

INTERNET SAFETY PROGRAM FOR PARAPROFESSIONALS:
AN EXPLORATORY STUDY

A DISSERTATION
SUBMITTED TO THE FACULTY
OF
THE GRADUATE SCHOOL OF APPLIED AND PROFESSIONAL PSYCHOLOGY
OF
RUTGERS,
THE STATE UNIVERSITY OF NEW JERSEY
BY
SCOTT KRAITERMAN
IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE
OF
DOCTOR OF PSYCHOLOGY

NEW BRUNSWICK, NEW JERSEY

MAY 2015

APPROVED: _____
Nancy Boyd-Franklin, Ph.D.

Patrick Connelly, Psy.D.

DEAN: _____
Stanley Messer, Ph.D.

Copyright 2015 by Scott Kraiterman

ABSTRACT

As the Internet increases its dominant influence in American life, the need for valuable Internet safety training becomes ever greater, especially in the nation's schools. This exploratory study examined the development, presentation, and evaluation of an Internet Safety Program in a New Jersey public school district. Through adapting publicly available programs to reflect current online trends, behavior and web tools, and incorporating an extensive knowledge of technology, an Internet Safety Program was delivered to a population of paraprofessionals identified by the district's administration as in need of improved awareness of issues disproportionately impacting students, specifically in the areas of cyberbullying, nonutilization of website security features, and the existence of online dangers, such as predators who target adolescents. Identical pre- and post-Program assessments were administered to ascertain both knowledge possession and attainment of targeted content relating to nine goals which exemplified best practices with respect to cyberbullying, utilizing online security, and reducing risk of exposure to online predators. The use of descriptive statistics to explore the program's value indicated that more than half (57%) of the goals were met. Goals relating to specific dangers and predators saw relatively high levels of attainment (62%), the primary cyberbullying goal of reporting to a superior was met by all participants, and goals relating to online security were met by half. However, measurements of value through capturing knowledge attainment fluctuated considerably, as many participants indicated previous knowledge in the areas of cyberbullying and predator avoidance. Although the program's exploratory nature involved a small, non-randomized sample and one administration, expanded usage would raise issues concerning the need for a standardized needs assessment, challenges in creating programs effective across age groups, the need to address emotional responses to

sensitive content, and consistency when the program is delivered by a presenter other than the developer.

ACKNOWLEDGMENTS

This dissertation has been a long journey, and I could not have possibly made it through without the help of a few amazing people in my life. I would first like to thank my dissertation committee for their incredible guidance and support. Dr. Nancy Boyd Franklin, you have been a constant source of guidance, knowledge, and support for me since I started graduate school and I am so thankful for everything that you've done for me. From our class discussions on race, religion, and family dynamics to your guidance through every step of the dissertation process, I cannot thank you enough. Dr. Pat Connelly, you've been a mentor for me since my earliest days at the Teen Center and I've been trying to emulate your masterful therapeutic style ever since. Thank you for being a part of my dissertation committee and I look forward to our continued time together as colleagues. Sylvia Krieger and Kathy McLean, thank you for keeping me on task through the years and for all your encouragement. I would also like to say thank you to Dr. Susan Forman, who has always been supportive of me throughout my years at GSAPP.

To my family, your unconditional support, patience, and love has been an invaluable source of strength throughout my graduate school career and I would not be here without your help. Mom, Dad, and Robin, thank you so much and please know that I appreciate you more than I could ever say. Elisa, your encouragement over the past year and a half has sustained me through the toughest times, and this final completed work is dedicated to you.

TABLE OF CONTENTS

	PAGE
COPYRIGHT.....	ii
ABSTRACT	iii
ACKNOWLEDGMENTS	v
CHAPTER	
I. STATEMENT OF THE PROBLEM.....	1
Rationale for the Internet Safety Staff Training Program.....	2
Structure of Needs	4
Population of the Study.....	4
Goals	5
Pre-Assessment Vs. Post-Assessment of Needs	5
The Internet Safety Program Training	6
Areas Targeted.....	6
Determining Effectiveness.....	7
II. REVIEW OF THE LITERATURE	9
The Internet Expands, and So Do its Dangers	9
Safe Online Behavior and Best Practices in Internet Safety.....	13
Sexting, Online Predators, and Vulnerability	18
Incorporating Current Data.....	20
III. METHODOLOGY	24
Participants.....	24
Procedures.....	25

Consent Form.....	26
Pre-Assessment Survey.....	26
Presentation.....	26
Post-Assessment Survey	30
Internet Safety Program Evaluation Components	30
Needs Assessment Protocols	30
Goals	31
Treatment of Data	33
Consent and Assessment Forms	33
Data Collection	33
Goal Attainment.....	33
Categories of Responses	34
“Incoming Knowledge” Indicated Desired Knowledge Possessed by a Participant Prior to the Training That Was Also Imparted by the Training, as Was Reflected in the Pre-Assessment Survey	34
“Learned Responses” Indicated Desired Knowledge Gained During the Training Not Present Prior to the Training, as Was Reflected in the Post-Assessment Survey	35
“Measured Responses” Indicated Participants Possessed Desired Knowledge Contained in the Training, Reflected in Pre-Assessment Surveys as “Incoming	

Knowledge” or Post-Assessment Surveys as “Learned Knowledge”	35
Data Analysis.....	36
Descriptive Data Analysis	38
IV. RESULTS	40
Internet Safety Program Target Areas and Goals	40
Goals 1-3: Responses to Cyberbullying.....	40
Goal 1: Reporting Incidents of Cyberbullying to a Superior.....	41
Goal 2: Saving Any and All Information From the Cyberbullying Event	41
Goal 3: Refer the Cyberbullying Victim to the Proper Support Within the District.....	42
Goals 4-6: Safe and Private Online Behavior	42
Goal 4: Effective Use of Privacy Controls on Facebook.....	43
Goal 5: Username/Password Generation Across a Social Media Landscape	43
Goal 6: Improving Their Own Safety and That of Their Students Online.....	44
Goals 7-9: Addressing Specific Dangers in the Online Community	45
Goal 7: Knowledge of Websites Frequented by Online Predators	45
Goal 8: Methods of Grooming.....	46

Goal 9: Actions Students Can Take to Decrease	
Exposure to Online Predators	46
Summary of Goal Attainment.....	47
Online Habits and Trends	48
V. DISCUSSION.....	50
Information Gathering	51
Value of the Internet Safety Program	52
Measuring Value: “Learned Responses” and Goal Attainment.....	55
“Incoming Knowledge” Vs. “Learned Responses”	58
The Utility of “Measured Responses”	59
Impact on Children and Adolescents	61
Strengths of the Study.....	61
Limitations of this Study.....	62
Implications and Recommendations	65
Implications for Future Research.....	65
Implications for Future Trainings	68
Implications for Future Internet Safety Program Dissemination....	69
REFERENCES	71
APPENDICES	78

Chapter I

Statement of the Problem

The rapid advances in, and widespread access to, communication, particularly with respect to the Internet, has drastically altered the ways in which people interact with and view the world. Technological progress has come at a price, however. When abuses occur, the lawmakers, service providers and parents who seek to address them confront a moving target. A further complication arises from the disparity in the familiarity and ability of Internet users and those who wish to limit abuses. This is especially evident in the school environment. Children, particularly adolescents, grasp concepts related to technological advances and master new tools at a much faster rate than adults. In addition, children often lack the judgment to discern the nature of the Internet as a public space, which impedes an evaluation of the appropriateness and possible consequences of their behavior. Schools are thus in a unique position to confront the challenges of the evolving digital landscape, as those in authority struggle to breach the significant disconnect between youth and adults with respect to knowledge of the dynamic nature of Internet technology, changes in digital cultural trends, and attitudes toward safety and propriety.

A school official in the district of R in New Jersey (the “District”), the Director of Pupil Services (the “Director”), became aware of online student behavior which subjected them to multiple risks, among them cyberbullying, identity intrusion as a result of oversharing, and potential exposure to Internet predators, among others, which was exacerbated by the nonutilization of Internet software security tools. Devising a method by which the dangerous activity might be identified and responded to, however, presented

a considerable challenge given the “digital divide,” i.e., the Internet sophistication of students versus the knowledge deficiencies of staff.¹

Rationale for the Internet Safety Staff Training Program

Although discussions of Internet safety were a component of the health class curriculum for students, the presentation was superficial and did not offer a consistent and valuable means of learning about this important issue. In addition, there were no district-wide Internet safety programs nor official policies on the delivery of content related to Internet safety. As incidents arose, they were responded to in an ad hoc, piecemeal fashion. Further evidence of the need for an Internet safety program was corroborated by alarming findings in a survey: approximately 22% of girls and 18% of boys between the ages of 13 to 19 have posted sexually provocative and/or nude pictures or videos of themselves online (National Campaign to Prevent Teen and Unwanted Pregnancy, 2008). In addition, the administration was concerned with oversharing on social media as well as cyberbullying. While incidents of cyberbullying had not been fully documented, the past decade had seen complaints escalate each school year with no coordinated response. Urgency was also indicated as a result of recent state legislation (Anti-Bullying Bill of Rights Act, 2010) which added a legal dimension to the District’s need to address this issue.

Prior Internet safety programs for staff and parents (to be discussed more fully below) had been offered and had received significantly positive responses as having been informative and valuable, but were available only on a few occasions to very limited

¹ The name of the district and all of the parties involved have been changed in order to protect their confidentiality.

groups, such as child study team members, health and physical education teachers, and a small number of parents of special education students. The Director had requested that the author of this study, who had served in several capacities in the District as a component of his graduate level studies in psychology at a nearby university, be responsible for the delivery of the programs, the details of which are as follows: On November 1, 2010, a federally-funded Internet safety program called *NetSmartz*, developed by the National Center for Missing & Exploited Children (National Center for Missing & Exploited Children, 2012a), was adapted for use and delivered to District members of child study teams during the course of an in-service training day. On March 25, 2011, another adapted version of *NetSmartz* was delivered to 45 District high school health and physical education teachers during an in-service training day. On the evening of May 4, 2011, a more heavily modified version of *NetSmartz* was presented to 12 parents of special education students as part of a series of presentations done four times a year for such families.

As the need for a standardized Internet safety program had been identified, the reaction to the targeted programs in the past had been favorable and administrative support within the District existed, the Director decided that an Internet safety program, adapting elements of the programs offered previously to limited populations, be developed and delivered to educators in the District. In developing an Internet safety program (“Internet Safety Program” or the “Program”), it was important to evaluate (a) what had been effective in the past, (b) what was currently available in existing programs, and (c) those topics missing from existing programs which would be valuable for inclusion. Internet Safety Program planning, development, implementation, and evaluation services were initiated and then presented to the Director at the District Board

of Education administration headquarters. Although she had overseen the implementation and evaluation of programs previously provided to students in the district, these had been limited to classified students receiving special education services.

Structure of Needs

Population of the Study

The Internet Safety Program was designed for currently employed paraprofessionals or “teacher’s aides” working in the District (a total of 83 adults). Such paraprofessionals are required to be college-educated adults with substitute teaching certificates whose responsibilities include assisting with classroom instruction, behavior management, and student work. In-service professional development days were earmarked for the purpose.

The target population of paraprofessionals had been identified by the Director as often unfamiliar with the social media outlets and mobile sharing applications popular with students; hostile to technology usage both for themselves and their children, with many staff members reporting that they did not permit their children access to the Internet; poorly informed about Internet safety; and without the knowledge or skill to help students—many of whom were relative experts in new technology, Internet tools, and web efficiency—maintain an online life that did not put them at risk.

Informal examinations of the responses to ever-increasing reports of cyberbullying (as discussed above), and other threats to online safety, revealed that these situations had been handled inappropriately, which often resulted in frustrated misunderstanding rather than resolution. As paraprofessional duties encompassed proficiency in the areas or domains of student academic support, student behavioral support and teacher instructional support, the Director maintained that exhibiting a lack

of knowledge of healthy and safe Internet safety practices fell under the domain of “teacher instructional support,” and thus required remediation.

Goals

The Internet Safety Program’s intention was that increased instructor knowledge about the realm of Internet safety would enable them to better offer guidance, support and instruction to students, and thus improve student behavior to correspond with standards of safety and privacy. After the identification of the domain as behavior on the Internet with regard to Internet safety skills and knowledge and the support paraprofessionals could provide to students, three specific questions were designed which would serve as the structure of program development:

1. What information do paraprofessionals need to learn to deal effectively with instances of cyberbullying?
2. How can paraprofessionals help their students learn to practice safe and private online behavior?
3. What information do paraprofessionals need to possess awareness of specific dangers that exist in the online community?

Pre-Assessment Vs. Post-Assessment of Needs

The structure of needs, identified by the Director as reasonable to address in the developed program, were determined as a result of her experiences as an administrator in the District and further clarified with the author of this study through an interview.

After an analysis of the paraprofessionals’ responses to the three questions listed above, their current status was identified as follows: Paraprofessionals did not possess knowledge of effective responses to cyberbullying, were not aware of practices that

facilitate safe online behavior for students, and could not identify specific dangers inherent in online activity.

This general overview of paraprofessionals' level of knowledge provided clarification for program development and guided development of a survey to target those areas. Such survey would clarify the level of knowledge paraprofessionals had prior to the Internet Safety Program (pre-assessment) and their level of knowledge after Program exposure (post-assessment). The two states could then be captured and compared through descriptive analysis (see Appendix C).

