, 2008). Linda Sharp, director of the Cyber Security for the Digital District program at the Consortium for School Networking (CoSN) states, "We need to start on Web usage education as soon as students are on the computer" (Butler, 2010, p. 53). PewResearchCenter conducted a survey of 2,462 Advanced Placement and National Writing Project teachers and found that digital technologies helped them in teaching their students in many ways (Purcell, Heaps, Buchanan, & Friedrich, 2013). Among the technologies used were mobile phones, e-readers, and tablet computers. Schools have an obligation to provide safety education to students as they introduce them to these technologies. The purpose of this research was to evaluate the Internet safety education for children in Virginia schools to determine if they are adequately preparing children for the online world. What minefields await children when they go online? What are Virginia schools doing now to educate children about the dangers and the proper usage of the Internet? What challenges may prevent teachers and schools from delivering a comprehensive Internet safety education program?

Numerous changes in technology since the year 2000 have increased the amount of Internet activity among children. In 2000, the U.S. Census Bureau estimated nearly 48% of teens

12 to 17 used the Internet at home (U.S. Census Bureau, 2001). By 2010, the number of teens between the ages of 12 and 17 that went online nearly doubled to 93% (Lenhart, 2010). A large part of the increase may be attributed to the introduction of mobile and gaming Internet devices. For instance, nearly 75% of teens 12-17 are accessing the Internet on cell phones, tablets, and other mobile devices (Madden, Lenhart, Duggan, & Gasser, 2013). Gaming systems such as Microsoft's XBOX and Sony's PlayStation3 allow users to connect to the Internet for gaming and chatting with other players around the world (Xbox One - How It Games). Terrorist cells are using these online games for planning, training, and recruiting for future attacks (Besheer, 2007). This leaves unprepared children vulnerable not knowing how to protect themselves and their personal information.

In addition to new technologies, the availability of the Internet has dramatically increased. The Internet is usually available to children these days via broadband connections at home, at schools, and free Wi-Fi hotspots. In the early days of the Internet when only dial-up was available, people typically connected only one device at a time. In addition, they generally paid for access by the minute, therefore, only connecting to the Internet to conduct specific business, and then disconnecting. In 2008, 71% of people connected to the Internet via some sort of constant broadband connection (Lenhart, 2010). The introduction of wireless routers has made it possible for multiple devices to connect to the Internet simultaneously. A study published by Parks Associates in 2013 shows that 78% of households with broadband Internet connections have a home network. They expect that to grow to 95% by 2016, and each household will have an average of 4.5 connected devices (Parks Associates, 2013). This allows children to connect to the Internet anywhere and anytime they want within their homes using their computers, iPods, iPhones, tablets, and games. Predators then have access to children 24 hours a day, 7 days a

week. Emma Teitel wrote an article about cyberbullying in which she describes her own experiences using the Internet, "While mom and dad were upstairs watching Frasier, we would be in the basement 'exploring' the Internet," stated Teitel (Teitel, 2012, para. 4). Teitel went on to say, "Sure, our parents checked in every once in a while…but it was when we went out, to the movies or a party, that they checked in with greater frequency and angst" (Teitel, 2012, para. 4). Parents assume their children are safe because they are home. However, they could be exploring a dangerous digital neighborhood; completely unprotected.

New technologies have not only increased the usage; they have expanded the age range of users. In 2009, Nielsen Online conducted a study of Internet usage among American youngsters, and found that close to 16 million children ages 2 to 11 were online during the month of May alone. Children in that age group made up 9.5 percent of total Internet users in the U.S. (Chow, 2009). Many of the younger ages are experiencing the Internet while in the laps of older users (Chow, 2009). Children watch parents provide personal information as they fill out applications, sign up for accounts, or access existing accounts. They may not understand the difference between when it is safe to provide certain information and when it is not. Without proper education, these children grow up failing to understand how their physical worlds and virtual worlds are very much connected.

A significant concern involving the abuse of technology is cyberbullying. Bullying among students is not a new phenomenon. However, cyberbullying takes advantage of cell phones, computers, and other electronic devices to harass students at any time and any place, taking it to a new level. Stopbullying.org defines cyberbullying as bullying using any form of electronic technology including "cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites" (StopBullying.gov, para.

1). Cyberbullying reaches far beyond the playground; it is a continuous event with no boundaries and no end. Experts attribute bullying as a significant factor leading to many of today's teen suicides. In 2006, Megan Meier experienced harassment on MySpace through the use of a fake profile set up for the sole purpose of harassing her, which ultimately led to her suicide (Jacobs, 2010). Rachel Neblett became petrified with fear while someone bullied her using a fake MySpace account. She received threatening emails and messages from this person and committed suicide because of these threats. (Jacobs, 2010).

In 2007, about one-third of teenagers faced some sort of online harassment including rumors spread about them, receiving threatening messages, forwarding of private material without permission, or posting of embarrassing pictures (Lenhart, 2010). In 2010, estimates reported 77% of children ages 10-16 were victims of bullying and 86% of them turn towards violence on themselves or others (Spencer, 2010). Many states have passed laws to address cyberbullying issues in some form. However, the laws are only reactive and do little for prevention. The real key to protecting children requires a proactive approach. Children today are growing up with the Internet as a major part of their lives. Children must be educated that what they do in their online world can have serious and lasting effects in the offline world, for them and others.

Many schools use technology in their curriculum. For example, the GO Center at R.S. Payne Elementary School, in Lynchburg, Virginia, integrates technology into its curriculum using computer experiences designed to help students learn. The school provides two networked computer labs with access to the Internet. In addition, the school maintains a wireless mobile laptop lab. All grades use the computer lab at least twice a week (Lynchburg City Schools, 2013). Schools integrating the Internet into their curriculum, expose children to the associated

online dangers. Therefore, those schools have an obligation to teach students to protect themselves online. Schools typically provide access to technology and the Internet in a safer environment than usual due to the use of firewalls and filters. In fact, the Federal Communications Commission (FCC) requires that schools seeking to receive discounts on Internet access comply with the Children's Internet Protection Act (CIPA). CIPA requires that

> School and library Internet safety policies must include a technology protection measure that protects against Internet access by both adults and minors to visual depictions that are (1) obscene; (2) child pornography; or, with respect to use of the computers by minors, (3) harmful to minors. (Federal Communications Commission, 2012)

In an effort to address the education gap, Congress passed the Protecting Children in the 21st Century Act in 2008, identifying public schools as the educator of children to prepare them for Internet life. The act requires public schools to educate their students about cyberbullying, online safety, and sexual predators (Jacobs, 2010). Much of how the school system complies with this act remains up to the individual school district; therefore, they may not be giving this the proper attention. A cybersafety survey in 2010 reported that only about 50% of school districts require lessons in online safety as part of their curriculum; 40% of teachers taught nothing about security or the dangers of social networking sites, and 30% taught nothing about online ethics (Khadaroo, 2010). "Schools are much more likely to have shielded students from certain content than to have integrated lessons about appropriate behaviors into their curriculum" (Khadaroo, 2010, para. 6). Shielding students using filters or policies while at school is not enough.

Laws, policies, filters, and firewalls may prevent some information from getting to children. However, none of these processes will necessarily keep them from voluntarily

providing sensitive information. When children are off school property, they must know how to protect themselves from inappropriate content when filters and firewalls are not in place. Khadaroo quotes Nancy Willard, a consultant who runs her own Center for Safe and Responsible Internet Use, "What we have to do is empower them with the knowledge, skills, and values to make good choices" (Khadaroo, 2010). Education is the key to protecting children.

Protecting children's online reputation is essential in today's digital world. Without the proper education, children do not understand how the choices they make today can affect them well into the future. How they use the Internet, social network sites and other online applications will likely have future consequences. Employers are researching potential employees on social networking sites to determine their character; often making it a requirement to accept a 'friend request' in order to review the less public material. The Reputation Group reports that more than 90% of employers use social media to evaluate applicants. John Millen, chief strategist of The Reputation Group stated, "Every day the news carries another story of college students ruining their online reputations with inappropriate comments, photos, and videos" (Millen, 2013, "Top 10 Tips for New College Grads", para. 2).

In his book, Judge Jacobs (2010) reviews several cases where students posted questionable material on websites, blogs, and other electronic media about their school, their teachers, or other students. The schools disciplined the students upon discovering this material. In turn, these students sued the school districts believing the schools violated their First Amendment rights of free speech. Many of the students won their cases because the courts agreed that the schools did violate their First Amendment rights. While the First Amendment does protect free speech, and a student may be simply exercising his or her right to post online, a prospective employer or college admissions staff may not consider certain content favorably later

in life. Children must be educated that what they post online may exist forever and can affect their future.

Two cases in particular demonstrate how the lack of knowledge in online ethics affected children and schools. In 1999, Zachariah Paul emailed a top ten list he wrote about his high school athletic director to his friends. In his mind, the list was a joke poking fun at the director's weight and career. However, school officials found the email and suspended Zach. Zach sued the school claiming it was a violation of his First Amendment right of free speech (Jacobs, 2010). Another example involves Nick Emmett who posted a webpage that he titled, "The Unofficial Kentlake High Home Page...Vote for who will be the next to die." He posted mock obituaries of students and teachers. The media noticed this webpage and labeled it a hit list. The school suspended Nick. Although the courts ruled in favor of the students in both cases, they still missed key school events. The incidents are now part of their public histories (Jacobs, 2010).

Children are naïve about protecting their personal information. It is up to adults to educate them about how to protect their personal information for many reasons such as being taken advantage of by sexual predators or others who prey on children. Sexual predators are lurking in the shadows of the Internet waiting for unsuspecting and uneducated children to disclose personal information. Online grooming techniques build a false sense of trust to a point that a child will reveal extremely intimate details of their personal lives. Predators use this information to lure the child into an inappropriate online relationship that can lead to an offline physical relationship or abduction. According to Ernie Allen (2012), National Center for Missing & Exploited Children (NCMEC) President and CEO, in the 13 years since their CyberTipline began; NCMEC has processed more than 1.26 million reports involving child pornography,

online enticement of children for sexual acts, child prostitution, and sex tourism involving children.

Identity theft among children is rising as well. Identity theft among minors rose from about 6,000 in 2003 to more than 19,000 in 2011 (Murray, 2012). Children make excellent targets for identity theft because they typically do not have bills or accounts in their names (Murray, 2012). Therefore, no one is monitoring a child's credit report. Fraudulent activity can go unnoticed for many years as thieves apply for and use credit under a child's clean social security number. According to Jamie May (2012), Chief Investigator at AllClear ID, credit bureaus only verify whether a Social Security Number is a valid number when using it for the first time to open an account. They do not confirm that the name and birth date match the person opening the account. A study done by AllClear ID found that the rate of identity theft is 35 times higher for children than adults; 15% of victims were five-years-old and younger, and 26% of victims were six to ten-years-old (May, 2012).

In her report, May (2012) reports on several cases of child identity theft. In one case, a girl named Olivia was 19 when she applied for a credit card before going to college. The bank notified her that they denied her application because the social security number she used did not belong to her. Further investigation showed that someone stole her social security number when she was 9-years-old. In the 10 years of its fraudulent use, someone opened over 40 accounts totaling over 1.5 million dollars (May, 2012, p. 2). In another case, a thief stole the identity of a one-year-old, using it for two years to open five accounts totaling over 4,000 dollars (May, 2012, p. 15). A third case involved a criminal stealing the identity of 19-year-old Lindsey, many years earlier. The thief used Lindsey's identity for employment. Lindsey discovered this when she applied for an internship job during college. Lindsey was classified as unemployable because she

did not have her own social security number. She spent months trying to clear up the situation; however, the internship was no longer available. Another applicant accepted the position during the process (May, 2012, p. 12).

Literature Review

According to Davina Pruitt-Mentle, Ph.D, Executive Director of Educational Technology, Policy, Research, and Outreach (ETPRO), "Improving student knowledge and awareness of Cyberethics, Cybersafety, and Cybersecurity (C3) concepts will provide them with the means to protect themselves, and will enhance the safety and security of our national infrastructure" (p. 14). Children face many dangers when going online; sexting, cyberbullying, online gaming, terrorist radicalization, damaging online reputations, and identity theft are a few of these dangers.

Pruitt-Mentle (2008) defines each element of C3 awareness in her study. Cyberethics is the discipline that deals with moral duty and obligation pertaining to online environments and digital media. Cybersafety is protecting personal information and reputations from a behavior standpoint instead of hardware or software based protection. It is the ability to use the Internet and other online environments in a safe and responsible manner. Cybersecurity is the physical protection of personal information and technology resources from unauthorized access using both hardware and software. Raising children with C3 awareness is as vital to this country's future as teaching the use of technology (Pruitt-Mentle, 2008).