The Internet Safety Program Training

Areas Targeted

Training provided during the Internet Safety Program included the following three broad categories, with accompanying subtopics, which had been targeted for improvement in the developed program:

1. *Effective response to cyberbullying.* This area included (a) alerting study participants to the need to report instances of cyberbullying as soon as they became aware of them; (b) explaining the context of the recent legislation, the New Jersey “Harassment/Intimidating/Bullying” law (Anti-Bullying Bill of Rights Act, 2010) with respect to cyberbullying; (c) informing participants of the obligation to save evidence; (d) educating participants about the school resources that students could utilize to help them to cope and heal after being victimized; (e) clarifying official school policy on appropriate responses to cyberbullying; and (f) acquainting participants of resources provided by the school for use with students and parents.

2. *Safe and private online behavior.* This area included instructing participants (a) of the importance that identifying information not be incorporated into online profiles,

and if such information had been already posted, to remove it promptly; (b) that privacy features of websites and Internet service delivery be utilized effectively; and (c) of all of the possible consequences resulting from the public nature of posted material on the Internet. Paraprofessionals were taught about how easily information could be accessed without knowledge of usernames and passwords, despite a user's belief that such information was "private," how material posted on many different websites could be pieced together to create full profiles on social networking users, and the potential consequences of posting or proliferating provocative material online. Participants were also informed about resources that websites provided to end-users for privacy protection.

3. *Awareness of specific dangers that exist in the online community.* This area included educating the participants as to knowing the methods by which Internet stalkers and predators (a) court and/or track victims, (b) trade in sensitive or private information, and (c) coordinate efforts to combine information and share advice. Paraprofessionals were taught about specific websites dedicated to Internet predators, the large numbers of predators present in some online communities, and how easy it is for predators to track and/or groom adolescents online. Legal and undetectable ways in which predators could gather information were demonstrated.

Determining Effectiveness

An effective program would help to address and remedy the identified problem of Internet safety, conveying to paraprofessionals within the district: (a) the knowledge to deal effectively with instances of cyberbullying, (b) a mastery of the practice of safe and private online behavior, and (c) a comprehensive awareness of the specific dangers that exist in the online community. The paraprofessionals, in turn, would utilize the

knowledge gained in the Internet Safety Program and pass that knowledge on in interactions with students.

Chapter II

Review of the Literature

The Internet Expands, and So Do its Dangers

As a result of the widespread proliferation of Internet use starting in the mid-1990s and continuing improvements in technology, Internet safety has become an increasing challenge. Significant empirical gaps exist in the research in the field of Internet safety, complicated by the mercurial nature and exponential developments in technological discovery. In a comprehensive review of 40 years of Internet technology and how the consistently changing landscape affects risks to children, Atkinson and Newton (2010) reviewed the lack of available research pertaining to discrepancies between need, perceptions, empirical study, and legislation (Atkinson & Newton, 2010). They highlighted how the incredible speed at which the medium evolves frustrates the ability of empirical study to keep pace (2010). They recommended further study focusing on the specific vulnerability of youth, with reference to changing behaviors and dangers alongside rapid online technological advances (2010).

The Internet safety issue is exacerbated by the fact that so much Internet content is accessible at no financial cost to users, forcing web developers and other Internet-based technology companies to look to other methods of generating income. The most effective method has proven to be advertising, which is especially lucrative as websites such as Facebook and Google compile profiles on their users that span virtually every possible domain imaginable (Acohido, 2011) (Miller & Sengupta, 2013), allowing advertisers to narrowly target their audience and customize their advertising. If a topic, trait, belief, or common interest can be tracked and collected, it will, and this increasingly valuable demographic information is sold to advertisers. As a result, websites, particularly social

networking websites, constantly push their users to share greater amounts of information—information that then becomes part of the public domain.

The public availability of this otherwise private information results in many problems for individuals, and is especially threatening to children and adolescents. Social networking websites, designed to maximize their ability to create advertising profiles on their users, have become a vital component in the lives of many children and adolescents. They are encouraged to share ever greater amounts of private information on the Internet while their profiles become increasingly accessible to the public.

Children and adolescents are not only lucrative targets for advertisers, but also for predators and hackers who capitalize on the open nature of social networking.

Technology advances at a faster rate than regulators and lawmakers can keep pace with. This situation has become a “perfect storm” of threat as children and adolescents use the Internet more and more, buy into technology companies’ business model and open up their lives in public, and expose themselves to an endless source of predators whose bad intentions are made more capable of realization with enhanced technical skill. Without knowledge of safe Internet practices and the dangers that exist on the Internet, children are exposed to bullying, harassment, predators who seek to exploit and endanger them, and other forms of personal harm. Internet safety programs seek to address these threats.

Among the responsibilities of government is to protect the vulnerable from harm. After several high profile cases of missing children highlighted the absence of any nationwide organization addressing this issue, Congress passed the Missing Children’s Assistance Act in 1984, which established a national database for the tracking and investigation of missing children under the auspices of the concurrently created National Center for Missing & Exploited Children (National Center for Missing & Exploited

Children, 2012). This organization, while private and non-profit in nature, continues to be funded in part by the United States federal government. Its role has expanded from a national resource center and clearinghouse on missing and exploited children to encompass many other threats faced by children and adolescents, among them Internet safety (National Center for Missing & Exploited Children 2012).

The United States government, acknowledging the federal role in addressing the need for Internet safety training for children across the country, has funded the development of various programs for public use designed to accomplish this goal, the most popular of which is *NetSmartz* (National Center for Missing & Exploited Children, 2012). Intended for children from the ages of 5-17, their parents or guardians, law enforcement, and educators (National Center for Missing & Exploited Children, 2012), *NetSmartz* provides “age-appropriate resources to help teach children how to be safer on- and offline” (National Center for Missing & Exploited Children, 2012a). The Internet Safety Program has three stated goals: (a) educating children on potential risks; (b) engaging parents and students together in discussions of Internet risks; and (c) empowering children to protect themselves, prevent exposure to predators, and report incidents to the correct adult (National Center for Missing & Exploited Children, 2012).

Considering that *NetSmartz* is currently one of the most widely used Internet safety programs in the country, the lack of empirical support for its effectiveness, especially recently, is a cause for concern. At the request of *NetSmartz*, George Washington University conducted a 2005 study of the program with a limited number of public school students in Maine and found that exposure to the *NetSmartz* program for students aged 9-14 resulted in more responsible online behavior (Brookshire & Maulhardt, 2005). Although the investigators had hoped to expand the study school-wide,

and received Institutional Review Board approval, timing issues intervened to prevent such expansion and, thus, the findings were restricted to individual students who had gone through the program (Brookshire & Maulhardt, 2005). Given the limited population of the study, the lack of any subsequent empirical support, the nature of the Internet and how far technology has progressed in the past ten years, it is questionable whether these findings are applicable to the current version of *NetSmartz*.

Another Internet safety program, available across the country as well as at many Department of Defense schools located around the world, is i-SAFE. i-SAFE, a recipient of federal funding since 2002, is the product of a 50(c)(3) non-profit foundation created in 1998. Its goal is “educat[ing] students on how to avoid dangerous, inappropriate, or unlawful online behavior” (i-SAFE, 2012a). The program, although also designed to be used in schools as well, offers a contrast with *NetSmartz* in terms of program delivery. While *NetSmartz* demands a dedicated block of time, i-SAFE’s programs are “on-demand” and spread into dozens of mini-lessons (i-SAFE, 2012). While lacking the national penetration and acceptance of *NetSmartz*, i-SAFE features a greater breadth of empirical support for its programming, despite also lacking recent evaluations (in this case, eight years). The United States Department of Justice ordered an evaluation by the consulting firm, Caliber Associates, in 2003 that was completed in 2006 (Chibnall, Wallace, Leicht, & Lunghofer, 2006). While the evaluation noted “positive and significant changes” (p. 59) in their knowledge of what constituted safe online activity, it was not shown to be effective in changing behavior of those who received i-SAFE programming (Chibnall et al., 2006).

Safe Online Behavior and Best Practices in Internet Safety

Researchers have begun to look at the contrast in attitudes, knowledge, behavior, and patterns of interaction between adults and children as it relates to the digital universe. Terms, such as “digital immigrants” versus “digital natives” (Prensky, 2001), are frequently used to delineate those born before or after the dawn of the “computer world,” approximately 1964 (Zur & Zur, 2011). “Digital natives” adapt to technology at a much faster rate and with more skill than “digital immigrants” born in a precomputer world. The divide between the two populations threatens to become even more stark as access to technology and cultural acceptance of online normalcy increase (Zur & Zur, 2011).

This growing divide may often be found in the relationship between parents and adolescents relating to online attitudes and behaviors with regard to what parents believe their children to be doing online and their children’s true behavior, according to the Family Online Safety Institute (Hart Research Associates, 2012). For example, while 91% of parents report being “very or somewhat well informed” of their adolescent children’s online activities and with their mobile devices, their teenage children report greater skepticism, with only 62% according their parents such knowledge (2012). A similar discrepancy exists (93% to 61%) with respect to expectations of time spent online, but the greatest gaps between the two exist in the areas of social networking and media sharing sites (2012). The study also reported that 43% of adolescents regretted having posted something online (2012).

Many websites and organizations in the private sector are devoted to providing adults with information and support about safe online behavior for their children. Common Sense Media, among the most popular of these websites, details their mission as “dedicated to helping kids thrive in a world of media and technology” by providing to

adults, including parents, teachers, and policymakers, “unbiased information, trusted advice, and innovative tools to help them harness the power of media and technology as a positive” in their children’s lives (Common Sense Media Inc., 2015). Instead of providing targeted and specific Internet safety programming, Common Sense functions as an aggregator of information concerning advances in technology, current topics about Internet safety, summaries of studies and news reports relating to Internet safety, and instructional videos for school-age children (Common Sense Media Inc., 2012). While there does not seem to be any available empirical support for its value to children in the realm of Internet safety, it does provide a very current (more so than other websites with a similar mission) and extensive resource of issues relating to youth Internet use (Common Sense Media, 2012, 2015). Interestingly, unlike many other organizations whose mission is the protection of children, Common Sense Media receives no federal funding, nor does it wish to, so as to insure its continued existence as independent and nonpartisan (Common Sense Media Inc., 2012).

Researchers in the United Kingdom currently seem to be leading the empirical charge in understanding and developing best practices for Internet safety. In the past few years, many of the major qualitative and longitudinal studies looking at cyberbullying, dangers specific to the Internet and online predators have been conducted in the United Kingdom.

The European Commission in the United Kingdom has partnered with three leading Internet and technology organizations in Great Britain (UK Council for Child Internet Safety, 2013a) in order to create a diverse, comprehensive, and current evidence-based research summary and compendium for youth Internet safety (UK Council for Child Internet Safety, 2013c). This guide provides empirical support for best practices in

the areas of social networking, Internet moderation, Internet searching, and chatting/instant messaging (2013c). Its guide, representing publications from academia, government, nongovernmental organizations (UK Council for Child Internet Safety, 2013b), and the technology industry, seeks to “identify, evaluate, and commission new research relevant to child Internet safety” (UK Council for Child Internet Safety, 2013c).

The above organization’s 2013 analysis of the state of the field, submitted for the Child Internet Safety summit (Livingstone & Davidson, 2013), discussed six significant findings. These included: (a) children’s Internet use is largely dependent on a range of contextual factors; (b) Internet use varies greatly across different ages, genders, and socioeconomic factors; (c) better quality Internet access leads to more diverse and dynamic Internet behavior; (d) children engage in a wide variety of risky behavior online, often within the realm of social networking; (e) resiliency of children seems to be related to risk and risk impact; and (f) it emphasized the importance of identifying effective safety strategies in an effort to develop future prevention programs (Livingstone & Davidson, 2013).

One of the most recent and comprehensive studies, featured by the group and completed by the London Grid for Learning Esafety Board, encompassed 17,000 students in the London public school system, grades 3 to 9 (Smith & Warner, 2013). The study concluded that while most children report “having fun” (p. 2) online, and do not regard themselves as in danger in the online space, United Kingdom Internet safety initiatives are having a positive impact in the schools for younger children in the early grades. One compensating factor is that most dangerous situations arise from home use, where children have greater unrestricted Internet access and encounter less supervision, than in schools—the locus of Internet training programs. One key finding of this publication is

that while grades 5 to 6 were considered a “watershed period” (p. 2), the older the students were, the less of an impact their evaluated programs had on their online behavior. Thus, there seems to be a greater need for programs that are effective for adolescents, rather than younger students (2013).

Current research seems to indicate that incidents of cyberbullying have been increasing in recent years. An online poll by leading Internet security firm McAfee, of upwards of 2,000 children and 2,000 adults with at least one child, found that 35% of children between the ages of 11-17 had experienced cyberbullying and 87% had witnessed cyberbullying (McAfee, 2014). This was an alarming increase from 2013, where they found 16% to have been victims and 27% to have witnessed an event (2014). Thus, within the span of a year, cyberbullying victimization more than doubled, and witnessing more than tripled. Their recommendations for best practices for parents included fostering open communication between themselves and their children, having access to their children’s accounts, staying current with new technological trends, using social networks to learn what their children are doing, and helping to manage their children’s online reputation (2014). Research in the past few years has highlighted the importance of open communication between children, their parents, and school personnel, and how important collaborative education and standardized response to cyberbullying can have a significant impact on victims (Snakenborg, Acker, & Gable, 2011).

In 2014, the University of New Hampshire’s Crimes Against Children Research Center published two studies concerning the Internet safety sphere. The first, which dealt specifically with the longitudinal impact of cyberbullying, examined increases in incidents of reported youth harassment over a ten-year span in an attempt to create better

prevention programs. They found that this increase was largely driven by “indirect harassment” (Jones, Mitchell, & Finkelhor, 2013, p. 64), or cyberbullying by two or more people targeting a third party. This is purported to be facilitated by changes in the way youths access the Internet as ease of access increases and online social interactions permeate the offline social space (2013), with victims of this activity experiencing greater social anxiety and being less willing to engage with others.

The second study, a telephone survey of over 1,500 students in the United States ages 10 to 17, and their guardians (Priebe, Mitchell, & Finkelhor, 2013), which targeted online predatory behavior, investigated whether a child responded to “unwanted Internet experiences” by reporting the occurrence to others (p. 1), such as teachers, parents, or friends. These experiences included “unwanted sexual solicitations” (p. 1) and exposure to online pornography, as well as online harassment (2013). They found incidents of harassment reporting to be significantly higher than sexual solicitation, with the lowest reporting numbers representing unwanted exposure to pornography. Perhaps most telling about the findings was what they indicated about the effectiveness of established Internet safety programs: When reporting does occur, only 15% tell a teacher, while between 60-70% disclose to a friend or parent. The researchers stated that their findings seemed to indicate no correlation between increased disclosure rates on the part of the child and parental access to Internet safety information and involvement in their child’s Internet behavior (2013). In fact, in the area of unwanted exposure to pornography, youths actually disclosed less information when their parents had been provided access to Internet safety information (2013). It seems apparent from these findings that existing programs were not persuading children to report offenses. Thus, the need remained for

the development and implementation of programs more effective at increasing child-adult online communication and harassment reporting.

Sexting, Online Predators, and Vulnerability

Recognizing a gap in the research regarding “sexting,” a practice primarily associated with sharing sexually explicit images or videos through text messages, London’s National Society for the Prevention of Cruelty to Children in 2012 commissioned several major universities in London to conduct a qualitative study examining the nature of sexting, why adolescents engage in the practice, the specific dangers involved and, lastly, to produce recommendations for best practices with regard to working with children about the behavior (Ringrose, Gill, Livingstone, & Harvey, 2012). Key findings were as follows: (a) the “primary technology-related threat” (p. 5) comes from peers, i.e., youth use peer pressure to coerce others to engage in the practice; (b) advances in technology accelerate the objectification of girls; and (c) schools must play a role in confronting, easing and compensating for “the gendered sexual pressures on youth” (p. 8) (2012). Recommendations are consistent with those of many other studies in the area of Internet safety, i.e., facilitating open lines of communication both in the school and at home, but goes further in encouraging that the dialogue in schools be more collaborative and that discussions be conducted in a less instructional manner so that ease with what may be a very uncomfortable topic for both students and teachers alike might be increased. They also discussed the importance of including sexting as part of a larger conversation about cyberbullying, addressing teacher embarrassment and the use of small groups for discussion of this issue whenever possible (2012).

Current research concerning the trends in and prevalence of sexting has revealed troubling developments. A major anonymous study of undergraduates at Northeastern

University found that over half of minors had reported sexting before the age of 18 (Strohmaier, Murphy, & DeMatteo, 2014), with approximately 28% of them involving transmission of photographic images (2014). In addition, although most (61%) were unaware that sending images of minors posing in such fashion could constitute “child pornography,” and thus subject the sender to legal consequences, such knowledge resulted in only a modest deterring effect (2014). Researchers discussed how a major shift in adolescent perceptions of privacy and sharing may be indicated by such results, as questionable online behavior, like sexting, may now be considered by teens to be a normal part of adolescent development (2014).

Another study considered the impact on actual incidents of sexual abuse of children of an online behavior known as “grooming” (p. 59), whereby predators cultivate youth over a period of time, using deceptive means to manipulate them into improper relationships (Whittle, Hamilton-Giachritsis, & Beech, 2013). Research on grooming and online predators has identified several risk factors that identify children who might be vulnerable to victimization and, as with cyberbullying, emphasize open communication between children and adults in their lives, as well as encourage a conceptual shift in attitude in today’s use toward Internet life (Dombrowski, Gischlar, & Durst, 2007; Livingston & Palmer, 2012).

Researchers found that the level of childhood “vulnerability” (p. 67) correlated with the impact of the sexual abuse on the victim, as well as on the victim’s experience with professionals after the abuse (2013). Protection, in the forms of both parental support and effective professional intervention, was found to be one of the most important factors in producing more positive outcomes with victims. Recommendations included fostering positive connections between parents and children, especially for

youth considered at-risk and thus vulnerable, i.e., those with a history of depression or self-harm, for example; improving police response so as to make it consistent with best evidence practices; and encouraging victims to have greater involvement with mental health professionals (2013).

A commonly cited 2012 report from the London School of Economics examined the need to clarify the risk factors which contributed to childhood vulnerability online (Livingston & Palmer, 2012). The report resulted in a follow-up effort, a major summit hosted by the UK Council for Child Internet Safety (UKCCIS), in which relevant elements, such as (a) the current state of empirical study, (b) understanding risk and protective factors for children in online activity, and (c) identifying the factors which lead to childhood vulnerability, were discussed. Conclusions suggested that online vulnerability is associated with the types of online services used, the nature of online contacts, the type of content regularly viewed, personal risky behavior, and exposure to advertising (2012). The consensus to which the summit arrived was that the area of most current concern involved the lack of a “holistic model/matrix” to outline the content to which children are vulnerable, the methods by which they are exposed to that content, and the genesis of vulnerability in the spectrum of childhood development (2012).

Incorporating Current Data

Given the fluid nature of media-device, i.e., smartphone, ownership and Internet use, effective Internet safety programs must constantly adapt so that the most recent information available on the Internet and patterns of media device use of children is incorporated. Childwise, a British organization which works closely with the United Kingdom government, releases a comprehensive qualitative survey every January concerning Internet access and use, media ownership and use, and social networking

membership (Duff & Leggett, 2014). This consistently current snapshot of youth between the ages of 5 to 16 examines multiple components of online life, ranging from music downloads, gaming, television viewing, mobile phone usage and application, Internet usage and logistics, and the ways in which children interact between all the above media platforms (2014). The annual updates prove invaluable in assisting Internet safety program developers to target content in a relevant and useful manner.

While the primary focus of research studies concerning Internet safety is, understandably, children, a 2012 study of 1,300 American teachers was published by the National Foundation for Educational Research. This study investigated teachers' Internet safety knowledge, their attitudes toward Internet safety and whether they considered their own online behavior to be safe, and their impact on students (Aston & Brzyska, 2012). Major findings were that most teachers feel their students are safe online at school. Most, however, also expressed concern about smartphone availability, which allowed students to access inappropriate content at school easily, and the extreme challenge such use presents to teachers. Fewer reported confidence that the levels of online safety at school extended to student behavior at home. Lastly, cyberbullying was found to be a major concern for teachers, and many did not know how to respond effectively when it was reported to them or they were otherwise made aware of its occurrence (2012).

WebMD, among the Internet's most often consulted health-oriented websites, published an online guide to help educate parents about Internet safety and facilitate healthy communication with their children. They identified four major "danger" areas of the Internet: cyberbullying, sexual predators, pornography, and damaged reputations (Kam, 2014).

The London-based National Society for the Prevention of Cruelty to Children (NSPCC) has created Safenetwork.org, an online database providing parents with advice on recognizing and preventing cyberbullying, utilizing online security measures, and identifying grooming behavior (NSPCC, 2011). In addition, the organization conducts workshops throughout the United Kingdom on Internet safety, provides assistance for individuals looking to start support groups or training sessions, and recently (January 2015) started a new e-learning course, Child Protection, which is available on their website (NSPCC, 2015a).

Another popular Internet safety program, an e-learning course entitled Keeping Children Safe Online (NSPCC, 2015), is a product of the many recent United Kingdom research efforts and also was released under the auspices of the NSPCC. Available online through the NSPCC's website, the course covers (a) how children currently use the Internet, (b) dangers they face from both their peers and online predators, (c) behavior that puts children at risk for victimization, (d) appropriate responses to cyberbullying and grooming, (e) improving existing online communities, and (f) methods by which current research can impact policy (NSPCC, 2015). Despite the program's comprehensive nature, important components of Internet safety have been largely unaddressed, such as full descriptions of the tools available to online predators; how to evaluate the effectiveness of social networking safety measures; and the ease of which an offender, possessing cursory knowledge of the Internet and available search tools, can target a child and share this easily retrieved information with others. Despite the volume of Internet safety material this organization offers, no information documenting the development of their programs is currently available (2015).

Technology blogs and file sharing websites frequently report on the cutting edge of issues dealing with Internet safety, but the lag between the information being in the public domain—albeit not in widely popular websites—and its inclusion into Internet safety programs is glaring, despite disclosing real and dangerous threats to children who regularly use the Internet. Information that may only be obtained by accessing somewhat obscure sources may prove invaluable in the development of effective Internet safety programs at the forefront of current practices and new technology.

Chapter III

Methodology

Participants

The R Township School District in New Jersey comprises one high school, three middle schools and six elementary schools serving almost 7,000 students. The student-to-faculty ratio is 14.0 and the high school is highly ranked, classified among the top 50 in the state as measured by the New Jersey High School Proficiency Assessment (HSPA) testing and college acceptance rates, according to information provided by the high school guidance office. The target population of the Internet Safety Program was the 83 paraprofessionals employed in the District, all of whom had college undergraduate degrees and substitute teaching certificates and were English-speaking, although some were multilingual (English and Spanish) as well. Paraprofessionals who had no current assignment to a team, school or program, a total of 15, were directed by the District's administration to attend the Program. Participants included nine women and six men between the ages of 25 and 70. All had worked as paraprofessionals for the District for at least one full school year prior to the current one. While paraprofessionals customarily are required by the administration to provide proof of attendance for in-service activity, participants retained confidentiality for the purposes of this Internet Safety Program.

There is no specific demographic information available about the subjects of the study, although they live in the community and are representative of its larger population. According to 2010 United States Census data, the population of R Township is 48.81% White, 24.80% Asian, 20.31% African American, 7.93% Hispanic or Latino of any race, 0.21% Native American, 0.03% Pacific Islander, 3.08% from other races, and 2.77% from two or more races. The median household income in R was \$68,721 and the median

income for a family was \$75,218. Males had a median income of \$47,188; females, \$36,271; the per capita income was \$26,321. A small percentage, 3.8%, was below the poverty line. This included about 2.7% of families, 3.3% of those under age 18, and 4.3% of those aged 65 or over. The poverty level was a weighted average of \$11,137 for a single individual, and a weighted average of \$22,315 for a family of four (United States Census Bureau, 2010).

Procedures

One week before the presentation, an email was sent out to all paraprofessionals in the District announcing the scheduled in-service training and notifying them of the topic of the Internet Safety Program, the logistics of its delivery, and a brief summary of its content. This information was also posted on the District website. For confidentiality purposes, paraprofessionals were asked not to respond to the email announcement; however, consistent with administration policy, as discussed above, the District needed to be aware of the identity of staff members attending in-service training. Participants would be paid their regular salary for the day, as was the custom for in-service training on workdays, with no additional compensation. The administration dedicated a full day for in-service training, February 18, 2013, of which this Program constituted a component. This would allow all subjects to attend at one time and remain for the entire Program duration.

The presentation was given in a lecture hall, which was also, on occasion, used as a cafeteria at the District high school. After a brief introduction by the Presenter (also the researcher), two forms were distributed to participants, a consent form and a pre-assessment survey. Once the completed forms were collected, the researcher introduced the Internet Safety Program. He cautioned participants about the sexually provocative

nature of its verbal and visual content, and notified them that they had the option of being excused from participation if they considered the material offensive or upsetting. None of the participants left.

Consent Form

The consent form (see Appendix B) explained the purpose of the research, the procedures to be undertaken by participants, a description of the Internet Safety Program, information about the in-service component, and the benefits of the study. The form also explained confidentiality provisions, and gave contact information for the researcher and the Institutional Research Board at the university whose oversight includes protection of research participants. In addition, given the provocative nature of Program content, participants were given contact information for sources of support if they experienced any adverse effects resulting from participation. They were instructed that they had the option to decline participation with no penalty and that they would receive a copy of the form for their records.

Pre-Assessment Survey

The pre-assessment survey (see Appendix C) was a questionnaire consisting of five primary questions and 14 related ones designed to assess knowledge relating to the three domains applicable to the presentation, i.e., effective responses to cyberbullying, safe and private online behavior, and knowledge of specific online dangers. Their responses constituted the pretest to determine baseline data about the pre-existing level of knowledge of the Internet Safety Program participants.

Presentation

The Internet Safety Program was delivered as a series of PowerPoint slides, with accompanying commentary, video, graphs, and handouts over the course of two hours.

(See Appendix D for a reproduction of slide content. For the full presentation, see <https://drive.google.com/file/d/0B0c5GnsUFUJDQ1RBanBkVzhBUWM/view?usp=sharing>.) Sources for presentation content included: (a) the concise, familiar, graphical, and comprehensive framework of the *NetSmartz* program (National Center for Missing & Exploited Children, 2012), supplemented by current statistical information provided by Common Sense Media (Common Sense Media, 2013); (b) Internet predator research from the National Society for the Prevention of Cruelty to Children (NSPCC, 2012); (c) a bullying prevention program created by Dan Olweus (Olweus, 1994), (d) the state of New Jersey's Anti-Bullying law (2010, amended 2012); (e) Hinduja and Patchin's cyberbullying research from their work at the Cyberbullying Research Center (Hinduja & Patchin, 2012) and from their own publication (Hinduja & Patchin, 2009); (f) additional cyberbullying research from David-Ferdon and Hertz (David-Ferdon & Hertz, 2007); and (g) personal knowledge of the researcher and his experience with the Internet.