Sexting

Teens regularly participate in sexting causing the National Society for the Prevention of Cruelty to Children (NSPCC), a child safety charity, to warn of an e-safety 'timebomb' (Young people face online safety 'timebomb', 2013). Pew Research Center defines sexting as "the

creating, sharing, and forwarding of sexually suggestive nude or nearly nude images by minor teens" (Lenhart, Teens and Sexting, 2009, p. 3). One in five teenagers has participated in sexting in some form (Herman, 2010). Just over two-thirds sent images to their significant others, expecting them to remain private (Herman, 2010). A study conducted by Plymouth University revealed that 80% of respondents aged 16-24 used smart phones or the web for sexual purposes (Teitel, 2012). According to the NSPCC, "The issue of e-safety is no longer a topic that can be left to chance and is something parents struggle to keep up with" (Young people face online safety 'timebomb', 2013, para. 8). Also according to the NSPCC, abuse via the Internet and cell phones is currently one of the biggest child protection issues (Young people face online safety 'timebomb', 2013).

The number of 12-year-old children owning cell phones rose from 18% in 2004 to 58% in 2009 (Lenhart, Teens and Sexting, 2009). However, teens are not only talking on cell phones; they are texting, accessing the Internet, and sharing photos and videos (Lenhart, Teens and Sexting, 2009). The National Campaign to Support Teen and Unplanned Pregnancy conducted a nationwide survey of 1,280 respondents revealing that nearly 20% of teens admitted to participating in sexting. Another survey suggested 22% of the 13-19 year old girls surveyed admitted they had sent nude or semi-nude photos or videos (Spencer, 2010). Spencer concluded that teens do not seem to recognize the dangers of sexting, and they need to be educated that sexting can result in emotional damage and damage to their reputations, both now and in the future (Spencer, 2010). "Sexting in the moment lasts forever," writes Spencer (Spencer, 2010, "Safe-sexting?", para. 4). Amanda Todd learned that a posted photo exists in cyberspace forever.

Michael Friscolanti (2012) tells Amanda Todd's story in an article for Maclean's news magazine. Amanda used her webcam to go online with friends. Eventually, an online predator

started grooming her by calling her stunning, beautiful, perfect, etc. The predator finally convinced Amanda to lift her shirt when she was in 7th grade (Friscolanti, 2012). The predator wanted more videos and tracked her down on Facebook a year later. He threatened to expose Amanda if she did not comply. Amanda refused. Shortly thereafter, the police were at her door. The predator followed through with his threat. According to Amanda, he sent the picture to everyone. Devastated by this, Amanda turned to drugs and alcohol. Her friends not only abandoned her, but they also started bullying her. She tried to kill herself several times by drinking bleach and taking pills. Amanda wrote, "Every day I think why am I still here… I have nobody. I need someone" (Friscolanti, 2012, para. 5).

In 2012, Amanda posted an eight-minute video online in which she described her ordeal written on a series of flashcards. Amanda wrote, "I can never get that photo back.… It's out there forever" (Friscolanti, 2012, para. 4). Amanda's mother told a Vancouver radio station, "She was really sad and didn't like how she felt. It overwhelmed her" (Friscolanti, 2012, para. 8). A month after posting this video, Amanda committed suicide. In another case, Spencer (2010) reports of a 13-year-old named Hope Witsell who also sexted topless photos of herself to a boy in an effort to win his approval. The photos were forwarded to students in three schools. Spencer also explains that in most cases, sexting results in cyberbullying as the recipient violates the sender's trust by sending the images to a larger audience (Spencer, 2010). For Hope, the cyberbullying led to her committing suicide (Spencer, 2010).

Sexting is common among teens to some extent; however, most do not realize that it is a crime (Herman, 2010). For example, in Illinois, sexting that involves minors as the subject is possibly a felony under the Illinois Child Pornography Act (Herman, 2010). The Act made no distinction for taking pictures of oneself at the time of Herman's article (Herman, 2010).

Therefore, any minors taking a picture of themselves have technically created child pornography, which is a Class 1 felony. In addition, soliciting a minor to take such a picture or video could result in a charge of "indecent solicitation of a child" which is a Class 4 felony (Herman, 2010). Forwarding sext messages of a person known to be a minor may also be committing a child pornography offense.

Laws concerning sex offenses have not kept up with technology, therefore, do not consider the ability and ease of teens to send such images (Herman, 2010). In an article appearing in Principal Leadership, Aldridge, Davies, and Arndt wrote, "The laws applied in sexting cases are evolving, but currently most are related to child pornography and were not written for sexting situations" (Aldridge, Davies, & Andt, 2013, p. 14). States are starting to charge teens with manufacturing, possession, and distribution of child pornography because the subjects are under 18 years of age. It does not matter if the pictures are of themselves or others; taking a nude or sexually suggestive picture of anyone under 18 and sharing it is distributing child pornography, which can be a felony (Spencer, 2010). In Illinois, for example, if a person under the age of 18 creates, sends, or receives a 'sext' message, he or she may have committed the criminal offense of child pornography (Herman, 2010). Many states are reviewing their existing child pornography laws to incorporate sexting (Herman, 2010).

Herman (2010) points out school administrators should be aware of the legal aspects regarding sexting and child pornography investigations. School personnel may be subject to the same criminal offenses that the teens face if they mishandle the investigation (Herman, 2010). The Illinois Child Pornography Act, allows only "law enforcement or prosecuting officers" to possess offending materials as part of the "performance of [their] official duties" (Herman, 2010, p. 194). School administrators have no protections when investigating sexting incidents among

students and must exercise extraordinary care when handling this type of material (Herman, 2010). Even school administrators are subject to charges of possessing child pornography if they are not careful (Herman, 2010).

Many states have laws similar to the Illinois Child Pornography Act. In 2009, CBS News reported that three teenage girls in a Pennsylvania school allegedly sent nude or semi-nude photos of themselves to three male classmates. Pennsylvania authorities charged all six of them with child pornography (Spencer, 2010). According to Elizabeth Eraker, at least ten states have publicly taken a stand on sexting by either contemplating or following through with child pornography charges (Eraker, 2010). Parry Aftab, founder and director of WiredSafety, says that the solution should include teen educators since teens do not listen to adults when it comes to regulating their behavior (Zetter, 2009). Herman (2010) states, "The school district should educate students and parents about sexting and school policies related to the behavior" (p. 217). Many districts consider sexting as a form of bullying (Aldridge, Davies, & Andt, 2013).

Cyberbullying

Online teenagers using cruel antics on social media are replacing the traditional playground bullies of the past (Spencer, 2010). Cyberbullying began as the use of computers, smart phones, and Internet among young people increased (Klomek, Sourander, & Gould, 2010). As the technology of bullying has advanced, the efforts to prevent it have failed to keep up (Cloud, 2010). The Pew Research Center conducted a study of 802 teens ages 12-17 and found that 78% of teens have cell phones; 37% of teens have smart phones increasing from 23% in 2011 (Madden, Lenhart, Duggan, & Gasser, 2013). The study also revealed that 23% of teens own a tablet computer and 93% either have their own computer or access to one at home

(Madden, Lenhart, Duggan, & Gasser, 2013). Teens are not the only bullies using the Internet to harass children. Adults have participated in cyberbullying as well.

Two cases in particular illustrate adults participating in cyberbullying against teens. The first case involves Lori Drew, a mother of a 13-year-old girl. In 2008, Drew created a fake MySpace account to find out whether Megan Meier was spreading rumors about her daughter. Lori befriended Megan, pretending to be a teen boy interested in her, drawing her into an online relationship. Lori then turned on Megan and started taunting her. The harassment drove Megan to hang herself (Spencer, 2010). Although bullying is not new, cyberbullying is unique compared to traditional forms of bullying because the bully can remain anonymous and harass their target endlessly from anywhere (Klomek, Sourander, & Gould, 2010). In another case, Amanda Todd's constant tormenting from Facebook members after an adult posted her online photos drove Amanda into a severe depression. Amanda finally succeeded in taking her own life after "social-media tormentors dared her to take her own life, and rejoiced in cyberspace when she eventually did" (Teitel, 2012, para. 1).

Hinduja and Patchin conducted a study in 2010 in which they determined that traditional bullying and cyberbullying related to suicidal ideation in similar ways (Hinduja & Patchin, Bullying, Cyberbullying, and Suicide, 2010). Bullied children exhibit poor social and emotional adjustment, have greater difficulty making friends, and have poor relationships with classmates along with greater feelings of loneliness (Nansel, et al., 2001). According to Klomek, Sourander, and Gould (2010) cyberbullying has a significant association with depression and suicidal thoughts among girls and severe cases of cyberbullying have led to teenage suicide.

In 2010, Klomek, Sourander, and Gould (2010) reviewed research for the previous 20 years that addressed the relationship of suicide and bullying from childhood to young adulthood.

Their review of the cross-sectional studies found that victims of bullying show higher levels of suicidal thoughts than non-victims. In addition, they found that bullies have increased suicidal thoughts as compared to those not involved in bullying. "Suicidal ideation and suicide attempts are significantly associated with victimization and with bullying others both in and away from school" (Klomek, Sourander, & Gould, 2010, p. 283). Klomek, Sourander, & Gould (2010) found these behaviors in elementary, middle, and high school students.

While many people consider cyberbullying as a growing concern, others believe that it is no different from previous bullying activity. The Huffington Post ran an article in 2011 where Larry Magid, co-director of ConnectSafely.org and founder of SafeKids.com, argued that although cyberbullying is a serious problem, it is not an epidemic (Magid, 2011). Magid admits it is probably one of the more common risks involving youth on the Internet but then goes on to say that, bullying and suicide have always been a problem among adolescents. Magid stated that while there have been a few known cases of cyberbullying that lead to suicide, there were likely other factors involved (Magid, 2011). However, Klomek, Sourander, & Gould (2010) found that school bullying is a significant risk factor for suicidal tendencies, independent of other suicide risk factors. The Cyberbullying Research Center's data indicates that one in five teens experienced cyberbullying at least once in their life, and 10% in the last 30 days (Magid, 2011).

Most of the 50 United States have bullying laws. As of April 2013, Montana was the only state that did not have one (Hinduja & Patchin, State Cyberbullying Laws, 2013). Within the 49 states that have bullying laws

- 16 include cyberbullying;
- 47 include cyber harassment;
- 43 require school discipline; and

- 49 require a school policy (Hinduja & Patchin, State Cyberbullying Laws, 2013).

In 2011, parents of a tenth grader filed a lawsuit against a school claiming the principal, coach, and a teacher failed to stop the bullying of their child. The parents claimed that the school did nothing even after the parents told school officials about it (Poland, 2011). Poland strongly urges that school administrators take proactive steps to expand their knowledge and to implement bullying and suicide prevention programs (Poland, 2011).

Online Gaming Threats

Online gaming poses risks to children. Beyond online computer games, online gaming is also a standard feature among many of the gaming consoles today. Microsoft Xbox, Sony PlayStation, Nintendo DS provide the ability to link up with other players around the world. For example, Sony PlayStation offers a network allowing users to "meet up millions of PlayStation®Network members to play online multiplayer games" (Sony Computer Entertainment America LLC , 2013, "PlayStation Network games", para. 1).

Sexual predators target children in online gaming sites. A recent article in The Irish Sun reported that game consoles "were increasingly being used for grooming," according to a leading cyber security expert, Paul C. Dwyer (Meneely, 2013, para. 9). Meneely reports that strangers are targeting children as young as six on game consoles. Michelle Conway said that her three children were getting worrying invites on their Nintendo DS systems; one stranger even asking for one of her son's name and birth date (Meneely, 2013). Conway's seven-year-old son accepted a friend request from a stranger claiming to be a girl (Meneely, 2013). Meneely quotes Dwyer saying, "It's becoming quite common for predators to use game consoles… They try to make friends with the children. The more sinister predators try to groom children as they play games" (Meneely, 2013, para. 10-11). According to Meneely (2013), Dwyer compares gaming

systems to telephone or Internet because the children have no idea with whom they are communicating.

Gillian Shaw (2013) describes how predators target children in online gaming sites, in an article published in the Montreal Gazette titled, "Predators target kids through online games," on April 6, 2013. Predators target sites based on their interested age range. They pretend to be children, hoping to gain the trust and friendship of young gamers. Merlyn Horton, executive director of Safe Online Outreach Society said, "Parents might be shocked at the language, the abuse and the deceit that can occur in online games" (Shaw, 2013, para. 6). The CBC News reported in April that the Winnipeg police investigated seven cases of online predators luring children through gaming consoles; all but one involved suspected predators from the United States (Sawicka & Larsen, 2013). CBC reporter Gosia Sawicka accessed an online game called PlayStation Home. She registered as a 13-year-old girl and interacted with other players in the public areas. Within minutes, Sawicka reported, several people contacted her character asking sexually explicit questions (Sawicka & Larsen, 2013). This continued even after they found out that she was only 13.