The researcher utilized a microphone amplified by a speaker at the front of the room, and was assisted by a District school psychologist. The Internet Safety Program targeted the three major domains identified as needs by the Director, i.e., responses to cyberbullying, utilizing safety tools and protection, and specific online dangers. Topics covered included cyber bullying; Internet privacy, safety and security; online sharing; and proliferation of sexually provocative pictures and videos; and specific dangers that exist for adolescents on the Internet. Participants were urged to retain the presented information regarding effective responses to instances of cyberbullying, utilizing online safety features, removing identifying information from online profiles, refraining from engaging in the creation and sharing of sexual content on the Internet, learning new ways

of protecting against specific dangers on websites popular with adolescents, and strategies for talking about these topics with students and their children.

The Internet Safety Program content began with an introduction of the researcher who served as presenter (slide 1), an overview of the Program (slide 2), an explanation of specific jargon and terms that were used throughout the presentation (slide 3), and a description of the different levels of public websites referenced over the course of the Program which are rife with unsafe opportunities (slide 4). The Program then proceeded with a discussion of the different ways of accessing the Internet, social media options, and types of video sharing (slides 5-7), followed by “risky online behaviors” (slide 8). Significant time was devoted to the next unit of the Program, bullying. After an introduction (slides 9-10), topics discussed (slides 11-24) included: (a) an explanation of New Jersey cyberbullying reporting laws; (b) differentiating cyberbullying from other types of bullying; (c) identifying incidents of cyberbullying; (d) a description of how information is shared; (e) how to recognize signs in victims or perpetrators; (f) appropriate responses to incidents of cyberbullying, including the reporting responsibilities of staff members; (g) identifying behaviors; and (h) the consequences of cyberbullying, both for victims and perpetrators.

The need for active communication with children was then introduced (slides 25-26). Because of Facebook’s popularity, it was discussed in detail (slides 27-30) and used to represent social media as a backdrop for discussions concerning online behavior and privacy. The researcher then explained how other sites can differ (slide 29).

Appropriateness of online sharing and screen name creation followed (slides 30-31).

The next unit contained a component referred to as the live hunt (the “Live Hunt”), a real, saved demonstration of how information can be pulled together across

different social networking sites through general online searching and limited knowledge of the Internet to create personal profiles of anyone on the Internet (slides 32-58). In addition to providing the user with knowledge about predator techniques and approaches, these slides, with their accompanying commentary, referenced the utilization of Internet protection and security to protect against such dangers. The Internet Safety Program then tackled the use of privacy settings and discussed best practices in that area (slide 59). The discussion on sexting ensued (60-65) which encompassed definitions, prevalence, growing social and cultural acceptance of the practice, and tips on communication to promote safe and appropriate online behavior.

Online predators, the last major content area (slides 66-74), covered identifying online predators; descriptions of predatory behavior; identifying at-risk behavior; testimonials from victims; information on the practice of “grooming”; and best practices in responding to incidents of interaction, including improving communication. The remainder of the Internet Safety Program discussed how to report incidents of behavior presented in the study (slide 75), more tips on fostering open communication and promoting technological responsibility (slides 76-77), an overview of Internet tools facilitating safe use (slide 78), suggestions on establishing rules for student or child Internet use and monitoring (slides 79-82), a discussion about where to find further resources online (slide 83), and information about talking to the community members about best online practices (84). Contact information for the researcher was provided at the conclusion of the presentation (slide 85).

After the slide show portion concluded, a 25-minute question and answer session was held, after which postassessment surveys were completed and collected. The participants then left for their subsequent professional development in-service trainings.

Post-Assessment Survey

Following Internet Safety Program completion, participants were asked to complete a blank survey containing the same questions they had been asked prior to Program presentation. (See Appendix C.) When participants' answers in this post-assessment survey corresponded with content presented during the Program, and those answers had not been present in the pre-assessment survey, they were categorized as "learned responses," i.e., responses attributable to content learned during the Program. Such "learned responses" also constituted "measured responses," indicating that those answers would be included as a component of goal attainment.

Internet Safety Program Evaluation Components

Needs Assessment Protocols

The Director, concerned with what she perceived to be the discrepancies between paraprofessionals' current and desired knowledge and instructional capacity about safe Internet practice, scheduled an interview with the author to identify the targeted needs of a program to be developed to remediate the situation and discuss the topics to be covered in such program. An outcome of this interview was the development of a questionnaire (or survey), designed to both target the identified areas of need and, later, to assess the Internet Safety Program's effectiveness. Thus, the two directives to be achieved were to: (a) establish a baseline of their knowledge about the target area, and (b) reveal the level of knowledge gained as a result of the Program. The questionnaire would be distributed twice: immediately prior to receiving the Program (the Pretest), and then upon the Program's completion (the Posttest). (See Appendix B.)

An outcome of this interview was the development of a questionnaire (or survey), designed to both target the identified areas of need and, later, to assess the Internet Safety

Program's effectiveness. Through the development and presentation of the Program, these needs would form the basis of the instructional support domain of the target population and, as they were addressed, the target population could gain the knowledge necessary to meet such needs. Thus, the two directives to be achieved were to:

(a) establish a baseline of their knowledge about the target area, and (b) reveal the level of knowledge gained as a result of the Program. The questionnaire would be distributed twice: immediately prior to receiving the Program (the pre-assessment), and then upon the Program's completion (the post-assessment). (See Appendix B.)

Topics discussed for inclusion were: (a) time spent online, (b) the types of social networking sites visited and used, (c) access to computers at home and in the classroom, (d) personal information shared across social networking sites, (e) behavior surrounding creation or dissemination of sexually explicit images or videos shared with others on the Internet, (f) webcam use and broadcasting, (g) knowledge about effective responses to cyberbullying, (h) knowledge of privacy settings online, and (i) communication styles when speaking to students about their online use. A comparison of survey responses pre- and post-Internet Safety Program would reveal knowledge gained and, thus, could be used to determine how effective the Program had been. If the Program was shown to have had value in targeting the identified areas, it would then be implemented with other populations, such as teachers, parents, and students in the District.

Goals

Goals, identified through determination of the District, as represented by the Director, addressed the three specific areas delineated as identified needs in the domain of instructional support. Goals 1-3 requested a single response from paraprofessionals, whereas for goals 4-9, the district had determined that at least two learned responses were

appropriate. Listed below are the areas to be addressed (in italics) along with their accompanying goals.

☛ *What information did paraprofessionals need to learn to deal effectively with instances of cyberbullying?*

1. Paraprofessionals would be able to identify the response of reporting incidences of cyberbullying to a superior.
2. Paraprofessionals would be able to identify the responsive act of saving any and all information from the cyberbullying event.
3. Paraprofessionals would be able to identify the responsive procedure of referring the victim to the correct support.

☛ *How could paraprofessionals help their students learn to practice safe and private online behavior?*

4. Paraprofessionals would be able to list two safe practices as outlined in the presentation about effective use of privacy controls on Facebook.
5. Paraprofessionals would be able to list two safe practices as outlined in the presentation about username/password generation as it pertains to behavior across frequented social networking sites.
6. Paraprofessionals would be able to name two safe practices as outlined in the presentation about action they can take immediately to improve their own safety and that of their students online.

☛ *What information did paraprofessionals need to possess awareness of specific dangers that exist in the online community?*

7. Paraprofessionals would be able to name two websites that are frequented by online predators.

8. Paraprofessionals would be able to name two methods that online predators use to groom children.

9. Paraprofessionals would be able to name two actions a typical student can take immediately to decrease their exposure to online predators.

Treatment of Data

Consent and Assessment Forms

The consent and survey forms were kept in a locked file cabinet at the home of the researcher. No one other than the researcher has access to this information. Each participant was assigned a code in order to keep his/her name confidential.

Data Collection

This study utilized survey questionnaires as the method for obtaining data from subjects directed by the District administration to participate. Each subject received the same survey questions. The questions were both closed and open ended and, at the conclusion of the Presentation, participants had the opportunity to address any related issues.

Goal Attainment

Goals were constructed pursuant to the purpose of the Internet safety program: that paraprofessionals in the District respond to students' online behavior issues in a coordinated and appropriate manner. Goals 1-3 relating to cyberbullying were straightforward—the goal was the same as the desired response. For goal 1, both the goal and the desired response was that cyberbullying incidents be reported to a superior. For goal 2, both the goal and the desired response was that all information from the cyberbullying attack be saved. For goal 3, both the goal and the desired response was that the victim be referred to the proper source of support within the school district. Thus, for

the first three goals, **one response reflecting specific program content, or one “measured response,” would constitute goal attainment for goals 1-3.**

The goal and the desired response were not equivalent for the next series of goals, goals 4-6, involving safe and private online behavior (goal 4: effective use of privacy controls on Facebook, goal 5: username/password generation across a social media landscape, and goal 6: improving their own safety and that of their students online), and goals 7-9, involving specific dangers in the online community (goal 7: knowledge of websites frequented by online predators, goal 8: methods of grooming, goal 9: actions students can take to decrease exposure to online predators). Rather, training content offered multiple suggestions for responses. Given those circumstances, **two responses reflecting specific program content, or two “measured responses,” would constitute goal attainment for goals 4-9.**

Categories of Responses

Two categories of responses, “incoming knowledge,” and “learned responses” constituted “measured responses.” Both reflected Program content, counted equally as “measured responses,” and were distinguished as follows:

“Incoming knowledge” indicated desired knowledge possessed by a participant prior to the training that was also imparted by the training, as was reflected in the pre-assessment survey. Prior to the training, participants possessed varying levels of knowledge about Internet safety as was indicated in the pre-assessment survey. When a response in the pre-assessment survey was also a desired response in the post-assessment survey, such pre-assessment response was classified as “incoming knowledge.”

“Learned responses” indicated desired knowledge gained during the training not present prior to the training, as was reflected in the post-assessment survey.

When a desired response that had not been given in the pre-assessment survey was given in the post-assessment survey, this knowledge was deemed to have been gained as a result of the training and was thus classified as a “learned response.”

“Measured responses” indicated participants possessed desired knowledge contained in the training, reflected in pre-assessment surveys as “incoming knowledge” or post-assessment surveys as “learned knowledge.” The Director’s primary concern was that paraprofessionals possess the desired knowledge of Internet safety as demonstrated by achieving the nine goals listed above. If content was included, defined, or explained in the body of the Program, any survey responses from participants reflective of that targeted information was considered to be a “measured response.” Thus, when a participant responded to a question in the pre-assessment survey reflecting content also present in the training, this “incoming knowledge” constituted a “measured response.” Similarly, when a participant responded to a question in the post-assessment survey reflecting content present in the training, this “learned response,” constituted a “measured response.”

There were some instances in which participants’ responses were not reflective of Program content but may very well have been appropriate, and may have even contributed to better Internet safety health. However, as they had not been arrived at as a result of the Program or been contained within Program content, they were not included as a “measured response.” For example, the researcher described how to identify cyberbullying and instructed participants to report incidents to a superior. One of the survey questions concerned how to respond to an incident. The measured response

reflected the Internet Safety Program content, i.e., “report the incident to a superior.” However, some participants also listed additional responses such as “talk to the victim to make them feel better,” and “refer them for counseling.” Whereas both responses could be considered appropriate and could be especially helpful methods of assisting a victim process and heal from an incidence of cyberbullying, neither qualified as “measured responses” and only “measured responses” captured knowledge contained in the Program, and thus counted toward goal attainment.

Because of the nature of the questions, the topic area, and the emotional impact the information presented may have had on the participants with personal experiences related to Internet safety, it was not unreasonable to expect responses to vary from Program content. For example, the section about online predators resonated in an emotionally striking and personalized way with some of the participants, eliciting responses such as “Deactivate my son’s Facebook account!” or “Monitor all of my students’ behavior all the time!” Again, these answers, albeit reactionary, could be considered effective responses at limiting exposure to online predators; however, as they were not included in the Program’s content, they were not considered to be “measured.” In this case, as in the case above, only “measured responses” could be counted toward goal attainment.

Data Analysis

The data analysis served to describe and summarize the data obtained through the surveys, identify relationships between the variables (receiving the Internet Safety Program and knowledge attainment), and forecasted outcomes of the Program. Data included knowledge captured in the pre-assessment and post-assessment surveys. The pre-assessment survey (see Appendix C), delivered to subjects before exposure to the

Program, was meant to capture any knowledge related to the identified domains that subjects possessed before exposure to the Internet Safety Program. The post-assessment survey (see Appendix C), delivered to subjects after the Program, was meant to capture knowledge gained as a result of the training and measured the extent to which the presented information had been retained by the participants.

The requirements for inclusion in the study were as follows: (a) participants were paraprofessionals working in the District; (b) they were present during the in-service event in which the Internet Safety Program was delivered; and (c) they completed surveys prior to the Program and upon its completion. All 15 paraprofessionals completed the pre-assessment survey, but one failed to complete the post-assessment survey. Thus, the results included the 14 paraprofessionals who had completed both tests ($n=14$).

Pre-assessment information analyzed the number of valid responses as “incoming knowledge” as well as “measured responses,” as participants who had not yet been exposed to the Program had pre-existing awareness of information in the Program’s targeted knowledge base. Post-assessment analysis referred to “measured responses” provided by participants which indicated the absorption of new knowledge as a result of the Program. “Measured responses” listed for each individual participant were tallied and separated by survey.

Each of the nine goals, described above, were measured separately. Chapter IV, Results, provides an analysis of participant responses that correlated with information contained in the Internet Safety Program, i.e., “measured responses,” and whether a number of measured responses given by individual participants was sufficient for goal attainment, as some goals required one measured response and others required two.

Descriptive data analysis was used to describe the results after comparison. Percentages of subjects satisfying the individual goal areas were compared to provide a simple assessment of how the subjects performed in each of the nine goal areas.

Descriptive Data Analysis

As indicated above, two types of valid “measured responses” were counted in the descriptive analysis: “incoming knowledge” and “learned responses.” “Incoming knowledge” pertained to “measured responses” present in the pre-assessment survey, i.e., a participant was previously aware of targeted information before exposure to the Internet Safety Program. “Learned responses” pertained to “measured responses” presented in the post-assessment survey, i.e., a participant was aware of targeted information after the Program’s completion.

For each of the nine goals, three percentage scores were calculated in each area of analysis. Firstly, the percentage of participants who responded with “measured responses” on the pre-assessment survey, reflective of previous knowledge in an area, or “incoming knowledge,” was tallied. Secondly, the percentage of participants who answered with “measured responses” on the post-assessment survey was tallied, reflecting gained knowledge in an area, or “learned responses.” Next, the percentage of participants whose responses corresponded to the individual goals set with the client was tallied. This figure, provided for the client’s use, was used to determine whether the Internet Safety Program was successful in meeting the District’s indicated need. Lastly, an overall percentage score was obtained, indicating a combined score of how many of the nine goals were achieved by all of the participants.

In conclusion, for each individual goal, the three percentages were described and listed. “Learned responses” or “measured responses,” as provided in the post-assessment

survey, were considered to be an important measure related to the Internet Safety Program's value, as it was an indication of the level of information assimilated by participants. "Incoming knowledge," captured by the pre-assessment survey, was a measure of what participants already knew. The level of "incoming knowledge" had no bearing on goal attainment. Goal attainment was judged on the basis of the knowledge criteria provided by the Director, and determined only after completion of the Program presentation.

Chapter IV

Results

Internet Safety Program Target Areas and Goals

The Internet Safety Program was designed to deliver content and knowledge in nine target areas that corresponded to the specific goals, as discussed above in Chapter III, Methodology. Each area, measured separately, was matched with slides which delivered corresponding content. Post-assessment surveys were intended to capture “learned responses.” “Measured responses” were “learned responses” only when such responses reflected information acquired during the Program’s presentation that had not been known prior to presentation.

Discussions of identified need with the Director had been based on best practices in the area of responses to cyberbullying, exemplified in programs developed from *NetSmartz* (National Center for Missing & Exploited Children, 2012) and in information presented by the Cyberbullying Research Center (Hinduja & Patchin, 2009, 2010, 2015).

Goals 1-3: Responses to Cyberbullying

Slides 9-25 described cyberbullying and presented numerous methods of identifying, responding to, and processing events both as they occurred and when witnessed by, or reported to, a school staff member. (See Appendix D for a reproduction of slide content. For the full presentation, see:

<https://drive.google.com/file/d/0B0c5GnsUFUJDQ1RBanBkVzhBUWM/view?usp=sharing>.) Cyberbullying was distinguished from general bullying, and the recent New Jersey state law on harassment, intimidation, and bullying (Anti-Bullying Bill of Rights, 2010) (New Jersey Department of Education, 2015), enacted in part, in response to the prevalence of incidents of cyberbullying, was described in detail. Several slides focused

on the speed at which cyberbullying threats can spread, the harm it can cause to victims, the legal consequences to perpetrators, and how to identify victims of cyberbullying.

Goal 1: Reporting incidents of cyberbullying to a superior. In accordance with New Jersey law, District policy compels staff to report incidents of cyberbullying to a superior. Slide 19 presented this information to the participants, directing them to notify a superior of any and all incidents.

All of the subjects (100%) listed the identified response in both pre- and post-assessment surveys, indicating that this was “incoming knowledge” for each participant. Thus, no subjects (0%) gained any knowledge in this area. One hundred percent of subjects supplied the “measured response,” and every paraprofessional met the area’s goal.

Goal 2: Saving any and all information from the cyberbullying event.

Beyond District policy, discussions of identification of needs with the Director with respect to cyberbullying represented the consensus of District administration, District police responders, and *NetSmartz* and Cyberbullying Research Center literature as the best practices in response to a cyberbullying incident: saving all information from the event, and encouraging the victim to seek further support by making referrals to such sources. The first best practice was exemplified in goal 2—participants were directed to save any and all digital information involved in a cyberbullying incident (slide 18). The second best practices response, i.e., referring victims for further support, became a component of goal 3, discussed below.

Of the 14 participants, only one (7%) showed “incoming knowledge” in this area in the pre-assessment survey. Two participants (14%) in the post-assessment survey showed “learned responses.” Thus, there were three (21%) “measured responses.” For

this goal, only a small number of participants gained knowledge about saving information.

Goal 3: Refer the cyberbullying victim to the proper support within the district. As discussed above in goal 2, a referral for support was considered one of the two best practices in helping a victim respond to an incident of cyberbullying. Slide 19, in addition to providing information about reporting to a supervisor, advised the participant to direct the victim to a school staff member who could provide emotional and administrative support. (This is distinct from a referral to an outside source, which would not be in the purview of a paraprofessional’s responsibilities.) Goal 3 was that the participant would gain knowledge about sources who could be of further help to cyberbullying victims within the school structure.

Of the 14 participants, six (42%) showed “incoming knowledge” on the pre-assessment survey, identifying the response of referring a cyberbullying victim to proper support. On the post-assessment survey, two participants (14%) indicated “learned responses.” Thus, eight participants (57%), or more than half the sample, were able to provide “measured responses” and able to meet the demands of this goal.

Goals 4-6: Safe and Private Online Behavior

Slides 2-8 and 26-65 presented great deal of varied, specific, and targeted information geared toward safe and private online behavior. Early slides featured definitions and descriptions of social media, online privacy terms, and methods of Internet communication. Different types of risky online behaviors were presented, as well as specifics about privacy settings and anecdotes representative of the dangers of sharing information online. This section also included the Live Hunt demonstration, as discussed

above, concerning how information posted across different social media platforms can be pooled together, resulting in an extremely detailed and revealing profile of an individual.

The targeted areas upon which the goals were based were mentioned several times in the presentation. Goals in this area were looking for two “measured responses” to each question which reflected specific information presented in the Internet Safety Program.

Goal 4: Effective use of privacy controls on Facebook. As the most widely used and accepted form of social media on the Internet, Facebook was a major focus in this area and featured heavily in the slides with accompanying commentary. Accessing privacy controls, a recurring theme throughout this area, was discussed in detail in slide 59, and several examples of best practices were presented, including: (a) setting a profile to “friends only,” (b) closing a profile to outside searches, (c) not using full names, (d) limiting post and “timeline” exposure, (e) being discriminatory about providing personal contact information, and (f) limiting the setting and nature of photos and videos shared on the website. Goal 4 was to receive two “measured responses.”

Of the 14 participants, 8 (57%) reflected “incoming knowledge” in this area on the pre-assessment survey. Regarding responses on the post-assessment survey, nine participants (64%)—almost two-thirds—exhibited “learned responses” by providing unique “measured responses” in the follow-up survey that were not present in their original survey responses. Those nine participants met the goal of providing two “measured responses” in the area of knowledge of Facebook’s privacy controls.

Goal 5: Username/password generation across a social media landscape.

While Facebook may have the most total users, numerous other social media websites are frequented by children, adolescents, and adults. The Internet Safety Program provided detailed information about how best to navigate username and password generation

across the social media landscape to avoid specific online risks (although it should be noted that the dangers listed below may be as a result of online activities other than use of social media websites). Such risks include: “phishing,” defrauding an online user financially by illegally posing as a legitimate company (Oxford United States English Dictionary, 2015); malware, software meant to damage or hijack computers or networks (Oxford United States English Dictionary, 2015); and identity theft. Slide 31 primarily features information in this area.

Of the 14 participants, three (21%) provided responses that indicated “incoming knowledge” in this area on the pre-assessment survey. Subsequently, 10 (71%) offered at least one “learned response” on the post-assessment survey, and a total of five (36%) met the goal of presenting at least two “measured responses” in the area of username/password generation techniques . While approximately one-fifth of the subjects possessed some “incoming knowledge” in this area, the majority were able to offer a “learned response” in the targeted area. Despite this gain, however, the goal was to provide two responses reflecting targeted information in the presentation and fewer than half were able to meet the goal. Two participants (14%) provided no “measured responses” and five (36%) provided one.

Goal 6: Improving their own safety and that of their students online. Among the methods of achieving the goal of safe and private online behavior was to personalize the experience for participants by asking them to provide information on how they could improve the safety of their own online presence and that of students. “Measured responses” on the pre-assessment survey constituted the application of previously acquired knowledge about safety to their own online life and included responses that were indicated in goals 4 and 5.

Of the 14 participants, three (21%) provided responses in the pre-assessment survey indicating “incoming knowledge,” and 11 (79%) responded with at least one “learned response” in the post-assessment survey. However, subjects were required to provide two answers to meet this goal and the presentation had offered dozens. Seven participants (50%) met the goal of providing two “measured responses” for the sixth goal, and five (36%) provided one “measured response” but failed to meet the goal of two.

Goals 7-9: Addressing Specific Dangers in the Online Community

Slides 3-4 and 66-77 discussed dangers specific to the Internet, concentrating on online predators. Participants were alerted to the different ways in which predators groom their victims, the tools they use across social media, and the websites they frequent where information and images are shared with others. Slides, with accompanying commentary, also addressed identifying victims and prevention techniques to help students from exposing themselves to predator threats. Tools, such as reporting sources and tiplines, were also provided to assist victims in obtaining professional help (National Center for Missing & Exploited Children, 2012).

As with goals 4-5, a great deal of information was presented in these slides and targeted areas were mentioned several times in the presentation. Participants were to reference two “measured responses” for each goal.

Goal 7: Knowledge of websites frequented by online predators. A crucial component of the Internet Safety Program was to help educate participants about areas of the Internet that were little known and far more dangerous than the immensely popular websites with which most were familiar. Here, participants were exposed to examples of the darker sides of the Internet. Slides 3 and 4 dealt specifically with jargon used in the world of online predators, the websites which form the base of their activities, and the

skill set they possess which facilitate the ease in which children can be tracked and lured. Subjects were asked to provide examples of websites frequented by online predators, and the goal was the inclusion of two “measured responses.”

Of the 14 participants, eight (57%), or more than half, provided responses on the pre-assessment survey indicating “incoming knowledge” in the area of websites frequented by online predators, and nine (64%) indicated “learned” knowledge in this area by providing information targeted in the Internet Safety Program on the post-assessment survey. Across the two surveys, 11 participants (79%) met the goal of providing two “measured” responses in this area.

Goal 8: Methods of grooming. The practice of “grooming,” i.e., luring victims, over time, into a false sense of security with the predator who then preys on that relationship to do harm, was the subject of several of the later slides about online predators, and was a main focal point of the third area of the Internet Safety Program. For this area, subjects were asked to provide examples of methods used by online predators to groom children. Answers containing two “measured responses” were considered to have met this goal.

Of the 14 participants, nine (64%) presented answers that indicated “incoming knowledge” on the pre-assessment survey. Subsequently, seven subjects indicated “learned responses” on the post-assessment (50%). Seven (50%) of the participants, were able to meet the goal of providing two “measured responses” in this area. Five participants (36%) presented one “measured response,” and two (14%) were not able to provide any “measured response” in this area.

Goal 9: Actions students can take to decrease exposure to online predators. The last focal point of the slides relating to online predators concerned preventative

actions students could take to reduce their risk of exposure. Many slides and their accompanying commentary presented examples of prevention practices that participants could discuss with students in the classroom.

Of the 14 participants, 13 (93%) presented answers that indicated “incoming knowledge” on the pre-assessment survey. In addition, six (43%) participants referenced information not known at the time of the pre-assessment survey, thus generating “learned responses” on their post-assessment survey. Eight (57%) participants met the area’s goal of providing two “measured responses” in the area of actions to prevent online predator victimization.

Summary of Goal Attainment

All of the 14 participants (100%) met goal 1 of reporting cyberbullying to a superior; 21% (three participants) met goal 2 of saving any and all related digital information; 57% (eight participants) met goal 3 of referring victims to their current and identified support; 64% (nine participants) met goal 4 of mentioning two safe practices on Facebook; 36% (five participants) met goal 5 of reporting two identified methods of protecting username and passwords across social media; 50% (seven participants) were able to meet goal 6 of providing two methods of improving personal safety online; 79% (11 participants) met goal 7 of naming two websites used by online predators; 50% (seven participants) were able to meet goal 8 of providing two grooming methods used against children; and 57% (eight participants) met goal 9 of naming two practices children could take to improve their protection or behavior against online predators.

Grouped by domain, 59% of participants met goals relating to cyberbullying, 50% met goals relating to privacy and security on social media, and 62% met goals relating to specific dangers in the online community and online predators. Of all the goals

combined, 57% were attained by the subjects in this survey. This figure was arrived at as follows: these subjects attained 72 out of the maximum achievable goals of 126 (nine goals for each of 14 participants), or 57%.