Terrorists Recruit Children

Sexual predators are not the only people targeting children online. Terrorists use the Internet to organize, share information, recruit new members, and spread their beliefs (Besheer, 2007). According to Perry Aftab, an attorney who specializes in Internet issues that affect children, terrorists are recruiting bored, middle-class young people via the Internet (Besheer, 2007). Children who typically have no interest in radical groups, and would have never been exposed to these ideas, are seeing it as a way to feel included (Besheer, 2007).

Terrorists are using online games to plot, plan, and train for attacks (Willetts & Wells, 2012). Games called "first person" fighting games like "Call of Duty," "Medal of Honor," and "Halo" provide protection for terrorists because they hide their real discussions as innocent web chat pertaining to the game (Willetts & Wells, 2012). These online games allow players to sign into a "lobby" using a password. Once in there, they can play against each other, chat in private, and train radicals (Willetts & Wells, 2012). By nature, violent games make it almost impossible to detect dangerous conversations (PTI, 2011). According to GovernanceNow.com, these games are a serious threat because they can hide real conversations during the game as normal game play conversation, escaping security technologies designed to intercept and monitor communication (PTI, 2011).

Some terrorist groups target youth by offering free online games designed for radicalization and training. One media outlet of Al Qaeda released a game called "Quest for Bush" where players can use weapons to hunt and kill President Bush (Weimann, 2008). Another online game called "Special Force" allows players to become warriors in a terrorist attack against Israel (Weimann, 2008). This game includes a training mode where players practice shooting skills on Israeli leaders (Weimann, 2008).

Terrorists are using online media to draw followers (Dodds, 2011). In 2011, the Associated Press reported that Al Qaeda planned to roll out Disney-like animated cartoons aimed at recruiting children that spread anti-Western propaganda (Dodds, 2011). Dodds states that the short film shows young boys "dressed in battle fatigues and participating in raids, killings, and terror plots. It is the latest attempt by the terror organization to use multimedia to draw in potential recruits" (Dodds, 2011, para. 2). Senator Joe Lieberman stated, "Al Qaeda or allied violent Islamic organizations manage a multi-tiered online media operation consisting of several

production units to create content with the core message used to recruit and train terrorists" (Starr, 2008, para. 13). This provides a mechanism for people with access to a computer to connect with and gain access to expertise that was previously only available in overseas training camps (Starr, 2008). Starr quoted Senator Susan Collins, "What makes it so troubling is we don't know how many people are being radicalized because it's very difficult to track" (Starr, 2008, para. 6).

Two specific terrorist incidents leading back to the writings of an American citizen, Anwar al-Awlaki, who became a senior operative in Al Qaeda. In the first example, Dodds (2011) describes how the U.S.-born Yemen cleric used video sermons about foreign policy and poor job prospects for young Muslims to gain a following of English speakers in the United States and Britain. Roshonara Choudhry admitted to listening to 100 hours of Anwar al-Awlaki's online lectures before stabbing a British lawmaker in 2010. The second and most recent event occurred in Boston when Dzhokhar Tsarnaev and his brother set off several bombs at the Boston Marathon finish line in 2013. According to an article in the Boston Globe, Tsarnaev was a sophomore at the University of Massachusetts Dartmouth and described by friends as a normal city kid who did not talk about politics (Coffey, Wen, & Carroll, 2013). The indictment against Tsarnaev alleges that he was inspired by Al Qaeda publications and that he downloaded several pieces of extremist Islamic propaganda from the Internet, including one from Anwar al-Awlaki (Abel, Finucane, & Ellement, 2013). In a note he left while hiding in a boat, he justified his actions because of the US military action in Muslim countries. The indictment reveals some of the words that Tsarnaev allegedly wrote, "The U.S. Government is killing our innocent civilians.... I can't stand to see such evil go unpunished" (Abel, Finucane, & Ellement, 2013, para. 4).

Online Reputation

The First Amendment protects the speech of United Sates citizens. Courts have struggled to define the extent at which to protect speech since the adoption of the Bill of Rights (Farlex, INC., 2013). Justice Hugo Black believed that freedom of speech is absolute, yet Justice Oliver Wendel Holms, Jr. felt that the Constitution allows some restrictions on speech under certain circumstances (Farlex, INC., 2013). For example, Holmes wrote the words that many people are familiar with today when speaking of free speech; a person cannot shout "fire" in a crowded theater when there is no fire. (Farlex, INC., 2013). In this case, shouting "fire" would not be protected speech under the Constitution (Farlex, INC., 2013). Speech that has a substantial disruption in school activities also may be restricted (Wheeler, 2011).

Thomas Wheeler, a member of the National School Boards Association, Board of Directors and Chairman of the Council of School Attorneys, wrote an article in the Pace Law Review where he stated, "any examination of student free speech rights must necessarily start with the seminal Supreme Court case of Tinker v. Des Moines Independent Community School District" (Wheeler, 2011, p. 185). The school system banned students from wearing black armbands to school in protest of the Vietnam War (Wheeler, 2011). The students claimed this violated their First Amendment rights (Wheeler, 2011). The Supreme Court agreed and overturned the ban (Wheeler, 2011). This decision resulted in a two-pronged test used to determine whether the First Amendment protects certain speech. The first prong determines whether the First Amendment protects the speech in question (Wheeler, 2011). The second prong determines whether a school can restrict the protected speech based on a "sufficiently compelling interest" (Wheeler, 2011, p. 186). The court's decision has become known as the Tinker standard for school censorship of student expression (Jacobs, 2010). According to Jacobs (2010), "Public

school officials must tolerate student speech as long as it does not materially or substantially disrupt the educational environment or invade the rights of others to be secure" (pp. 11-12). However, Jacobs (2010) also states, "You can't post a threat online about hurting your teachers or classmates without facing examination, and, possibly, serious consequences" (p. 8). A person cannot just say anything they want to about anyone with no consequences (Jacobs, 2010).

Judge Jacobs (2010) discusses some First Amendment cases involving students and their schools. In one case, Justin Swindler published a website called "Teacher Sux" while in 8th grade. The site contained degrading and personal attacks against his algebra teacher, along with her face morphing into Adolph Hitler. He posted the phrases "Why she should die" and "Take a look at the diagram and the reasons I gave, then give me $20 to help pay for the hit man." Another picture showed her with head cut off and bleeding from her neck. He also posted, "We all wish this would happen" along with the picture. The teacher was unable to complete the semester and took a medical leave for the next year because she was afraid someone would try to kill her. Justin also posted sexual comments and personal attacks about his principal. The school board permanently expelled Justin for the threats against the teacher and principal.

Justin and his parents appealed the decision claiming that the website did not contain a legitimate threat to anyone and there was not a sufficient disruption at school. The court concluded that even though the speech was vulgar and highly offensive, it did not constitute a real threat. The court did not believe that the site reflected a "serious expression of intent" to inflict harm. However, they did conclude that this site was disruptive to school because the teacher was unable to continue teaching, forcing the school to hire substitute teachers. Therefore, the court denied Justin's First Amendment claim and upheld the expulsion. The teacher and principal sued Justin and his parents for violating their civil rights. A jury awarded the teacher

and her husband $500,000 in damages and the principal settled his case for an undisclosed amount.

Another case highlighted in Jacobs' (2010) book involves Zachariah Paul. Zach wrote a top ten list about his high school athletic director. The list criticized the director and his weight. In a previous incident, Zach described the school librarian as a "book Nazi" and suggested others to request books about making bombs. The school suspended Zach for 10 days and gave him five Saturday morning detentions. Zach could not participate in any school activities during his suspension, including track and field events. Zach and his mother claimed that the school violated Zach's First Amendment rights and sued the school for immediate reinstatement in school. Jacobs (2010) quoted Zach saying, "What I say in my own home is my business" (p. 36). The court overturned the school's decision to suspend Zach because they found no evidence of actual disruption at school. As a result, the school district had to pay Zach and his family $65,000. Although some people may have found Zach's list to be rude, his speech against the director was not threatening, therefore, protected under the First Amendment (Jacobs, 2010).

A third case in Jacobs' (2010) book, Nick Emmett created a website he called, "The Unofficial Kentlake High Home Page," where he posted fake obituaries of his friends created during an assignment in a creative writing class. He requested viewers to vote for "who would die next" referring to whose fake death notice he would post next. Nick included a disclaimer that his site was for entertainment purposes only and not sponsored or endorsed by the school. Regardless, a television news story incorrectly characterized it as a "hit list." Nick removed the site from the Internet that night. However, the school suspended Nick causing him to miss a basketball playoff game. Nick was the co-captain of the basketball team, had a 3.95 GPA, and no prior disciplinary record at school.

The court found that the First Amendment did protect Nick's speech referring to the Tinker case and others. They determined that Nick's writings were not threatening to anyone and did not pose any real threats. The court found in favor of Nick and ordered the school to lift the suspension. In addition, the school agreed to pay Nick's legal fees of $6,000. Jacobs (2010) concludes, "Even something written tongue-in-cheek can backfire…. What began as a humorous project went seriously astray" (p. 111). Nick won his case but still suffered irrecoverable consequences.

In yet another case from Jacobs' book, Katie Evans was an honor student in her senior year of high school with no prior disciplinary record. She used her Facebook page to express her discontentment with her English teacher, Sarah Phelps. Katie posted a comment stating Phelps was the worst teacher that she had ever met. She encouraged other students to post their feelings of hatred towards this teacher. Katie downloaded a photo of the teacher from the school's website and posted that, as well. Eventually, the school principal found out, suspended Katie for three days for cyberbullying and harassing the teacher, and pulled her from her Advanced Placement classes. She filed a lawsuit to have all mention of the suspension removed from her record because the label of cyberbully in her official school record concerned her. The courted ruled in Katie's favor stating that her Facebook page is off-campus speech and protected. The court specified in its ruling that under any form of the Tinker test, her speech "cannot be construed as even remotely disruptive, nor was her speech in any way lewd, vulgar, defamatory, promoting drug use or violence as seen in other cases" (KATHERINE EVANS, Plaintiff, v. PETER BAYER, in his individual capacity, De-fendant., 2010). It was Katie's concern that this event would affect her graduate school and job applications that prompted her to file the lawsuit (Jacobs, 2010).

Controversy continues as to whether employers and colleges should access social network sites to screen candidates (Marklein, 2011). Kenyon College forbids this practice; considering it similar to wire-tapping phones and reading diaries (Marklein, 2011). However, Paul Marthers, vice president for enrollment at Rensselaer Polytechnic Institute, said this information is "fair game" (Marklein, 2011, para. 8). Jacobs (2010) asks his readers to consider whether a student winning a free speech claim means that they won from an ethical standpoint. He goes on to say, "You have the right to criticize others, but refrain from hateful attacks and falsehoods" (Jacobs, 2010, p. 74). Jacobs (2010) stated, "Causing emotional distress to a person or harming a reputation are acts that carry real consequences-no matter what the court rules" (p. 42). In 2008, a survey of 300 top colleges revealed that 10% of admissions officers use social networking sites to evaluate applicants and 38% said that what they saw negatively affected their views of applicants (Jacobs, 2010). In 2011, a new survey of 359 colleges found that 24% used Facebook and 20% used Google for evaluation applicants (Marklein, 2011). College recruiters are using social media sites, like Facebook, to see their digital personalities (Marklein, 2011).

Education Week published an article by Caralee Adams written in February 2013 about character education in schools. Adams (2013) describes character education simply as teaching children about how people treat each other. According to Adams (2013), many school administrators are realizing the benefits of character education, whereas they used to think of it as a distraction. Scott Seider, an assistant professor of education at Boston University said, "Concern over sexting, bullying, and the need to get students college-ready are also factors for the increased interest" (Adams, 2013, "Signs of a Renaissance", para. 5). According to Marvin Berkowitz, schools that teach character education are promoting respect, responsibility, caring,

fairness, and honesty (Adams, 2013). Berkowitz goes on to say, "More intense academics" sometimes replaces character education in secondary levels (Adams, 2013, para. 5).

Identity Theft

Children are targets for identity theft. AllClear ID published a Child Identity Theft Report in 2012 stating that children are 35 times more likely to be targeted in identity theft than adults (May, 2012). According to May (2012), younger children are better targets for identity theft because thieves have a longer time to use the information undetected. Parents usually apply for social security numbers for newborns while in the hospital, yet the child typically will not use it for 18 years. This leaves 18 years for a thief to use this identity undetected (May, 2012).

In her report, May (2012) describes how a thief can build a credit history using a stolen social security number. Thieves know that credit bureaus and lenders do not validate all of the details of new credit applications when a credit file does not already exist. Therefore, the thief tries to open accounts with the lowest credit history requirements, such as cell phones, utilities, or unsecured credit cards using the stolen number with a different name to create a credit history. The only validation is whether the number is a valid and that it does not belong to a deceased person.