Online Habits and Trends

In addition to the nine goals, participants were asked questions about their exposure to, and familiarity with, the Internet, such as how much time they spent online per day, what social media sites they visited, how many computers were present in the home and in what locations, and what type of information they shared online.

Five participants reported spending an hour online per day and two participants reported spending two hours per day online. None of the remaining participants gave the same answer as another participant. Their responses were, respectively, “varies, with a 2 hour limit,” 1-2 hours, 1½ hours, 40 minutes, 20-30 minutes, “occasional” use, and one reported zero use.

Regarding social media sites visited, the only two reported by subjects were Facebook and Instagram. Seven reported visiting Facebook, of the two who reported frequenting Instagram, one used Instagram alone and the other used both Facebook and Instagram. Six reported visiting no social media sites at all.

Participants provided varied answers about how many computers were present in their homes and their location within the home. Seven participants reported possessing one computer in the home, and locations were listed as in the “den,” “basement,” “office” and “living room,” with three respondents omitting location information. Four participants responded with an answer of two computers, with locations in the “family room and laptop [i.e., no set location],” “bedroom and family room,” and “family room and game room.” The two participants who spent 2 hours online per day did not provide

information as to the number of computers in the home or their location. One participant listed five computers in the home, which were located in the “living room and bedrooms.”

Regarding shared information by subjects online, eight participants answered that they do not share anything online. All who shared specifics listed their name (six participants); one listed “name and cell”; one provided “name and family”; another responded “name and places visited”; one listed “name, family, and school”; and the last reported “name, cell, address, family names, and school.”

Chapter V

Discussion

The motivation for the development of any software program, such as an Internet safety program, is to address a need which is not being met adequately by existing products. The author of this study has had considerable experience with and exposure to technology, Internet security, and developing online trends both in cultural behavior and social responsibility. It was his observation that that the publicly available Internet safety programs were deficient in content and breadth. Even empirically supported existing programs, like *NetSmartz* (National Center for Missing & Exploited Children, 2012), lacked features essential to functionality.

Security controls on widely used websites, such as Facebook, can change as often as weekly. Underground networks of Internet criminals adapt readily to developing technology, cybercrime legislation, and methods of law enforcement. While *NetSmartz* provided an adequate baseline of information and structure of content delivery, rapidly changing online behavior and trends exposed its limitations, especially in the area of safe and private online behavior. In such vacuum, a program that could combine the baseline knowledge of *NetSmartz* with the nuanced depth and experience of an Internet expert, such as the author of this study, could prove exceptionally valuable. It was his intention to develop such a program.

The hallmark of the Internet Safety Program was the Live Hunt, as discussed above, a 26-slide depiction of the Internet as a powerful search and profiling tool with seemingly endless possibilities and dangers. Starting with a Google search, the demonstration explored how an Internet user, with only basic knowledge of how the Internet works, could gather information across different websites and social media

outlets to create a comprehensive profile of a target. A woman, whose facial features were blocked and identifying information redacted, was selected at random to follow through a *private* and *protected* Facebook page to reveal extensive information about her, including her address, cell phone number, aerial pictures of her neighborhood, and a photograph of her house and car. Although the primary purpose of this presentation was to deliver helpful and accurate content, it was also designed to make an emotional connection with the participants and, thus, elicit a greater level of care and focus than would typically result from participation in such a program.

Information Gathering

The first step in analyzing the value of any program is to set some simple goals in the areas of identified need in the target population. Once the District's administration identified the areas of need, development of goals corresponding to the identified needs began. In this case, three areas of identified need were accompanied by nine goals, as discussed above. A slide presentation containing the required content related to each area was prepared. Although slides available from the *NetSmartz* Internet safety program (National Center for Missing & Exploited Children, 2012) were source material for many of the slides, they were supplemented with content presented by the Cyberbullying Research Center (Hinduja & Patchin, 2009, 2015), the National Society for the Prevention of Cruelty to Children (NSPCC, 2014), and from the researcher's own extensive knowledge base.

As an exploratory study, descriptive statistics were employed to analyze participants' responses, delineated as reflecting "incoming knowledge," "learned responses," and "measured responses." Ascertaining "incoming knowledge" was made more difficult due to the derivation of the Internet Safety Program: it was developed

during a process involving a school district administrator (the Director) and the author of this study without a formal needs assessment, and no interaction had occurred between the participants and the Program developer prior to the presentation. Constructing a needs assessment without any input from the pool of participants from whom needs could be identified may limit the effectiveness of any program delivery.

Although “incoming knowledge” was a major factor in data analysis, and the researcher had no opportunity prior to the Internet Safety Program’s commencement to ascertain participant knowledge, the category of “learned responses” distinguished between information already known by a participant, as reflected in the pre-assessment survey, and information specifically acquired from the Program, as reflected in the postassessment survey. The sole input constituting goal attainment status—“measured response”—made no distinction between information known before, i.e., “incoming knowledge,” and that known after Program presentation, i.e., “learned knowledge.” Therefore, goal attainment could not be attributed to the effectiveness of the Program content as the participant could have gained the desired knowledge in an identified area at any prior point. “Incoming knowledge” and “learned responses” were identified and differentiated, but only insofar as “learned responses” were unique to the participant. Goals were considered to be met if the total amount of “measured responses” met or exceeded the target number.

Value of the Internet Safety Program

The main focus of developing the Internet Safety Program was to create value for the participants. Value is achieved when (a) a specific need in a domain is identified, (b) those needs are addressed with developed goals, and (c) changes in knowledge with respect to the domains, reflecting needs being met, have been evaluated.

A formalized needs assessment is the preferred method for identifying needs. In the case of the present study, a formalized needs assessment would have started with a survey distributed to the target population before program development. The results of the survey would then form the basis for need identification. Had this method been pursued, direct input from the pool of potential participants would have eliminated much of the guesswork and, thus, would have been ideal for capturing their specific needs. Although the Internet Safety Program developer made his preference for a formal needs assessment clear, discussions with the Director made it evident that this was not feasible, primarily due to barriers presented by District directives, as well as professional restraints and logistical challenges. The conclusion was reached that the best needs assessment method available would be a survey conducted with administration, in the person of the Director.

The Director expressed to the author of this study her interest in the professional development of staff members and sought, on previous occasions, his participation as a presenter, particularly in his area of expertise, technology. In this instance, the Director and other decision makers in the District had long been troubled by issues arising out of student activity on the Internet, among them cyberbullying; incidents of “sexting”; student reports of being targeted by anonymous harassers and predators online; and oversharing on social media sites, such as Facebook, that led to serious problems at school. Paraprofessionals, who have a great deal of contact with students, were considered by the Director to have little ability to offer assistance in the area of Internet safety because of their own lack of knowledge concerning Internet use.

As District employees, the competent and helpful work exhibited by paraprofessionals benefit not only students and their parents, but teachers, other school

and administration personnel, and members of the community. Identified need in a population of paraprofessionals in the area of Internet safety would add value for each of those groups: paraprofessionals would increase their knowledge base in a topic that is not only important for their careers but increasingly essential in today's world; the students they work with would learn appropriate practices in Internet behavior, as well as helpful intervention and effective prevention; the student body as a whole would benefit when safer behavior online results in a safer school experience; and the administration would benefit as fewer behavioral and social issues arising from online activity would diminish crisis situations.

The District administration's goals concerning the knowledge paraprofessionals should possess about domains in Internet safety corresponded with what they identified as problematic behavior among students. In addition to the offenses listed above, i.e., cyberbullying, "sexting," confrontations with anonymous harassers and predators, and oversharing on social media sites, recent state legislation (the Anti-Bullying Bill of Rights Act, 2010) made them aware of possibly serious implications for the administration were they to leave incidents of harassment, intimidation, and bullying unaddressed or improperly addressed.

The domains of response to cyberbullying, safe and private online behavior, and responding to specific dangers that exist online were developed to best address the identified need that arose from discussions with administration. Increased, measureable knowledge in those areas would have the intended effect of providing value for paraprofessional participants, the students with whom they work, and the administration as a whole. In addition, some in the administration were enthusiastic about the prospect

of a program that could eventually be expanded and delivered to teachers, other staff members, students, and parents.

Measuring Value: “Learned Responses” and Goal Attainment

As this was an exploratory study, descriptive statistics were employed in data analysis to assess for change in the identified domains. While not as comprehensive and statistically significant as a formal statistical analysis, descriptive statistics were useful in helping Internet Safety Program evaluators understand where the Program provided the most value in terms of goal attainment. There were two ways in which the Program could prove value in such manner: Either a high level of “measured responses” would demonstrate goal attainment through participant competency in the domain irrespective of the derivation of knowledge, or a high level of “learned responses” would demonstrate goal attainment through Program effectiveness in imparting knowledge in the targeted area. Goal areas that produced measurable “learned responses” indicated that the participant learned desired knowledge in a targeted domain and, as reflected in the postassessment survey, was able to transmit that specific content back to the researcher, as only unique and targeted responses were counted. Goal areas that generated higher percentages of met goals provided value as they helped ensure that participants in the study achieved the standard set by the client.

The goals individually provided varying amounts of value, assessed by the measured values of “learned responses” and goal attainment. Goals in the domain of cyberbullying offered solid value insofar as “measured” or targeted knowledge was the criterion, however, this domain did not capture many “learned responses.” The first goal, reporting cyberbullying events to a superior, was met with 100% accuracy in the pre-assessment survey—a figure impossible to improve upon. Even though no “learned

responses” were capable of being achieved through Internet Safety Program delivery, such high goal attainment provided value by confirming that the target population is equipped with productive knowledge in this area. The second goal, which involved the act of urging victims to save all information related to a cyberbullying incident, had very low measures of both “learned responses” (14%) and “measured responses” (21%). The pre-assessment survey did not reveal significant incoming knowledge, nor did many participants gain the knowledge as a result of Program delivery. Thus, few participants met the goal. The third goal, referring the cyberbullying victim to the proper support within the district, fared a bit better, as 57% of participants met the goal of providing the intended “measured response”; however, the level of “learned responses” (14%) was low. This again indicated that the Program provided value here by affirming that more than half of the participants possessed the intended knowledge in this area, although not necessarily as a result of Program delivery.

The next goal area, involving safe and secure online practices, saw more consistent value across the areas of “learned responses” and goal attainment, even when accompanied by high “incoming knowledge.” Almost two-thirds of participants (64%) showed “learned responses” in addition to meeting the goal of listing two “measured responses” in the area of Facebook privacy settings. This was noteworthy as more than half of the participants displayed “incoming knowledge” in this area, indicating that even when subjects had some prior knowledge in an area that aligned with targeted program information, they still were able to show growth and meet the area’s goal. The next goal, involving username/password generation and safety, saw similar numbers in terms of “learned responses” (71%) but lower goal attainment (36%). This was coupled with far less “incoming knowledge” (21%), which may allow the logical conclusion to be drawn

that goals were more easily achieved when participants exhibited more “incoming knowledge” in an area. The third goal in this area, targeting changes a participant could make personally to improve his/her own safety and security, was again met with higher amounts of “learned responses” (79%) following lower levels of “incoming knowledge” (21%). Half of the participants (50%) achieved the goal, listing two “measured responses.” This again indicated that when paraprofessionals showed little “incoming knowledge” and high numbers of “learned responses,” the goal attainment numbers seemed to decrease as the criterion for meeting a goal was two “measured responses” which was less easily attainable when participants lacked prior knowledge. This goal seemingly provided good value in the area of teaching participants new information; however, when attempting to measure for a specific standard, i.e., two “measured responses,” the results were mixed.

The last goal area included in the data analysis addressed dangers specific in the online community. This area saw fairly consistent levels of “learned responses” and goal attainment, but also featured the highest consistent levels of “incoming knowledge.” The seventh goal asked about knowledge of websites frequented by online predators, and saw a high percentage, 64%, provide “learned responses” and an even higher number meet the goal of listing two websites (79%). More than half indicated “incoming knowledge” as well. This goal seemingly provided good value both in terms of teaching ability and ensuring a knowledge standard. The next goal, which dealt with online predator grooming methods, resulted in half of the participants gaining knowledge (50%) and half reaching the goal (50%), showing somewhat mixed results in terms of providing value as 64% possessed incoming knowledge. The last goal, addressing actions that students can take to decrease exposure to online predators, presented with an extremely high amount

of incoming knowledge (93%). While 43% provided “learned responses,” 57% met the goal of providing two responses.

All areas produced varying levels of “learned responses,” which indicated that the Internet Safety Program provided value in passing on targeted information to participants, other than the first goal concerning cyberbullying, wherein all participants demonstrated the desired knowledge prior to Program delivery with their performance in the pre-assessment survey. Regarding goal attainment, on average, about half of the participants met the intended goals per area with the exception of 100% for goal 1, as discussed above. In terms of assessing for a baseline of desired knowledge, some value was present, but the Program’s effectiveness was more evident in improving the raw knowledge of participants.

“Incoming Knowledge” Vs. “Learned Responses”

The dichotomy between “incoming knowledge” and “learned responses” provided some interesting insights when reviewing the effectiveness of the Internet Safety Program. Both contributed to goal attainment, as the goals developed with the District’s administration measured whether or not participants possessed the targeted information. From the client’s perspective, goal measurement was paramount. Consistent with such priority, no distinction was made in determining whether goal attainment was a result of “incoming knowledge” or “learned responses.” Both were treated equally.