Identity thieves have many ways to steal a child's information. They use viruses specifically designed to search computers for documents that typically include social security numbers of children including tax, health care, and school related documents (May, 2012). Email phishing can entice people into providing the child's personal information (May, 2012). Data breaches also provide access to social security numbers (May, 2012).

In 2012, Nicole Vincent (2012), Consumer Education Specialist for the FTC, reported the social network site RockYou suffered a security breach that exposed the personal information of

over 100,000 children. Over a two-year period, RockYou collected personal information from around 179,000 children under 13 in violation of the Children's Online Privacy Protection Act (COPPA) (Vincent, 2012). The website required users to provide a valid email address and password for that email address as well as their birth year, gender, country and zip code in order to save content (Vincent, 2012). RockYou stored passwords in clear text and failed to protect the data against common data breach attacks (Vincent, 2012).

A study conducted by AllClear ID's scanning various databases of existing accounts using data from 27,000 American children found nearly 3,000 cases of child identity theft (May, 2012). The number of identity thefts of children under age five nearly doubled to 426 cases, an increase of 105% compared to 2011 (May, 2012). The number of cases involving children between six and ten was 759, representing an increase of 34% since 2011 (May, 2012). Children between 11 and 14 represented a 1% increase since 2011 at 843 cases, and ages 15-18 fell 33% to 848 cases. Their research also found 6,273 cases in which a child's social security number appeared in credit bureau records, 2,352 found in utility service records, 1,459 found in property related records, 214 in driver license records, and 345 in vehicle registration records (May, 2012).

May (2012) describes several identity theft cases involving children. Hanna was 2 years old when someone stole her social security number. Multiple people used her social security number to establish two mortgages and an installment account (May, 2012). Over the 14 years, they had established over $170,000 of credit and over $82,000 of debt (May, 2012). In another case, Brianna, an 11-year-old victim had a mortgage, car loan and nine credit cards (May, 2012). Someone stole her identity when she was six years old. At the time AllClear discovered her case

there was a mortgage totaling $93,157, credit cards totaling $24,746 and an auto loan totaling $11,199. In addition, there were three installment accounts totaling $3,625.

Virginia Schools and Internet Safety Education

Virginia was the first state to mandate Internet safety lessons across all grades in public schools (Vargas, 2008). Maryland and the District of Columbia schools already had Internet safety education, but they did not mandate their programs nor were they spread across all grades (Vargas, 2008). Delegate William H. Fralin, Jr. introduced House Bill 58 (HB58), requiring acceptable use policies for schools "include a component on Internet safety for students that is integrated in a division's instructional program" (Virginia Department of Education, 2007, p. 2). The legislation passed in the 2006 General Assembly.

In 2007, the Virginia Department of Education (VDOE) published Guidelines and Resources for Internet Safety in Schools. The purpose was to provide a starting point as divisions add the required Internet safety components to their acceptable use policies and integrate it into their curricula (Virginia Department of Education, 2007). However, the document only offered recommendations, leaving the specific details to the discretion of the school systems (Virginia Department of Education, 2007). Billy Cannaday, Jr., Virginia's Superintendent of Public Instruction, stated in his Forward, "The Department will periodically disseminate additional information and resources, beginning with a fall 2006 document that demonstrates how Internet safety issues can be integrated with the Standards of Learning" (Virginia Department of Education, 2007, p. v). Cannaday goes on to say, "instructors need to be well informed about the latest computer threats and integrate Internet safety into their curricula throughout the school year. Administrators should keep staff and community members apprised of new developments" (p. v).

The VDOE provides issues that school divisions must address. Among the list are:

- Professional development opportunities for staff across the division and integration of Internet safety into the K-12 curriculum and instruction;
- The material for Internet safety education needs to be age appropriate and should start in kindergarten continuing through graduation with each year building on the previous year's lessons; and
- All instructors should teach Internet safety; modeling safe and appropriate Internet use and warning of potential danger as opportunities arise (Virginia Department of Education, 2007).

Students must learn how to use the Internet safely and effectively (Virginia Department of Education, 2007). They must understand that people are not always whom they say they are and should never give out personal information without an adult's permission (Virginia Department of Education, 2007). Students should know predators are always present on the Internet; recognize the various forms of cyberbullying and know what steps to take if confronted with that behavior (Virginia Department of Education, 2007). Finally, the VDOE (2007) states that students "students and their families should discuss acceptable social networking and communication methods" and "know the potential dangers of emailing, gaming, downloading files, and peer-to-peer computing (e.g., viruses, legal issues, harassment, sexual predators, identity theft)" (p. 5).

Nancy Willard (2012) states, the Protecting Children in the 21st Century Act requires that any school receiving E-rate or other technology funds must teach minors on appropriate online behaviors; including how to interact with others on social networking websites, in chat rooms, and teach them about cyberbullying awareness. Yet, the FCC did not specify how schools are to

provide this education. In their opinion, schools are better able to make these decisions themselves. Willard goes on to say, “Further, there is no stated requirement for schools to document that every student has received this safety instruction” (Willard, 2012, p. 86).

Lynchburg City Schools (LCS) published their Education Technology Plan for 2010 through 2012. In this plan, they describe how they will respond to the guidelines published by the VDOE. The plan covers three components: technology infrastructure, the use of educational technology in the area of instruction, and the professional development for all staff members in the use of technology (Lynchburg City Schools, 2011). LCS states, “Recently the focus has moved from teaching students how to use technology to relying on technology to support content. This is due much in part to the elimination of Standards of Learning testing in this area” (p. 33). Therefore, LCS no longer considers technology as an isolated topic but “part of a planned program of school change as it relates to student achievement” (Lynchburg City Schools, 2011, p. 33). In response to the VDOE's guidelines, LCS proposes their K-12 Internet safety instructional program in the appendices of their technology plan (Lynchburg City Schools, 2011).

The professional development component discusses different ways that LCS plans on providing or promoting technology training for teachers. LCS recognizes that most teachers are proficient in the basic uses of technology, but lack the time and support to develop and implement lessons that integrate technology (Lynchburg City Schools, 2011). LCS (2011) states, “the greatest needs facing teachers in the use of instructional technology are to become adept at both integrating technology into instruction and using purchased software to supplement their classroom instruction” (p. 45). LCS determined that student Standards of Learning (SOL) scores should increase as teachers become more effective in integrating technology into their

curriculum (Lynchburg City Schools, 2011). LCS concludes, “Teachers will be able to lead students through activities and lessons using technology to master SOL content material” (p. 45).

The LCS plan outlines some required training expectations. The Instructional Technology Specialists (ITS) will assist teachers who need to master technology by conducting sessions designed to teach them how to use technology (Lynchburg City Schools, 2011). The VDOE requires mastery of technology standards for initial and renewed teacher licenses (Lynchburg City Schools, 2011). LCS has a technology points program requiring all staff members to accumulate points as part of their professional development requirement. Employees must earn a minimum of six technology points each year by participating in workshops, ITS led technology sessions, and independent study. However, LCS states, “the ultimate goal is to improve academic achievement as measured by the SOL assessment process” (p. 47).

The technology used in LCS consists of local area networks (LAN) connecting all classrooms together as well as a wide area network (WAN) connecting all schools together (Lynchburg City Schools, 2011). Each classroom has at least one multimedia computer and printer with direct Internet access (Lynchburg City Schools, 2011). All schools have computer labs with access to the LAN, WAN and Internet. Each elementary school has at least two, each middle school has at least four, and both high schools have at least eight (Lynchburg City Schools, 2011).

The appendix of the LCS technology plan includes their acceptable use policy (AUP). Within this AUP, LCS confirms that they comply with the CIPA by filtering Internet content including pornographic material, access to non-educational spaces, private web-mail services and other content that LCS deems inappropriate (Lynchburg City Schools, 2011). The AUP specifies appropriate user behavior for personal safety, illegal/inappropriate activities, system security,

inappropriate behavior, respect for privacy, respect for resource limits, electronic communications, use of external devices, plagiarism, copyright infringement, software, access to material, and personal accounts (Lynchburg City Schools, 2011). There is more clarification including examples within each category.

The teacher responsibilities outlined in the technology plan call for teachers to provide students with a "sequential, structured approach to gaining the skills that will allow them to become independent, responsible users of technology" (p. 89). The plan states that teachers will make a reasonable effort to ensure that students access only information that is age and subject appropriate (Lynchburg City Schools, 2011). This includes supervising children while using the Internet and exploring Internet sites before directing students to them.

The LCS divides their Internet Safety Curriculum into three categories: K-5, middle school, and high school. The K-5 curriculum provides a lesson for each grade using animated videos and other activities from websites such as NetSmartz and Media Awareness Network (Lynchburg City Schools, 2011). The goal of the curriculum at this age level is to teach children that people they meet on the Internet may not be whom they claim to be, encourage them to talk about their encounters on the Internet with a trusted adult, teach about the dangers of the Internet and teach skills to avoid them (Lynchburg City Schools, 2011).

The middle school Internet Safety Program involves four units of study: cyber citizenship, cyber bullying, cyber safety, and cyber copyright (Lynchburg City Schools, 2011). This program intends to develop a concept of cyber community, good cyber citizenship, and educate students about legal and ethical behaviors when using information and technology (Lynchburg City Schools, 2011). Recognizing and avoiding dangerous, destructive, or unlawful online behavior, understanding the consequences of misusing technology, and understanding fair

use and copyright regulations are other objectives for the middle school students (Lynchburg City Schools, 2011).

High school students will learn about issues relating to personal privacy and social use of the Internet, intellectual property, identity theft, cyber-citizenship, and cyber harassment (Lynchburg City Schools, 2011). Specific subjects mentioned within their curriculum are plagiarism, copyright, public domain, steganography, computer hacking and cyber terrorism (Lynchburg City Schools, 2011).

Roanoke County School District describes the use of technology in their comprehensive plan. Like most schools today, Roanoke County uses technology to assist teachers to plan and deliver lessons (Roanoke County Schools Board, 2010). However, Roanoke County also implemented a virtual high school program that allows students to take courses online instead of attending in person, and all high school students receive laptops (Roanoke County Schools Board, 2010).

Roanoke County has subtle mention of Internet safety within its comprehensive plan. Instructional Technology Resource Teachers (ITRT) will train all staff and work with classroom teachers to ensure they provide Internet safety training to students (Roanoke County Schools Board, 2010). The ITRT staff is responsible for building the Internet safety curriculum and updating it as needed (Roanoke County Schools Board, 2010). In addition to the comprehensive plan, Roanoke County provides sample lesson plans for middle school children that suggest ways to incorporate Internet safety into the curriculum. The sample plans identify ethics, Internet community, cyber-citizenship, cyberbullying, creating a safe persona, and intellectual property topics weaved into the standard courses of math, science, history and English (Roanoke County Public Schools, 2009).

Bedford County Schools (BCS) briefly mentions Internet Safety in its Technology Plan. However, there is no detail about the training provided. The BCS Technology Plan lists objective 2.3 as, "Facilitate the implementation of high-quality Internet safety programs in schools" (Bedford County Public Schools, 2011, p. 9). Under this objective, BCS (2011) will:

- Strategy 2.3.1: Research and identify best practices and provide resources to promote the integration of Internet Safety throughout curricula.
- Strategy 2.3.2: Provide resources and support for faculty, staff, students, and parents to assist in promoting Internet Safety.
- Strategy 2.3.3: Develop virtual professional development for school personnel in Internet safety and security training. (p. 9)

These objectives call for an Internet Safety Committee to examine the national trends relating to Internet Safety and distribute the information. Under Strategy 2.3.3, there is intent to develop an online "Teacher Training Academy" to aid teachers on integrating new technologies into their curriculum as they relate to Internet safety and security (Bedford County Public Schools, 2011).

Campbell County Schools (CCS) addresses Internet safety in their Educational Technology Plan 2011-2017 document. According to CCS's plan, students must develop technology skills from kindergarten through the twelfth grade (Campbell County Schools, 2013). CCS does recognize the need to keep students safe on the Internet while using this technology (Campbell County Schools, 2013). Media specialists teach Internet safety and school counselors discuss cyberbullying issues with students (Campbell County Schools, 2013). The CCS staff also recognized that they share this burden with the community, so they provide Internet safety information to parents using videos, presentations, and newsletter articles.

Roanoke City Public Schools does not address Internet safety in their published Strategic Plan document for 2009-2014. Its plan mentions school safety in terms of physical safety and the learning environment (Roanoke City Public Schools, 2009). The Roanoke City plan also recognizes that technology connects students to the community (Roanoke City Public Schools, 2009). However, Internet safety and the use of technology are not included in the plan.

The latest Richmond Public Schools (RPS) technology plan also does not address Internet safety education. The RPS plan mentions using technology to aid teachers in their instruction, curriculum and technology integration, and student assessments; however there is no mention of teaching children how to use technology safely (Richmond Public Schools, 2010a). The RPS website does have an Internet Safety page. Here, RPS mentions that Internet safety is about balancing the protection of students with the need to use technology to its full potential. However, they follow this statement with, "Since it is not preferable that we institute policies that completely restrict students and teachers in regards to the content of their websites, we nevertheless must attempt to put certain guidelines in place" (Richmond Public Schools, 2010b, para. 1). The RPS (2010b) Internet Safety page does state that employees need to be vigilant in helping students make informed decisions when using the Internet. It also states that teachers must incorporate Internet safety into their curriculum on a regular basis. The website also contains many links to other Internet safety websites.

Challenges Facing Schools

Several factors may prevent schools from offering the level of education needed to address the dangers children face online. According Pruitt-Mentle, data indicates that while states and local education agencies place the responsibility of C3 training on teachers, it is not necessarily happening (Pruitt-Mentle, 2008). Key findings from a study conducted by ETPRO in

2008, revealed that C3 education material is scarce, content marginally discusses the issues, and teachers do not feel comfortable with the topics (Pruitt-Mentle, 2008). Many responded that they believe parents should provide C3 education; it should not be the teacher's responsibility (Pruitt-Mentle, 2008). However, Michelle Dennedy of the online security company McAfee said, "Many parents are overwhelmed by the onslaught of technology available to their children and feel like they can't keep up with their tech-savvy children" (Palmer, 2013, para. 8). According to Palmer (2013), McAfee polled 1,301 parents in April 2013 and found that 80% of those with preteen children claim they do not have the time or energy to monitor their child's online activity; and only 9% know how to how to do so.

A poll conducted in December 2009 and January 2010 by the National Cyber Security Alliance (NCSA), Microsoft, and ETPRO surveyed 1,003 teachers. The poll found that only about one-third of the teachers said their districts required teaching C3 topics (Butler, 2010). School districts often rely on prevention by limiting access, preventing downloads and allowing only specific site access instead of proactive promotion of C3 concepts (Pruitt-Mentle, 2008). Michael Kaiser, NCSA executive director, stated that even though administrators and teachers think it is important to teach Internet safety, it does not translate into classroom education (Butler, 2010).

More than half of the respondents in a 2008 C3 education survey did not know how their schools teach students on C3 issues (Pruitt-Mentle, 2008). Some educators do not feel qualified to teach about cyber security. According to Stay Safe Online, only 10% of educators received more than six hours of professional development on cyber security, only 22% are comfortable teaching about cybercrimes, and only 23% feel prepared to teach students how to protect their personal information online (National Cyber Security Alliance, 2013). Most educators

responding to the survey indicated a lack of confidence and admitted to a limited understanding about most C3 topics (Pruitt-Mentle, 2008). In a poll conducted by the NCSA et al., only 56% of the 1,003 teachers felt that their districts did a reasonable job preparing them to discuss C3 topics with students (Butler, 2010).

Financial and time constraints are additional factors making it difficult for schools to respond appropriately (Pruitt-Mentle, 2008). Claude Almansi published an interview she conducted with Nancy Willard for Educational Technology and Change Journal. Willard stated, "The biggest obstacle right now is that the financial situation of schools is so bad that it is challenging for them to think about adding anything new" (Almansi, 2011, para. 35). Regarding time, national, state, and local standards and assessment place high demands on today's education community (Pruitt-Mentle, 2008). According to Pruitt-Mentle, "The school day is busy, and teachers are reluctant to include topics not specifically mandated or assessed" (p. 3).

Discussion of Findings

The Internet can be an excellent resource for children if used wisely, and it can be a dangerous minefield for children who do not know the risks. Children need to protect themselves while online in their virtual world just as they need to protect themselves when offline in the physical world. Their personal information, reputations, and lives are at stake. Children lack the proper knowledge on how to protect themselves from those looking to take advantage of them. They need the help of trained educators to prepare them for what they will face when exploring their virtual world. Similar to a minefield where every step is perilous, interacting with the Internet is a virtual minefield where every click could be a dangerous step.

The Internet, in and of itself, is not an evil playground; not every place a child visits will be dangerous. However, if children are not trained to recognize danger, they will not know how

to avoid it. Children learn at an early age not to talk to strangers. However, many times children explore the Internet alone and end up talking to strangers online. Many parents have a false sense of security. The reality is they can be in more danger within their house as they surf the World Wide Web alone.

Threats to children come in many forms: identity theft, cyberbullying, online grooming, and abduction to name a few. Children can also jeopardize their future reputation if not careful how they use the Internet. Children can even become weapons used by terrorists against the United States. Equipping children, with knowledge and tools to protect themselves is essential to keeping them safe in the digital world. This education needs to start in kindergarten and continue through high school (Pruitt-Mentle, 2008). Linda Sharp, director of the Cyber Security for the Digital District program at the Consortium for School Networking (CoSN) states, "We need to start on Web usage education as soon as students are on the computer" (Butler, 2010, para. 6).

Public schools have an obligation to provide a safe online environment for students as well as provide education on the dangers of being online. The purpose of this research was to evaluate the Internet safety education for children in Virginia schools to determine if they are adequately preparing children for the online world. What are the dangers awaiting children when they go online? What are Virginia schools doing now to teach children about the dangers and the proper usage of the Internet? What are the challenges that prevent teachers and schools from delivering a comprehensive Internet safety education program?

Dangers in the Minefield

Dangers on the Internet go beyond the well-known child predator and abduction issues; identity theft, online reputations, and national security are at stake. This does not mean that child predator and abduction issues are not serious. They are real threats and deserve attention.

However, educating children on Internet safety can protect them from all of forms of online dangers.

The three tenants of Internet safety include cybersecurity, cybersafety, and cyberethics. These are referred to collectively as C3 education. This research identified cyberethics as a core education component that can help children avoid most dangers on the Internet. Cyberethics is the least known component and is becoming the most critical to teach. Treating others with respect in the virtual world is as essential as the physical world, if not more so. Keeping personal data and details of others confidential is essential for Internet safety.

Character education is essential for teaching children to respect themselves and others. Promoting respect, responsibility, caring, fairness, and honesty are the focus of character education. These traits are missing from youth today in how they behave online. Many schools have abandoned character education in secondary levels of education to focus on teaching the more intense academic courses. However, many school administrators now realize that character education is not a distraction in the school day, but a necessary subject having many benefits. Scott Seider, an assistant professor of education at Boston University said, "Concern over sexting, bullying, and the need to get students college-ready are also factors for the increased interest" (Adams, 2013, "Signs of a Renaissance", para. 5). Correcting these character issues would help solve most of the danger issues on the Internet today.

Sexting is gaining popularity among teens. Teens regularly participate in sexting thinking it is cool yet do not understand the dangers involved. Twenty percent of teenagers have participated in sexting in some form, and more than two-thirds sent images to significant others expecting them to remain private (Herman, 2010). However, once the relationship is over, if not

before, the pictures often get forwarded to others. Good character education and ethics would teach children that this behavior is destructive; it will never achieve the results that they seek.

Beyond the embarrassment and ridicule that follows a sexting exposure incident, all participants involved may face criminal charges. Sexting is a crime under the current law of most states. Many states make no distinction between minors taking their own picture and adults taking pictures of minors; anyone participating in sexting could face charges of creating, possessing, or distributing child pornography. Most teens are not aware that they could face Class 1 felony charges by participating in sexting. Anyone asking a minor for such material could result in a Class 4 felony charge of indecent solicitation of a child. The threat of criminal prosecution may not be enough to deter this trending behavior. Character education is necessary to redirect this trend in children who will eventually become adults.

Existing laws also do not account for the ease in which teens can create and distribute these photos. Prior to digital photos, it was much harder to create pictures than today because it required a photo lab to develop them. Digital pictures need no lab for processing pictures; therefore, have immediate results. Distributing the pictures is just as easy; sending the same photo to hundreds of people takes only seconds. Sexting often results in another very serious threat to children, cyberbullying.

Cyberbullying is gaining attention as an epidemic in schools. Online teenagers using cruel antics on social media are replacing the traditional playground bullies of the past (Spencer, 2010). Cyberbullying began to appear as the use of computers, smart phones, and Internet among young people increased (Klomek, Sourander, & Gould, 2010). More teens have access to the Internet than ever before. Their almost incessant Internet usage increases the capacity of a person to bully others, to become a victim of a bully, or both. Technology has not made the effects of

bullying worse; it has increased the ease and ability of bullies to operate while decreasing the ability for victims to escape.

The results of traditional bullying and cyberbullying are similar. Bullied children exhibit poor social and emotional adjustment, have greater difficulty making friends, and have poor relationships with classmates along with greater feelings of loneliness (Nansel, et al., 2001). According to Klomek, Sourander, and Gould (2010) cyberbullying has a significant association with depression and suicidal thoughts among girls; severe cases of cyberbullying have led to teenage suicide. Amanda Todd's life and death substantiates that claim.

Amanda Todd committed suicide as the result of cyberbullying following a sexting incident. Her friends abandoned her and started to abuse her on Facebook. Amanda was not able to escape the tormenting and turned to drugs and alcohol. She attempted suicide several times only to receive additional ridicule on Facebook because she was not successful in her attempts. She described her feelings in an eight-minute video posted on YouTube a month before she died describing her loneliness. After Amanda's death, her mother described her daughter's feelings as "really sad and overwhelmed" (Friscolanti, 2012).

Sexting and cyberbullying have real consequences; often they are deadly. Some argue that cyberbullying is not an epidemic; that bullying has always been around, and so has teen suicide. However, there should be no doubt that the Internet has intensified bullying in some respects. The Internet increased the audience and increased the access bullies have to their victims. Cyberbullying must be stopped; whether it leads to suicide or not, whether it is an epidemic or not. One child dying as the result of cruel and disrespectful behavior is one too many. Cyberethics and character education are critical elements in stopping cyberbullying.

School administrators who are not proactive in the prevention of cyberbullying could face disciplinary actions. Since most states have a cyberbullying law that affects schools, administrators must become familiar with these laws and their respective responsibilities to reduce risk for themselves and the school district when cyberbullying is reported. In 2011, parents of a bullied teen sued his school because the principal, a coach, and a teacher did not stop the bullying, even after the parents told school officials about it. Educating children on ethical issues is certainly a proactive approach to help eliminate cyberbullying. The risk is too high for all involved: the child, the staff, administrator, and the school system, to fail at offering this crucial educational component in the cyber world we live in today. One educator, administrator, or legislator who reads this body of research and takes action can save a child's life.

School administrators must avail themselves of the current laws affecting sexting and child pornography. There is no safe haven for anyone involved in this activity, and that includes school personnel. School officials must handle the evidence with extreme caution during an investigation or they risk facing various child pornography charges themselves. For example, in Illinois, the only people allowed to possess this material are law enforcement or prosecution officers and then, it is only within the boundaries of performing their official duties. Therefore, school administrators trying to handle a sexting incident on their own may be charged with possession and distribution of child pornography, if they do not immediately report it to the authorities.

Reputations of children are at risk now more than ever before. Children need guidance on how to protect their online reputations. The Internet provides a virtual soapbox for anyone to say anything. However, this does not mean that children should say whatever is on their mind just because it is legal to do so. The First Amendment does protect free speech in the United States;

however, there are still some restrictions. Justice Oliver Wendel Holmes felt that the Constitution allows some restrictions on speech under certain circumstances. For example, a person cannot shout "fire" in a crowded theater when there is no fire because it would cause panic and disruption. Similarly, language that has a substantial disruption in school activities also may be restricted.

Most courts apply the Tinker test to determine whether the First Amendment protects a student's speech. The Tinker test uses a two-prong evaluation. The first prong determines whether the First Amendment protects the language in question. The second prong determines whether there was substantial disruption in school activities. These two questions are relevant for two reasons. First, it allows a school to discipline a student when their speech causes a substantial disruption, even if the First Amendment protects it. Secondly, it allows the school to punish off-campus speech. This is an extremely vital aspect, especially in today's social media world. Students think that there are no legal consequences if they use their own computer, their own time, and are off school property. However, this is not true. Comments posted to Facebook, emails, and other off-campus speech that cause substantial disruption in school activities can result in disciplinary action.

Beyond legal issues, reputational damages often result. Comments and photos posted online may exist in cyberspace forever and will affect the future of a child. Typically, there is no evidence of verbal comments made in the heat of an argument, but electronic posts made in the same vein are permanent and non-retractable. Companies and colleges often review the behaviors of applicants on the Internet to ensure the integrity of their organizations. Social media sites allow them to find information much easier than in the past. People have no issue posting extremely personal details or stating opinions that others may find offensive; yet complain it is

unfair when people see this information and make a determination of their character. If people are going to post information publicly, there is a reasonable chance that an unintended person will see it. Children must understand that this is now a reality in a digital world. With colleges, employers, and other organizations utilizing social media and the Internet to research the online character of prospective students, employees, and club members, children must think about what they say and what they post online. Their futures depend on it. Cyberethics education will teach children to think before they post content.