When comparing “incoming knowledge” with “learned responses” as factors in goal attainment, the results presented as unclear. Some goals seemed to depend entirely on “incoming knowledge,” while others were met through high levels of “learned responses.” The first goal, reporting incidents of cyberbullying to a superior, was achieved entirely through “incoming knowledge.” Other goals, such as goal 2 (saving

information), produced very low “incoming knowledge,” but also low goal attainment. These examples could indicate that, for some goals, “incoming knowledge” was the greatest indicator of goal attainment.

Other goals did not present as clearly. For example, goal 5, username/password generation, produced high “learned responses,” but relatively low goal attainment. Still some subsequent goals seemed to have an additive effect: goal 7, knowledge of websites frequented by online predators, had both moderately high “incoming” and “gained” knowledge (57% and 64%, respectively), and higher goal attainment (79%). The ninth goal, actions students can take to decrease exposure to online predators, seemed somewhat anomalous: 93% presented with “incoming knowledge,” 43% showed “learned responses,” yet only about half (57%) met the goal of two “measured responses” with respect to actions students can take to decrease exposure to online predators.

As has been stated previously, a more comprehensive needs assessment could have greatly relieved evaluative issues. A survey of the target population could have identified “incoming knowledge” in advance, and thus refine the set of goals so that they would exclusively result from “learned responses.”

The Utility of “Measured Responses”

One of the key components of this Internet Safety Program was the “measured response,” as discussed above. The Program contained a great deal of content across the three listed domains. The surveys were designed to measure how that information was assimilated, looking for inclusion of information, advice, and examples, unknown by participants prior to the Program, that had been drawn from the Program presentation. A response reflecting such situation would constitute not only a “learned response,” but a “measured response” as well.

Despite the breadth and comprehensiveness of the Internet Safety Program, the targeted domains of Internet safety lent themselves to far more information, much of it helpful and appropriate, than could be contained in the presentation. Participants' responses, which may very well have been correct in their real-life application, were not counted toward goal attainment as they were not "measured responses": the content was not specifically presented in the Program. This may have been a major weakness of this study given the intention of creating the Program: enable staff members who work closely with students to respond to issues arising out of online activity in an appropriate and helpful manner—qualities which may prove to be subjective and individualistic.

In addition to other possible responses, the Internet Safety Program itself tended to elicit an emotional reaction in the viewer. Some of the information presented, specifically in the Live Hunt component of the safe and private online behavior domain, visibly affected some participants and caused emotional and charged responses. For example, the question, "What are some changes you can make RIGHT now to your online behavior that could help improve your own online safety?," received answers suggesting that the techniques offered by the Program might not have been considered equal to facing the challenge. Certain participants wanted to eliminate the possibility that dangers such as those depicted in the presentation could be visited upon themselves and their families, giving responses such as quitting the Internet entirely or blocking their child's access to the Internet. Those participants may very well have possessed the knowledge to answer with "measured responses" and meet the goal; however, their emotions impacted their willingness to answer with targeted responses and, instead, they chose to respond with passion.

Impact on Children and Adolescents

As has been stated above, the Internet Safety Program may have provided value beyond only the participants who attended the Program. Paraprofessionals, without the instructional, grading and disciplinary responsibilities of teachers, may be in a better position to offer moral, psychological and other support to children and adolescents in the classroom, and therefore be a valuable asset for disseminating knowledge about safe online behavior. A widespread expansion of this Program, coupled with a more formal evaluation system, could eventually result in the online behavior of children and adolescents in the District to be tracked and measured for value. In addition, many of the participants are parents and, during the discussion portion at the conclusion of the Program, spoke at length about their desire to increase communication about online behavior with their children. Thus, although this outcome was not tracked or evaluated in the study, it stands to reason that improving the Internet safety of the participants might have some degree of a ripple effect on the behavior of children in the community.

Strengths of the Study

The Internet Safety Program developed and delivered in this study exhibited several strengths as a result of its unique design, conception, and presentation. While the majority of the participants reported having computers present in the home and had a great deal of cultural exposure to the Internet, their online usage with regard to websites popular with children and adolescents, i.e., the social media websites most likely to threaten safety and privacy, was minimal. A typical Internet “savvy” population tends to be younger than the participants, most of whom were over the age of 40. Thus, the target population, largely lacking a significant amount of “incoming knowledge,” would be seemingly ripe for positive knowledge gains in the target areas. In addition, many of the

participants were motivated not only because the subject matter of Internet safety related to their employment, but had resonance in their personal lives as well. Parents may have had an increased dimension of interest as learned responses may have helped to foster better communication with their children about Internet safety. All these factors all may have contributed to the strength of the study: a population ripe for knowledge attainment and extremely receptive to the content.

Another major strength was the fact that the Internet Safety Program's developer was also the Program's presenter. This provided the participants with the unique opportunity to receive content delivered by someone who possessed intimate and nuanced knowledge of Program content, flow, and message through his own experience and independent development of the Program. It is unlikely that a trained presenter, however high the standardized parameters required by the developer, could be as personally invested in the Program's effectiveness.

Limitations of this Study

While the dual developer/presenter may have been a strength of this study, it may have served as a limitation as well. While the unique qualities of the presenter, as discussed above, may have been instrumental in goal achievement, such exceptionalism may have hindered the ability to ascertain Internet Safety Program effectiveness on a larger scale. To test for statistical significance and effect size of measured goals, many more presentations would have to occur, necessitating that trained presenters, who would more than likely not have the comprehensive knowledge of the Program developer, nor embody the same level of passion for the subject, be responsible for content delivery. Such substitution may introduce a variable, the impact of which is unknown, to Program evaluation.

After presenting the Internet Safety Program, analyzing the results, and exploring its impact as an exploratory study, two major limitations, attributed to design, implementation, and evaluation, became apparent: the number of participants and needs assessment determination. While the relatively minimal number of participants, or small *n*, fit the parameters of this exploratory study, such a small sample made it difficult for the study to be interpreted as a true representation of any population. A larger number could have provided Program planners or evaluators with a group sufficient to obtain (a) a greater representative sample of a school population, (b) powerful effect size, and (c) statistical significance. Thus, while the descriptive statistics this study produced were helpful in describing outcomes of an exploratory study conducted with these particular individuals, a larger, more standardized and representative sample of participants might have resulted in a more powerful study, the results of which might be extrapolated to a greater universe.

A related issue was that the narrow subject focus of the survey restricted its representativeness as well. While the participants might have provided a valid snapshot of the Internet Safety Program's value for paraprofessionals in the District, paraprofessionals comprise a small segment of the school population. Paraprofessionals and teachers, for example, have different educational backgrounds; occupational requirements; roles within the school; and responsibilities to the students, their families, and the school's administration. The current design might not have equivalent value with students or other school staff members. For example, the simple scope of the study may have been appropriate for the target population, but the evaluation of the Program as having value beyond that of an initial study was severely limited.

In addition to issues arising out of the size and scope of the population, the Internet Safety Program lacked a formal needs assessment, as discussed above, which may have had an impact on analysis of results and goal attainment. A formal process, with its more comprehensive ability of delineation and clarification, could have identified a more standardized and accepted set of needs. Domains of exploration were determined in interviews with a District official, the Director, rather than as a result of formal survey of the entire staff population. While such interviews provided adequate knowledge for the purposes of this study, a more formalized needs assessment would have provided greater confidence in addressing needs, and a streamlined process of clarification of target knowledge domains. The domains in the present study were the functions of the administration's best guesses as to what information was lacking. That process, while not ideal, was nonetheless in accordance with many accepted needs determinations in other empirically supported programs. However, a formal needs assessment would have had far greater potential to produce a more valid set of goals to fill measured needs.

While subjects consistently gained knowledge in most sections, goal attainment was mixed. In some cases, goals were attained with greater ease when participants possessed significant amounts of "incoming knowledge," as such goals could be reached with little need for "learned responses." In that case, the current state of knowledge was the desired state. An example of this could be seen with respect to goal 1: all participants possessed the prior knowledge that a cyberbullying incident must be reported to a superior. A formal needs assessment would have been aware of this prior to Internet Safety Program development, thus allowing more appropriate goals, addressing the true current gaps in knowledge, to be constructed.

Implications and Recommendations

Implications for Future Research

After completing the needs assessment, design, presentation, and evaluation of this Internet Safety Program, several issues emerged that could improve the value, efficiency, and richness of the Program in the future. First and foremost, future research should be conducted with significantly increased sample sizes. A larger participant pool (*n*) could (a) facilitate a more detailed statistical analysis, (b) assess for statistical significance and effect size, and (c) greater capture the value provided for the target population.

The goals assessed in the surveys could be reworked for greater specificity in measurement and accuracy in addressing identified need. As was stated above, a formal needs assessment completed through a presurvey with a sample of future participants would have greatly aided in the development of a set of goals that truly captured weaknesses in the target area, i.e., knowledge of Internet safety. Administrative surveys and discussions were valuable components in helping to construct goals during Internet Safety Program development, but were based on informal observations and anecdotal information. A specific survey conducted directly with participants before goal development would have been far more accurate. For example, as discussed above, the first goal achieved an “incoming knowledge” measurement of 100%, signifying that each participant already knew to report a cyberbullying incident. The “desired state of affairs” had been attained in the absence of any training. A formal needs assessment could have accounted for this, adjusting goals to address actual areas of need, instead of corroborating already existing knowledge.

In addition, goals could be measured on scales with more precise instruments, like multiple choice responses or a Likert scale. Open-ended responses have their benefits, but when determining whether specific, targeted information was conveyed by a presentation, a more efficient and streamlined measurement system could help analyze data from larger sample sizes and produce more accurate information.

Subject size, scope and breadth could be increased to address specific needs in other populations present in or associated with schools, such as students, parents, teachers, administrative staff, and mental health professionals. Needs assessments could be performed for each group, tailoring the content of presentations to a specific group of participants. Were this to occur, greater value would be provided for the school community and for the Internet Safety Program itself.

One distinct feature of this program's administration was that the Internet Safety Program's developer was also its presenter, as discussed above. This fact, presenting as both a benefit and weakness of the Program, could be mitigated in impact in future research by preparation of a training module built by the developer so as to allow for additional presenters and, thus, expand the Program. Such training module would conform presentations to a uniformly high standard.

For the purposes of this exploratory study, the Internet Safety Program was presented and assessed largely in a vacuum. A variety of sources supported its development, including (a) accepted standards and practices presented in the program *NetSmartz* and supplemented by information from the Cyberbullying Research Center and the National Society for the Prevention of Cruelty to Children, (b) the enthusiastic knowledge of the presenter, and (c) discussions with a District decision maker. It would

be helpful to compare the Program's value with older, more widely used and accepted programs, such as *NetSmartz*, so that Program content could be modified, if needed.

Changes in the school population could be tracked as well in order that those students who are in particular need of training in Internet safety, but whose connection to the Internet Safety Program is only peripheral in the form of interaction with prior participants, could be identified. This might be accomplished through reference to school behavioral and disciplinary records, police reports related to Internet issues, and formal reports related to cyberbullying that fall into the harassment, intimidation, and bullying categories addressed by state legislation. This information could be tracked over time to compare how the establishment of a standardized Internet safety program could affect behavioral change in its participants, and whether those changes can be evidenced in the school and/or larger community. These factors could be analyzed longitudinally to account for the Program's impact on the population of participants and its value with the larger numbers who might benefit from its peripheral influence.

An extremely important component during the conceptualization and development phases of the Internet Safety Program was the prospect of emotional response and connection with the audience through the powerful images and messages that would be presented. However, during the later phase of Program development, planning for evaluation and capturing programmatic value, the focus shifted to analyzing information presented by participants in the specific goal areas. It would be interesting to discover whether a deeper emotional connection to the material fosters a greater level of attention and care on the part of Program participants. The ability to measure emotional response through a scale or survey question could help support the Program's value when compared against other standalone, existing Internet safety programs. A measure to

account for the emotional response of participants could be extremely effective in future program iterations and analysis.

Implications for Future Trainings

In expanding upon the concept of developing a formalized training module that could standardize the deliverance of future programs by more than one presenter, as discussed above, knowledge gained from prior presentations of the Internet Safety Program could be incorporated into the training module to help create a standard of practice that provides the greatest programmatic value. These might include updated information for existing topics, adding new topics when relevant, and structural improvements, i.e., better flow. Such training could include provisions for tailoring the Internet Safety Program to meet the needs of specific populations, so that language, content, and other elements may be adapted for each group of participants, whether it be students, teachers, parents, or administrative personnel.

There must also be a degree of flexibility so that a presenter can respond to a situation that may be relevant to Internet Safety Program goals and of vital concern to participants, but absent from a training module. For example, while the focus of the developed Program, as a District-approved in-service activity, was to address Internet safety issues faced by paraprofessionals working with students, it was evident during the discussion phase that the participants, as parents, were extremely invested in Internet safety as it related to their own children. An ability to pivot to focus on participants' relevant concerns not only improves the connection between presenter and participants, but encourages them to feel as though the Program has resonance in their lives. An additional example of the importance of flexibility arose when the participants expressed great interest in news stories related to presentation content. The researcher obliged with

a quick overview of the interplay between those current events and the need for safe and private online practices.

Implications for Future Internet Safety Program Dissemination

While this Internet Safety Program has only been delivered to one target population, this presentation, as well past presentations of earlier Internet safety programs elicited a number of requests for more information. Frequently, the researcher is requested to repeat the Program to additional audiences, i.e., classrooms, assemblies, or parents. These examples, while anecdotal, indicate that a great deal of need may exist for widespread expansion and dissemination of such a program. Exploring that need could expose untapped potential in other school districts, communities, or even states for standardized and powerful Internet safety programming.