Judge Jacobs (2010) covers many cases in his book where teens used poor judgment posting things that were of bad character. Some posts were vulgar; some were threatening, and some seemed like funny pranks with no perceived implications at all, yet the child and others were affected. The five cases highlighted in this research found that teens tried to hide their actions behind the First Amendment to erase the consequences they faced. Many won their legal battles, but all of them experienced irrecoverable consequences of missing important school events that they will never have the opportunity to regain. In addition, they tarnished their online reputation forever. While the First Amendment does provide extensive liberties to say whatever a person wants without legal recourse, public opinions and prospective colleges, employers, and societal organizations do not follow the same rules. They make their determinations based on protecting their organization from accepting new applicants who have proven to be of poor character. Judge Jacobs (2010) sums this up well by asking his readers to consider whether a student winning a free speech claim means that they won from an ethical standpoint.

The First Amendment does protect the speech of Americans, but it should not be a shield to protect hateful attacks. These attacks involve real consequences, no matter what the court decides. The concerns of cyberbullying, sexting, harassment, and online speech all come down to

basic character education. Character education and moral ethics must be brought back into the school and expanded to include online life, especially now with the explosion of technology.

Children are also becoming a primary target for identity theft. According to May (2012), children are 35 times more likely to be targets of identity theft than adults are. In fact, the younger a child is, the better the target. There is very little verification performed when starting a new credit file using a clean social security number. Therefore, a thief who obtains the social security number of a minor can use any name to initiate a credit file. The actual owner will not find out until they apply for their own credit file many years later. One thief was able to open over 40 accounts totaling over 1.5 million dollars within a 10-year period using a nine-year-old child's social security number.

There are many ways to steal the social security numbers. A few of the more common methods include using viruses specifically designed to search for documents that most likely contain social security information, email phishing scams, and data breaches. Children must know how to keep their data safe. They must learn to keep this information private. Children should never use their social security number unless an adult is approving its use. They also need to know how viruses can enter the computer. Downloading files, visiting risky websites, email attachments, and peer-to-peer computing all pose risks. Cybersecurity education plays a key role in protecting against this danger.

Online gaming threats are on the rise as well. Console gaming systems not only allow children to go online and interact with people all over the world, they encourage it. Most of these people are complete strangers and could pose a threat. Parents realize that playing online games on the computer involves using the Internet. They may even take precautions to protect the computer environment while their children play online games. However, gaming systems pose a

slightly different risk because many parents are not aware of the online gaming capabilities. Once online, the dangers are similar. Foul language, harassment, bullying, online grooming, and terrorist recruiting can occur while children play games online. Cyberethics and character education will teach children that this is not a good environment for them and leave the area.

Sexual predators are grooming children as young as six within these online gaming sites. They hang around the sites where they know children will be; specifically targeting sites based on their interested age range. They are clever in their attempts to lure children into a false sense of security. They often pretend to be children in hopes of gaining trust and friendships of the young gamers. As Michelle Conway, a mother of three, reported, her children were getting worrying invites on their Nintendo DS units. One stranger asked for her son's name and birth date. Children do not realize how personal those pieces of information are, and how dangerous it is to provide them to a stranger online. These questions are the beginning of an online grooming relationship that can lead to much more inappropriate behaviors. Starting with seemingly innocent questions and gradually getting more personal soon turns into an invitation to meet in person. From there, the results could be disastrous.

In April 2013, Winnipeg police investigated seven cases of online predators luring children through online gaming consoles; all but one case involved suspects from the United States. CBC reporter Gosia Sawicka accessed an online game called PlayStation Home. She registered as a 13-year old girl and interacted with other players in the public areas. Within minutes, Sawicka reported, several people contacted her character asking sexually explicit questions (Sawicka & Larsen, 2013). This continued even after they found out that she was only 13. Children will believe anything they read online and can easily enter into an inappropriate relationship. People are not always who they say they are online. Responding to inappropriate

questions may seem innocent until it goes too far to stop. Abduction, rape, and murder can result from these inappropriate Internet relationships. Cybersafety education is essential to teach children how to protect themselves while interacting online.

Another significant threat for children online comes from terrorists using online games to take advantage of children to mold their thoughts and possibly their activities in the future. Games like “Call of Duty” and “Medal of Honor” allow groups of people to join forces online, participating in simulated military battles in a highly realistic manner. These war simulation games allow terrorists to plot, plan, and train for attacks while staying hidden by the game play. By nature, these games are extremely violent and realistic. Therefore, conversations about strategies for real life attacks seem to be innocent conversations about the current game, escaping sophisticated security technologies designed to detect suspicious communication. Children can join a terrorist's training exercise while they are acting as part of a campaign, having no idea the real intent of the game.

In addition to plotting their next attacks with online games, terrorists have designed games, which they use to engage young people for promoting their anti-American agenda. One game in particular discovered in this research, allows players to hunt and kill President Bush (Weimann, 2008). This can have extremely dangerous results, especially if the child is exposed to others who oppose President Bush’s politics. The child may overhear others talking negatively about President Bush; then play a game where he or she can hunt the President and virtually kill him. Each of these events on its own would not be cause for concern; however, both together could subliminally plant and strengthen anti-American thoughts into a young impressionable mind geared toward any American president. “Special Force” was an online game allowing players to become warriors in a terrorist attack against Israel. It included a training mode where

players practice shooting skills on Israeli leaders. These games can gradually desensitize children allowing terrorists opportunity for recruitment into their radicalism.

The Boston Marathon bombing tragedy is a direct result of online radicalization. Tsarnaev, who was 19 at the time of the bombings, did not decide to carry out this terrorist attack overnight. It took years of cultivation and desensitizing, resulting from reading extremist Muslim propaganda available on the Internet. Slowly the propaganda turned his mind away from US allegiance and towards an anti-US belief. This is obvious by his words accusing the US Government of killing innocent civilians. However, in his words, he uses the phrase "our innocent civilians" revealing that he abandoned his US allegiance (Abel, Finucane, & Ellement, 2013).

Beyond online games, terrorists are producing Disney-like cartoons; grabbing the attention of young children to spread their anti-Western propaganda. Some show young boys dressed in combat fatigues and participating in various terrorist activities. These subtle messages can slowly whittle away at a child's common sense and start growing a thought process that terrorist can use in the future. Children who never had the ability to hear this propaganda are now within reach via the Internet. Anwar al-Awlaki, a U.S.-born Yemen cleric, used video sermons about foreign policy and poor job prospects for young Muslims to gain a following of English speakers in the United States and Britain. Roshonara Choudhry admitted to listening to 100 hours of al-Awlaki's online lectures before stabbing a British lawmaker in 2010. Children are impressionable and easily led astray when given hours of interaction with any person, especially one who has their same interests and appears "cool" to hang out with. It is imperative that children learn to recognize this agenda and not only avoid it, but also report it. Cybersecurity

education taught in Virginia schools would prepare children for these terrorists' agendas. Vigilant children are another source of homeland security threat reporting.

What Virginia schools are doing to educate children about Internet safety education

Virginia was the first state to mandate Internet safety lessons across all grades in public schools. Throughout this study, the evaluation of six Virginia School district technology plans revealed surprising results. Some address all of the various dangers of Internet safety and some had no mention of it at all. This is in part because there is no accountability that a school system is doing the necessary education. Some schools just do not know what to do. The VDOE produced guidelines for what schools need to do leaving the details to the discretion of each school system. As the one time leader of Internet Safety education, Virginia is the perfect state to step out and embolden its programs statewide.

Plude's Internet Safety Education Plan Grading System (see Table 1) shows the evaluation results for each school and assigns a grade for each school's Internet safety education plan. The evaluation consisted of reviewing publically available data on each school's website. This review took into account all information found in technology plans, Internet safety plans, technology department web pages, and Internet safety pages hosted on the schools websites. The schools reviewed in this research may have more detailed information that was not publically available from their websites.

The bare minimum a school district must have in place, according to the awareness and policy section (See Table 1), is an acceptable use policy and mention that they are addressing Internet safety. Any school district that does not provide the bare minimum receives an F. School districts meeting the bare minimum receive a grade of D since this is the minimum level of effort to protect children while in school. A school district having a plan that specifically addresses at

least three of the eight risks, in addition to the bare minimum, earns a grade of C. A school district having a plan that specifically addresses at least six of the eight risks, in addition to the bare minimum, earns a grade of B. Any school district that has the bare minimum in place, specifically mentions all risk components, and has a program validation process that shows that the schools are providing the education, receives an A.

Each section has a total and a weight assigned to that total to calculate a raw score. The raw score calculations are as follows:

- The Awareness and Policy section has a weight of 30. This results in a score of 60 if both of these items are in place.
- The Plan section has a weight of 3.4. This allows three risk categories to raise the overall score by 10 and six risk categories by 20. Therefore, a school district covering two or five risks can easily increase its grade by adding one new risk to its education plan.
- The training section has no weight, however it does add to the overall raw score. The training section is important to determine whom the plan is educating, however, not deemed as important for an overall grade.
- The Program Validation section carries a weight of 10 so that it increases by one letter grade as well. Therefore, a school can increase its grade one whole letter grade by implementing some form of validation process, whether that is testing, student survey, or teacher surveys.

Raw scores use the following scale to assign the letter grades:

- A – Raw Score is greater than 97.19. This takes into account that a school has every element in place (excluding the training section). The standard was set high

into the 90s for an A to set apart those schools that address all risks, and have a validation process in place to ensure that they are providing this critical education.

- B – Raw score is between 80 and 97.19, inclusively.
- C – Raw score is between 70 and 79.99, inclusively.
- D – Raw score is between 60 and 69.99, inclusively.
- F – Raw score is below 60.

Lynchburg City Schools (LCS) had the most comprehensive plan, earning a grade of B, based on its total calculated score of 86.8 (See Table1). Its plan addressed nearly every risk that this research identified as critical. LCS also realized that this education must begin in kindergarten and continue each year until graduation. LCS suggested lessons and curriculum for Internet safety training based on the VDOE guidelines. However, LCS also admits that their focus is no longer on teaching students how to use technology, but on using technology to support their current activities. This is in part due to the elimination of the technology Standards of Learning (SOL) testing. While LCS has a comprehensive plan, there was no evidence of the plan's application. Testing and reporting would be evidence of this education as required.

Roanoke County School (RCS) also received a B, based on its total calculated score of 84.4, for having six out of the eight risks identified in its plan (See Table1). The RCS plan states that the ITRT staff is responsible for the Internet safety curriculum and includes educating teachers, parents, and students. The RCS technology plan only briefly mentions Internet safety. However, further research discovered an "Internet Safety Lessons for Middle School" document. It includes examples of how to incorporate Internet safety topics into existing subjects (Roanoke County Public Schools, 2009). It covers many topics like ethics, Internet community, cyber-citizenship, cyberbullying, and intellectual property. The document is quite beneficial in that it

provides guidance on how to weave the Internet safety topics into existing classes and where each fits well. However, it only focuses on middle school students, ignoring other grades. Campbell County School (CCS) received a grade of D, based on its total calculated score of 67.4, because its plan does not contain specific topics or an intentional education plan (See Table 1). The CCS technology plan does mention Internet security and recognizes the need to keep students safe on the Internet. It takes into account children from kindergarten to grade 12, parents, and the community in its plan. The CCS website does have links to Internet safety sites as well. However, there is no specific plan for education. Most of the plan addresses preventing children from having access to engage in risky behavior, not educating children on the behaviors themselves.

The Roanoke City Schools also received a grade of D, based on its total calculated score of 63; because they have no plan in place that addresses any of the identified risks (See Table 1). Its technical plan does mention that Internet safety is a focal point for the division with purpose to "facilitate the implementation of high-quality Internet safety programs in schools" (Roanoke City Public Schools, 2010, p. 19). Yet there was no Internet safety education plan detailing what will be taught.

Bedford County Public School received a grade of D, based on its total calculated score of 63; due to the lack of an education plan as well (See Table 1). Its educational technology plan does have a summary of an Internet safety plan; however, that summary does not specify what will be taught. It did have some positive statements about supporting faculty, staff, student, and parents for Internet safety. It also mentioned integrating current technology into the curriculum as they pertain to Internet safety. Its website did have a link to another Internet safety page but the link was not functional.

The Richmond Public Schools (RPS) plan and policies were the most alarming. The RPS plan fails to address Internet safety at all. Based on the district's Internet Safety page, RPS is not interested in restricting content posted on the websites of students and teachers. Its website implies that it is only attempting to put certain guidelines in place. RPS does try to instruct teachers and employees to help students make good decisions while using the Internet and provides links for Internet safety. However, using the phrases, "not preferable that we institute policies that completely restrict students" and "nevertheless must attempt to put certain guidelines in place", makes one question how serious they are at providing any education for Internet safety at all. RPS received a grade of D, based on its total calculated score of 63 (See Table 1).

Table 1

Plude's Internet Safety Education Program Grading System

		Lynchburg City	Campbell County	Roanoke City	Roanoke County	Richmond Public	Bedford County
	Internet Safety Plan Grade	**B**	**D**	**D**	**B**	**D**	**D**
Awareness And Policy	Internet Safety Mentioned	1	1	1	1	1	1
	Acceptable Use Policy	1	1	1	1	1	1
	TOTAL	**2**	**2**	**2**	**2**	**2**	**2**
Plan	Cyberbullying	1	1		1		
	Sexting						
	Ethics	1			1		
	Copyright	1			1		
	Identity Theft	1			1		
	Online Predators	1			1		
	Terrorism	1					
	Online Reputation	1			1		
	TOTAL	**7**	**1**	**0**	**6**	**0**	**0**

Training	Teachers	1	1	1	1	1	1
	Parents		1	1	1		1
	Students	1	1	1	1	1	1
	Link to Internet safety education websites	1	1		1	1	
	TOTAL	**3**	**4**	**3**	**4**	**3**	**3**
Program Validation							
		12	**7**	**5**	**12**	**5**	**5**
	Raw Score	**86.8**	**67.4**	**63**	**84.4**	**63**	**63**

Lack of time is a significant factor inhibiting schools from including Internet safety in their curriculum. The school day is already full, and there is little time for something that is not high on the priority list. For example, Lynchburg City Schools (LCS) no longer considers technology as an isolated topic; they consider it as a tool to aid student achievement. LCS (2011) states, "the greatest needs facing teachers in the use of instructional technology are to become adept at both integrating technology into instruction and using purchased software to supplement their classroom instruction."

The VDOE mandates that schools must teach Internet safety, yet they eliminated technology from SOL testing. This devalues the importance of teaching how to use technology and how to use it safely; sending a mixed message to educators about what is essential. LCS admitted to switching their focus away from teaching students how to use technology to simply relying on technology to support other learning objectives. That decision is a result of Virginia eliminating technology SOL testing. LCS, like many Virginia schools, focuses their efforts on mastering SOL content material. Teachers are reluctant to focus attention on something that is a lower priority from an academic monitoring perspective.

Teachers sometimes do not feel qualified to teach about the safety, especially when they do not understand the technology themselves. However, parents are in the same predicament. Many parents do not understand the technology and feel overwhelmed trying to keep up with their tech-savvy children. McAfee surveyed 1,301 parents in April 2013 and found that 80% of those with preteen children claim they do not have the time or energy to monitor their child's online activity and only 9% know how to how to do so (Palmer, 2013). Children can easily manipulate parents due to a parent's lack of knowledge.

Many teachers do not recognize that teaching Internet safety is their responsibility. However, in Virginia, the VDOE requires schools to educate children on Internet safety. The teacher responsibilities outlined in the LCS technology plan also call for teachers to provide students with a "sequential, structured approach to gaining the skills that will allow them to become independent, responsible users of technology" (Lynchburg City Schools, 2011, p. 89). In Virginia, teachers are required to provide this education whether they feel it is their responsibility or not.

The constant change in technology makes it difficult to keep up with the latest risks. It is imperative that teachers keep their skills current. The VDOE requires mastery of technology standards for initial and renewed teacher licenses (Lynchburg City Schools, 2011). The LCS plan outlines required training expectations in response to the VDOE requirements. They have a technology points program requiring all staff members to accumulate points as part of their professional development requirement. Employees must earn a minimum of six technology points each year by participating in workshops, internally led technology sessions, and independent study. As long as teachers are directing children to use mobile phones, e-readers,

tablets, and computers in their classes, they have an obligation to teach children how to use these tools safely.

Recommendations

Very few would argue that Internet safety education is not a vital component for children to protect themselves in online environments. Even though some states and local education agencies require Internet safety education, data indicate that this education is not happening as thoroughly as necessary to prevent or reduce the risks associated with those identified in this research. According to Pruitt-Mentle, "We need an integrated approach to develop a technologically-savvy workforce that understands the context and usage of digital communication as well as the nuts and bolts behind coding and functionality" (Pruitt-Mentle, 2008, p. 1). There are many challenges preventing Internet safety education in schools. Time, money, and accountability are three factors influencing whether a school incorporates Internet safety education into their curriculum.

Virginia has lost its focus of how important Internet safety education is to children and the safety of every American citizen. The VDOE requires that schools teach Internet safety and created guidelines for doing so. However, their guidelines leave the specific curriculum up to the discretion of each school. This is not working. There needs to be verification that schools are providing the required education. Richmond Public Schools (RPS) admits that they do not want to restrict students posting to websites, yet protecting a child's online reputation is a critical risk that needs attention. In addition, RPS reluctantly put "some" guidelines in place to restrict student activity on the Internet. School districts should be accountable; with validation that they are providing mandatory Internet safety education. SOL testing on Internet safety is one way to ensure that schools are adhering to the state mandate.

Financial constraints limit the education schools can provide. Although Virginia mandated Internet safety education, there is no evidence that they provided any funding for the program. Budgets are tight, making programs like Internet safety education easy targets for elimination, especially when there is no accountability. Funding should be provided for schools to implement the changes in their curriculum. Further research will identify what funding schools need to integrate Internet safety education into their current curriculum.

Many free programs available to schools are designed for delivering a comprehensive Internet Safety program. The VDOE provides links to various Internet safety resources on their website. Many of the Virginia schools, as well as the VDOE website, have a link to NetSmartz.org (Virginia Department of Education, 2007). NetSmartz is a comprehensive website and training system provided by the National Center for Missing and Exploited Children (NCMEC) (National Center for Missing & Exploited Children, 2013). NetSmartz website has a section for children of all ages, parents, police officers, community workers, and educators. Many schools across the country incorporate the NetSmartz system as their Internet safety program. NetSmartz provides hours of Internet safety material for online and downloadable offline usage. Most activities are designed for a few minutes of time, recognizing that schools are already under time pressure. The interaction uses colorful Pixar style characters for elementary grades, and cartoons or real-life stories told by teen agers for middle and high school students. However, many Virginia schools do little to ensure children visit NetSmartz and learn the material. Most parents do not know the NetSmartz links are on the school's website, and many do not have time to visit them with their children. Children are in school for up to eight hours a day and encouraged to use technology in nearly every class. Schools must put Internet safety

education back into their curriculum. The VDOE should do more than post links and guidelines. They need to create a specific curriculum for schools to use, and ensure its delivery.

Many organizations will come to schools and help start these programs for little to no cost. The International Information Systems Security Certification Consortium, Inc. $(ISC)^2$ is an organization that educates and certifies security professionals. They encourage members to volunteer their time by sharing their knowledge of cybersecurity with various organizations, especially schools. $(ISC)^2$ introduced the Safe and Secure Online program in 2006 in conjunction with Childnet International ($(ISC)^2$, 2013). According to their website, the Safe and Secure online program "brings $(ISC)^2$'s information security expert members into classrooms to help children ages 7-14 learn how to protect themselves online and become responsible digital citizens" ($(ISC)^2$, 2013). Other organizations, such as colleges and police departments, are more than willing to help schools take on this challenge to ensure that children receive the necessary education. Schools are not likely to reach out on their own to access these programs. First, the VDOE should approve the program. The mandate to use these tested and free methods of Internet safety classroom education must come from the VDOE, with accountability testing to ensure the delivery.

Each of the schools reviewed in this research could easily increase their scores. Bedford County, Campbell County, Roanoke City, and Richmond Public School districts could easily improve their scores to a B by modeling or adopting the Lynchburg City education plan, which covers most of the identified risks. Lynchburg City and Roanoke County School districts can improve to an A by adding the missing risks and validating that the students do receive the education as stated.

Many teachers do not recognize that teaching Internet safety is their responsibility. However, in Virginia, the VDOE requires schools to educate children on Internet safety. The teacher responsibilities outlined in the LCS technology plan calls for teachers to provide students with a "sequential, structured approach to gaining the skills that will allow them to become independent, responsible users of technology" (Lynchburg City Schools, 2011, p. 89). With about eight hours a day at school, more time than spent with their parents, children are highly influenced by the teachers interacting with them. Teens and parents often clash when it comes to the teen's behavior. It is not uncommon that the same rebellious teen at home, will often take direction from a teacher at school. As a service to society, our educational system must encompass Internet safety education and must include teachers. This does not exclude a parent's involvement, however. Teaching the parents with the children allows parents to share the responsibility and reinforce the training.

Schools must allocate time and money for educators to attend the necessary training in order to educate children to be safe online. The VDOE requires mastery of technology standards for initial and renewed teacher licenses (Lynchburg City Schools, 2011). The LCS plan outlines required training expectations in response to the VDOE requirements, which is a great start. However, additional research needs to identify the skills needed to address the gaps in the current curriculum.

This research identified cyberethics as a key component that addresses most of the dangers children face online. Character education is something that schools can teach now with no technology expertise to start building morals and ethics into students. Many of the dangers that children face online are ethical issues. Building a solid foundation on character will have tremendous benefits as they learn the intricacies of technology. The mass killing incident in a

Newtown, Connecticut school is bringing a renewed focus on character education. According to Russ Sojourner, the director of leadership development for the Character Education Partnership, a Washington-based advocacy organization, and a former principal, "School life can be so much better than it is. Teachers and kids can be happier. Disrespectful behavior can be reduced, and all the disastrous things from chronic bullying can be so reduced" (Adams, 2013, "Signs of a Renaissance", para. 8). Data reveal that attendance goes up, discipline problems go down, and achievement rises when schools focus on character education (Adams, 2013). This is a win-win scenario for schools and children.

It is important to keep in mind that the machines used by children are not the danger; how children use the machines presents the danger. Technology is great and provides tremendous benefits when used properly. Haphazardly using technology exposes children to a great number of risks. The Internet can be a dangerous place for children who do not know how to protect themselves. Schools introduce children to technology, provide access to technology, use technology in classrooms, and require the use of technology outside the classroom; therefore, they are responsible for teaching children how to use technology safely.

Virginia took a stand by being the first state requiring schools to teach Internet safety. However, since then Internet safety has taken a back seat to other subjects deemed more important. The VDOE must make Internet safety a priority again. They must monitor schools' progress in teaching Internet safety and aid schools beyond publishing guidelines.

School districts must incorporate Internet safety into their curriculum whether the VDOE mandates it or not. This is the right thing to do for children and society. Furthermore, school districts need protection against dangers that result from not teaching Internet safety. Schools and their employees are subject to serious consequences when students participate in sexting and

cyberbullying, for example. Raising children to be responsible digital citizens is necessary to limit the dangers children face on the Internet, for all involved. Allowing children to use the Internet without the proper training is like sending them into a minefield. Every click is a virtual step in a field of danger. Education is necessary to protect our children and our country from these risks.

References

(ISC)². (2013). *Safe and Secure Online - Internet Safety for Kids*. Retrieved from https://www.isc2cares.org/safe-and-secure/

Abel, D., Finucane, M., & Ellement, J. R. (2013, June 27). *Boston Marathon bomb suspect Dzhokhar Tsarnaev to face state, federal indictments*. Retrieved from http://www.boston.com/metrodesk/2013/06/27/boston-marathon-bomb-suspect-dzhokhar-tsarnaev-face-state-federal-indictments/cOVfMAxx47SE77qR4e74WL/story.html#

Adams, C. J. (2013). Character education seen as student-achievement tool. *Education Week, 32*(22), 7.

Aldridge, M. J., Davies, S. C., & Andt, K. J. (2013). Is your school prepared for a sexting crisis? *Principal Leadership, 13*(9), 12-16.

Allen, E. (2012, January 4). *Testimony to the Committee on Commercial Sexual Exploitation and Sex Trafficking of Minors in the United States.* Retrieved from http://www.missingkids.com/Testimony/01-04-12

Almansi, C. (2011, February 14). *Cyberbullying: An Interview with Nancy Willard*. Retrieved from http://etcjournal.com/2011/02/14/cyberbullying-an-interview-with-nancy-willard-2/

Bedford County Public Schools. (2011, April 28). *Educational Technology Plan 2011-2016*. Retrieved from http://bedford.sharpschool.net/UserFiles/Servers/Server_1057178/File/Departments/Technology/Tech_Plan/tech_plan.pdf

Besheer, M. (2007, November 8). Voa news: Expert - terrorists exploit internet to recruit, spread ideology. *US Fed News Service, Including US State News*. Retrieved from http://search.proquest.com/docview/468802796?accountid=28902

Butler, K. (2010). Cybersafety in the Classroom. *District Administration, 46*(6), 53-57.

Campbell County Schools. (2013). *Educational Technology Plan.* Retrieved from www.campbell.k12.va.us/Modules/ShowDocument.aspx?documentid=5613

Chow, D. (2009, July 8). *Study: Children ages 2 to 11 make up 9.5 percent of total Internet users in the U.S*. Retrieved from http://www.nydailynews.com/news/study-children-ages-2-11-9-5-percent-internet-users-u-s-article-1.428224

Cloud, J. (2010). Bullied To Death?. *Time, 176(16),* 60-63.

Coffey, S., Wen, P., & Carroll, M. (2013, April 19). *Bombing suspect spent Wednesday as typical student*. Retrieved from http://www.bostonglobe.com/metro/2013/04/19/bombing-suspect-attended-umass-dartmouth-prompting-school-closure-college-friend-shocked-charge-boston-marathon-bomber/8gbczia4qBiWMAP0SQhViO/story.html

Dodds, P. (2011, July 20). *Al Qaeda Plans Cartoon Recruiting Film for Kids*. Retrieved from http://cnsnews.com/news/article/al-qaida-plans-cartoon-recruiting-film-kids

Eraker, E. C. (2010). Stemming Sexting: Sensible Legal Approaches To Teenagers' Exchange Of Self-Produced Pornography. *Berkeley Technology Law Journal, 25*(1), 555-596.

Farlex, INC. (2013). *Freedom of Speech legal definition of Freedom of Speech*. Retrieved from http://legal-dictionary.thefreedictionary.com/Freedom+of+Speech

Federal Communications Commission. (2012, April 19). *Protecting Children in the 21st Century Act Amendment*. Retrieved from http://www.fcc.gov/document/protecting-children-21st-century-act-amendment

Friscolanti, M. (2012). Shunned In Life, Remembered In Death. *Macleann's, 125*(42), 70-72.

Herman, J. D. (2010, April). Sexting: it's no joke, it's a crime. *Illinois Bar Journal, 98*(4), 192+. Retrieved from Retrieved from http://go.galegroup.com/ps/i.do?id=GALE%7CA223226067&v=2.1&u=nysl_ce_uticacol&it=r&p=AONE&sw=w

Hinduja, S., & Patchin, J. W. (2010). Bullying, Cyberbullying, and Suicide. *Archives Of Suicide Research: Official Journal Of The International Academy For Suicide Research, 14*(3), 206-221. doi:10.1080/13811118.2010.494133

Hinduja, S., & Patchin, J. W. (2013, April). *State Cyberbullying Laws.* Retrieved from http://www.cyberbullying.us/Bullying_and_Cyberbullying_Laws.pdf

Jacobs, T. A. (2010). *Teen Cyberbullying Investigated: Where Do Your Rights End and Consequences Begin?* Minneapolis: Free Spirit Publishing.

KATHERINE EVANS, Plaintiff, v. PETER BAYER, in his individual capacity, De-fendant., 08-61952-CIV-GARBER (UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF FLORIDA February 12, 2010).

Khadaroo, S. T. (2010, February 26). *Internet safety: Whose job to teach kids about it?* Retrieved from http://www.csmonitor.com/USA/Society/2010/0226/Internet-safety-Whose-job-to-teach-kids-about-it

Klomek, A. B., Sourander, A., & Gould, M. (2010, May). The Association of Suicide and Bullying in Childhood to Young Adulthood: A Review of Cross-Sectional and Longitudinal Research Findings. *Canadian Journal of Psychiatry, 55*(5), 282-288. Retrieved from http://search.proquest.com/docview/366139246?accountid=28902

Lenhart, A. (2009, December 15). *Teens and Sexting.* Retrieved from http://www.pewinternet.org/Reports/2009/Teens-and-Sexting.aspx

Lenhart, A. (2010, May 6). *Cyberbullying 2010: What the Research Tells Us.* Retrieved from http://www.pewinternet.org/Presentations/2010/May/Cyberbullying-2010.aspx

Lenhart, A. (2010, February 3). *Social Media and Young Adults.* Retrieved from http://www.pewinternet.org/Press-Releases/2010/Social-Media-and-Young-Adults.aspx

Lynchburg City Schools. (2011, April 13). *Lynchburg City Schools 2010-2012 Educational Technology Plan.* Retrieved from http://www.lcsedu.net/category/postings/documents

Lynchburg City Schools. (2013). *Academics | Robert S. Payne Elementary School*. Retrieved May 28, 2013, from http://www.lcsedu.net/schools/rsp/academics

Madden, M., Lenhart, A., Duggan, M., & Gasser, U. (2013, Mar 13). *Teens and Technology 2013.* Retrieved from http://www.pewinternet.org/~/media//Files/Reports/2013/PIP_TeensandTechnology2013.pdf

Magid, L. (2011, September 17). *Cyberbullying Is a Serious Problem, but Is It an Epidemic?* Retrieved from http://www.huffingtonpost.com/larry-magid/cyberbullying-is-a-seriou_b_967310.html?view

Marklein, M. B. (2011, September 22). *More college officials learn about applicants from Facebook.* Retrieved from http://usatoday30.usatoday.com/news/education/story/2011-09-21/facebook-google-college-applicants/50497248/1

May, J. (2012). *Child Identity Theft Report 2012.* Retrieved from https://www.allclearid.com/themes/allclearid/docs/ChildIDTheftReport2012.pdf

Meneely, G. (2013, March 26). *I didn't sleep for a week after my kid was 'friended' by online stranger*. Retrieved from http://www.thesun.ie/irishsol/homepage/news/4859744/I-didnt-sleep-for-a-week-after-my-kid-was-friended-by-online-stranger.html#ixzz2PszOGTjB

Millen, J. (2013, May 21). *Top 10 Tips for New College Grads to Clean up Their Online Reputations*. Retrieved May 27, 2013, from http://www.schoolofrep.com/blog/

Murray, R. (2012, April 10). *Identity theft among children on the rise: How to keep your kids safe*. Retrieved from http://www.nydailynews.com/news/money/identity-theft-children-rise-kids-safe-article-1.1059311

Nansel, T. R., Overpeck, M., Pilla, R. S., Ruan, W. J., Simons-Morton, B., & Scheidt, P. (2001, April 25). Bullying Behaviors Among US YouthPrevalence and Association With Psychosocial Adjustment. *The Journal of the American Medical Association*, 2094-2100. doi:10.1001/jama.285.16.2094

National Center for Missing & Exploited Children. (2013). *NetSmartzKids*. Retrieved from http://www.netsmartzkids.org/

National Cyber Security Alliance. (2013). *C-SAVE-StaySafeOnline.org.* Retrieved from http://www.staysafeonline.org/teach-online-safety/csave

Palmer, G. (2013, June 4). *85 percent of US tweens are on Facebook: survey* . Retrieved from http://www.nbcnews.com/technology/85-percent-us-tweens-are-facebook-survey-6C10189125

Parks Associates. (2013, April 25). *Parks Associates: 78% of U.S. Broadband Households Have a Home Network Router, Driving Demand for Tech Support - Yahoo! Finance*. Retrieved from http://finance.yahoo.com/news/parks-associates-78-u-broadband-123000864.html

Poland, S. (2011, May). The Phenomenon Known as Bullicide. *District Administration, 47*(5), p. 92.

Pruitt-Mentle, D. (2008, October). *2008 National Cyberethics, Cybersafety, Cybersecurity Baseline Study.* Retrieved from http://www.edtechpolicy.org/cyberk12/Documents/C3Awareness/NationalC3BaselineSurvey_Extract_sept_2010.pdf

PTI. (2011, April 15). *Terrorists using online games a major threat*. Retrieved from http://governancenow.com/gov-next/egov/terrorists-using-online-games-major-threat

Purcell, K., Heaps, A., Buchanan, J., & Friedrich, L. (2013, February 28). *How Teachers Are Using Technology at Home and in Their Classrooms.* Retrieved from http://pewinternet.org/Reports/2013/Teachers-and-technology

Richmond Public Schools. (2010a). *Educational Technology Plan 2010-2015*. Retrieved from http://web.richmond.k12.va.us/Portals/0/assets/ICTS/pdfs/RPSTechPlanFinal12062010-1.pdf

Richmond Public Schools. (2010b). *Internet Safety*. Retrieved from http://web.richmond.k12.va.us/Departments/DepartmentOfInstruction/Technology/NetSafety.aspx

Roanoke City Public Schools. (2009, July 1). *Roanoke City Public Schools Strategic Plan (2009-2014).* Retrieved from http://rcps.info/modules/cms/pages.phtml?pageid=184506&sessionid=af9b3d01cb0864654cca507064a91a46&sessionid=af9b3d01cb0864654cca507064a91a46

Roanoke City Public Schools. (2010, October 22). *Roanoke City Public Schools 2010-2015 Educational Technology Plan.* Retrieved from

http://rcps.info/modules/cms/pages.phtml?pageid=184506&sessionid=af9b3d01cb0864654cca507064a91a46&sessionid=af9b3d01cb0864654cca507064a91a46

Roanoke County Public Schools. (2009, February 25). *Internet Safety Lessons for Middle School.* Retrieved from http://www.rcs.k12.va.us/isafety/lessons/ms/ms.pdf

Roanoke County Schools Board. (2010). *Comprehensive Plan.* Retrieved from http://www.rcs.k12.va.us/administration/default.shtml

Sawicka, G., & Larsen, L. (2013, April 2). *U.S. predators use video games to lure Canadian kids*. Retrieved from http://www.cbc.ca/news/technology/story/2013/04/01/mb-online-luring-children-winnipeg.html

Shaw, G. (2013, May 6). *Predators target kids through online games*. Retrieved from http://www.montrealgazette.com/life/Predators+target+kids+through+online+games/8341242/story.html

Sony Computer Entertainment America LLC . (2013). *PlayStation®3 Features – PS3™ Feature Review, PlayStation® Trophies, Updates & Multimedia*. Retrieved from http://us.playstation.com/ps3/features/

Spencer, A. (2010, October 23). *Bullying, Sexting, Lead to Teen Suicide.* Retrieved from http://voices.yahoo.com/bullying-sexting-lead-teen-suicide-7031510.html?cat=4

Starr, P. (2008, July 7). *Congress: Al-Qaeda Using Internet to Recruit Terrorists in the US*. Retrieved from http://cnsnews.com/news/article/congress-al-qaeda-using-internet-recruit-terrorists-us

StopBullying.gov. (n.d.). *What is Cyberbullying*. Retrieved from http://www.stopbullying.gov/cyberbullying/what-is-it/index.html

Teitel, E. (2012). Bullied to death. *Maclean's, 125*(42), 68.

U.S. Census Bureau. (2001, September). *Home Computers and Internet Use in the United States:August 2000.* Retrieved from http://www.census.gov/prod/2001pubs/p23-207.pdf

Vargas, T. (2008, May 3). *Virginia Tries to Ensure Students' Safety in Cyberspace*. Retrieved from http://articles.washingtonpost.com/2008-05-03/news/36860897_1_internet-safety-online-safety-safety-skills

Vincent, N. (2012, March 28). *Social Networking Site Settles FTC Charges*. Retrieved from http://www.onguardonline.gov/blog/social-networking-site-settles-ftc-charges

Virginia Department of Education. (2007, October). *Guidelines and Resources for INTERNET SAFETY in Schools*. Retrieved from http://www.doe.virginia.gov/support/safety_crisis_management/internet_safety/guidelines_resources.pdf

Weimann, G. (2008, March 5). *Online Terrorists Prey on the Vulnerable*. Retrieved from http://yaleglobal.yale.edu/content/online-terrorists-prey-vulnerable

Wheeler, T. (2011). Facebook Fatalities: Students, Social Networking, and the First Amendment. *Pace Law Review, 31*(1), 182-227.

Willard, N. (2012, September). Protecting children in the 21st century: to keep children safe, it is necessary to ensure that they have the values and skills to make good choices. *District Administration, 48*(8), 86-87.

Willetts, D., & Wells, T. (2012, March 20). *Islamic extremists use Call of Duty to plan terror attacks*. Retrieved from http://www.thesun.co.uk/sol/homepage/news/4205896/Terrorists-play-online-games-like-Call-of-Duty-to-plan-attacks.html

Xbox One - How It Games. (n.d.). Retrieved from http://www.xbox.com/en-US/xboxone/how-it-games

Young people face online safety 'timebomb'. (2013). *Community Practitioner, 86*(3), 6. Retrieved from Retrieved from http://go.galegroup.com/ps/i.do?id=GALE%7CA326505514&v=2.1&u=nysl_ce_uticacol&it=r&p=AONE&sw=w

Zetter, K. (2009, January 15). *Child Porn Laws Used Against Kids Who Photograph Themselves*. Retrieved from http://www.wired.com/threatlevel/2009/01/kids/