Were this expansion to occur, more standardized and complete needs assessments must be included so that the content is appropriate for the target population concerned. For example, the needs of a school district other than R may not align with R's. Thus, the Internet safety program would have to be varied and flexible enough to accommodate fluctuations in need. In addition, as the realm of Internet safety is extremely elastic and unusually sensitive to cultural trends and technological advances, great care would need to be taken to ensure that the topics covered remain current and relevant, Thus, provisions for revisions would have to be developed so that such information is disseminated as it is known. In addition, presenters would be required to be informed regarding the constant evolution of Internet safety, placing on the researcher/developer the responsibility to disseminate all material related to technological advances and local trends in the area. Given the ever-evolving online threats and dangers, the need for Internet safety programs

is not likely to be obsolete any time soon and a program that can keep pace with such challenges will be valuable to many populations.

References

- Acohido, B. (2011). Facebook tracking is under scrutiny. *USA Today*. Retrieved from <http://usatoday30.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-data/51225112/1>
- Anti-Bullying Bill of Rights Act, P.L. 122 § N.J.S.A. 18A:37-13 (2010, Amended 2012).
- Aston, H., & Brzyska, B. (2012). *Protecting children online: Teachers' perspectives on eSafety*. Milton Keynes: Vital. Retrieved from <http://www.nfer.ac.uk/publications/95001/95001.pdf>
- Atkinson, C., & Newton, D. (2010). Online behaviours of adolescents: Victims, perpetrators, and Web. 2.0. *Journal of Sexual Aggression, 16*(1), 107-120.
- Brookshire, M., & Maulhardt, C. (2005). Evaluation of the Effectiveness of the NetSmartz Program: A Study of Maine Public Schools. Retrieved from www.netsmartz.org/sitecore/content/Netsmartz/~/_media/Netsmartz/Pdf/gw_evaluation.ashx
- Chibnall, S.; Wallace, M.; Leicht, C., & Lunghofer, L. (2006, January). *I-Safe evaluation*. Retrieved from <https://www.ncjrs.gov/pdffiles1/nij/grants/213715.pdf>
- Common Sense Media (2012, 2013). *Privacy and internet safety*. Retrieved from <https://www.commonsensemedia.org/privacy-and-internet-safety>
- Common Sense Media (2015). *Our mission*. Retrieved from <https://www.commonsensemedia.org/about-us/our-mission#about-us>
- David-Ferdon, C., & Hertz, M. (2007). Electronic media, violence, and adolescents: An emerging public health problem. *Journal of Adolescent Health, 41*(6), Supplement: S1-S5.

- Department for Children, School and Families (2010). *Working together to safeguard children: A guide to inter-agency working to safeguard and promote the welfare of children*. London: DCSF. Available from <https://www.education.gov.uk/publications/eOrderingDownload/00305-2010DOM-EN.pdf>
- Dombrowski, S., Gischlar, K., & Durst, T. (2007). Safeguarding young people from cyber pornography and cyber sexual predation: A major dilemma on the internet. *Child Abuse Review, 16*(2), 153-170.
- Duff, R., & Leggett, S. (2012). *Trends in media use*. UK Council for Child Internet Safety. London: Childwise Research, RH28. Retrieved from http://www.saferinternet.org.uk/content/childnet/saferinternetcentre/downloads/Research_Highlights/UKCCIS_RH_28_Childwise.pdf
- Hart Research Associates (2012). *The online generation gap: Contrasting attitudes and behaviors of parents and teens*. Family Online Safety Institute. Retrieved from <http://safekids.com/pdfs/fosireport2012.pdf>
- Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior, 29*(2), 129-156.
- Hinduja, S., & Patchin, J. W. (2009). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Thousand Oaks, CA: Sage Publications.
- Hinduja, S., & Patchin, J. W. (2010). *Cyberbullying research*. Cyberbullying Research Center. Retrieved 2015 from www.cyberbullying.us
- Hinduja, S., & Patchin, J. W. (2013, 2015). *Cyberbullying facts*. Cyberbullying Research Center. Retrieved 2013, 2015 from www.cyberbullying.us

- i-SAFE Inc. (2012). *i-SAFE, The leader in e-safety education*. Retrieved from <http://www.isafe.org/>
- i-SAFE Inc. (2012a). *i-SAFE, The leader in e-safety education*. Retrieved from <http://www.isafe.org/about>
- Jones, L., Mitchell, K., & Finkelhor, D. (2013). Online harassment in context: Trends from three youth internet safety surveys (2000, 2005, 2010). *Psychology of Violence, 3*(1), 53-69. Retrieved from <http://www.unh.edu/ccrc/pdf/Online%20Harassment%20in%20Context.pdf>
- Juvonen, J., & Gross, E. F. (2008). Extending the school grounds?—Bullying experiences in cyberspace. *Journal of School Health, 78*, 496–505.
- Kam, K. (2014). *4 Dangers of the Internet, WebMD Feature*. Retrieved from <http://www.webmd.com/parenting/features/4-dangers-internet>
- Kessel-Schneider S., O'Donnell, L., Stueve, S., & Coulter, R. W. S. (2012). Cyberbullying, school bullying, and psychological distress: A regional census of high school students. *American Journal of Public Health, 102*(1), 171.
- Lazuras, L., Pyzalski, J., Barkoukis, V., & Tsorbatzoudis, H. (2013). A process model of cyberbullying in adolescence. *Computers in Human Behavior, 29*(3), 881.
- Livingstone, S., & Davidson, J. (2013). *Child online safety: Summary of recent research findings*. UK Council for Child Internet Safety. Retrieved from http://www.saferinternet.org.uk/content/childnet/saferinternetcentre/downloads/Research_Highlights/Child_Online_Safety_-_Summary_of_Recent_Research_Findings.pdf
- Livingstone, S., & Palmer, T. (2012). *Identifying vulnerable children online and what strategies can help them*. London: UK Safer Internet Centre.

- Malware [Def. 1]. (n.d.). In *Oxford's US English Dictionary*. Oxford University Press.
Retrieved January 15, 2015, from
http://www.oxforddictionaries.com/us/definition/american_english/malware?searchDictCode=all
- McAfee (2014). *Teens and the screen study*. Retrieved from
<http://blogs.mcafee.com/consumer/teens-and-screens>
- Miller, C., & Sengupta, S. (2013) Selling secrets of phone users to advertisers. *The New York Times*. Retrieved from
http://www.nytimes.com/2013/10/06/technology/selling-secrets-of-phone-users-to-advertisers.html?pagewanted=all&_r=0
- National Center for Missing & Exploited Children (2012). *NetSmartz internet safety presentation: Educate parents & communities*. NetSmartz Workshop. Retrieved from <http://www.netsmartz.org/Presentations>
- National Center for Missing & Exploited Children (2012a). *About us*. NetSmartz Workshop. Retrieved from <http://www.netsmartz.org/Overview/AboutUs>
- New Jersey Department of Education (2015). *Keeping our kids safe, healthy & in school: Harassment, intimidation, and bullying (HIB)*. Retrieved from
<http://www.state.nj.us/education/students/safety/behavior/hib/>
- The National Campaign to Prevent Teen and Unplanned Pregnancy. (2008). *Sex and tech: Results from a survey of teens and young adults*. Retrieved from
http://thenationalcampaign.org/sites/default/files/resource-primary-download/sex_and_tech_summary.pdf
- National Society for the Prevention of Cruelty to Children (2011). *Safe network: Safe activities for everyone*. Retrieved from <http://www.safenetwork.org.uk/>

- National Society for the Prevention of Cruelty to Children (2012). *Children, young people and “sexting”*: Summary of a qualitative study. London: NSPCC.
- National Society for the Prevention of Cruelty to Children (2015). *Keeping children safe online*. London: NSPCC. Retrieved from http://www.nspcc.org.uk/Inform/trainingandconsultancy/learningresources/keeping-children-safe-online_wda90164.html
- National Society for the Prevention of Cruelty to Children (2015a). *Child protection course: An introduction*. London: NSPCC. Retrieved from <http://www.nspcc.org.uk/what-you-can-do/get-expert-training/child-protection-introduction/>
- Olweus, D. (1994). Bullying at school: Basic facts and effects of a school based intervention program. *Journal of Child Psychology and Psychiatry*, 35(7), 1171-1190.
- Phishing [Def. 1]. (n.d.). In *Oxford’s US English Dictionary*. Oxford University Press. Retrieved January 15, 2015 from http://www.oxforddictionaries.com/us/definition/american_english/phishing?searchDictCode=all
- Prensky, M. (2001). Digital natives, digital immigrants. *On the Horizon*, 9(5). Retrieved from <http://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf>
- Priebe, G., Mitchell, K. J., & Finkelhor, D. (2013). To tell or not to tell? Youth’s responses to unwanted internet experiences. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 7(1), article 6.

- Rafferty, R., & Vander Ven, T. (2014). "I hate everything about you": A qualitative examination of cyberbullying and on-line aggression in a college sample. *Deviant Behavior, 35*(5), 364.
- Ringrose, J., Gill, R., Livingstone, S., & Harvey, L. (2012). *A qualitative study of children, young people and "sexting": A report prepared for the NSPCC*. London: NSPCC. Retrieved from <http://www.nspcc.org.uk/globalassets/documents/research-reports/qualitative-study-children-young-people-sexting-report.pdf>
- Sticca, F., Ruggieri, S., Alsaker, F., & Perren, S. (2013). Longitudinal risk factors for cyberbullying in adolescence. *Journal of Community & Applied Social Psychology, 23*(1).
- Smith, C., & Warner, H. (2013). *E-safety in schools - The results of the London e-safety survey and the impact on schools*. The London Grid for Learning Esafety Board. Retrieved from <http://files.lgfl.net/eSafety/Survey/LGFL%20Esafety%20Survey%20Report%202013%20%28full%20version%20with%20Exec%20Summary%29.pdf>
- Snakenborg, J., Acker, R., & Gable, R. (2011). Cyberbullying: Prevention and intervention to protect our children and youth. *Preventing School Failure: Alternative Education for Children and Youth, 55*(2), 88-95.
- Strohmaier, H., Murphy, M., & DeMatteo, D. (2014). Youth sexting: Prevalence rates, driving motivations, and the deterrent effect of legal consequences. *Sexuality Research and Social Policy, 11*(3), 245-255.
- UK Council for Child Internet Safety. (2013a). *About*. UK Safer Internet Centre. Retrieved from <http://www.saferinternet.org.uk/about>

- UK Council for Child Internet Safety. (2013b). *Research highlights series: UKCCIS evidence group*. UK Safer Internet Centre. Retrieved from http://www.saferinternet.org.uk/content/childnet/saferinternetcentre/downloads/Research_Highlights/Introduction_to_the_Research_Highlight_series.pdf
- UK Council for Child Internet Safety. (2013c). *Research: Research summaries from the evidence group of the UK Council for Child Internet Safety*. UK Safer Internet Centre. Retrieved from <http://www.saferinternet.org.uk/research>
- Whittle, H., Hamilton-Giachritsis, C., & Beech, A. (2013). Victims' voices: The impact of online grooming and sexual abuse. *University Journal of Psychology, 1*(2),59-71. Retrieved from <http://www.hrpub.org/download/201308/ujp.2013.010206.pdf>
- Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and Violent Behavior, 18*, 62-70.
- Zur, O. & Zur, A. (2011). *On digital immigrants and digital natives: How the digital divide affects families, educational institutions, and the workplace*. Zur Institute - Online Publication. Retrieved on month/day/year from http://www.zurinstitute.com/digital_divide.html.

Appendix A

Program Procedure and Materials

1. Preprogram stage
 - a. Emails disseminated to target population informing of program
 - b. Information about program posted on the school district's website
2. Program preparatory stage
 - a. Enter designated classroom one hour prior to program start time
 - b. Set up equipment
 - i. Plug in and turn on laptop, load internet safety program in Microsoft PowerPoint
 - ii. Connect to internet and prepare online components
 - iii. Plug in and test speakers, microphone, and amplifier
3. Program introduction (12-12:35pm)
 - a. Consent forms handed out, completed, and collected
 - b. Program survey handed out, completed, and collected
 - c. PowerPoint program commenced, introduction slides presented to paraprofessionals
4. Internet safety program, phase I: Staying safe and private online (12:35-12:50pm)
 - a. Presentation of corresponding PowerPoint slides
 - b. Index cards used by presenter to orally deliver program
5. Internet safety program, phase II: Specific dangers that exist online (12:50-1:15pm)
 - a. Presentation of corresponding PowerPoint slides
 - b. Index cards used by presenter to orally deliver program

6. Internet safety program, phase III: Cyberbullying (1:15-1:35pm)
 - a. Presentation of corresponding PowerPoint slides
 - b. Index cards used by presenter to orally deliver program
7. Question & answer, clarification period (1:35-2:00pm)
 - a. Presenter fields questions from participants
 - b. Presenter discusses strategies for talking to students about internet safety and leads discussion
 - c. Paraprofessionals fill out program survey for second time, survey is collected
8. Break-down stage
 - a. Laptop shut down and materials gathered for departure
 - b. Materials organized for evaluation and storage

Materials

- 50 copies of statistical handouts per class
- Two copies of the internet safety program
 - o One copy in Microsoft PowerPoint form
 - o One copy as a physical printout
- One printed copy of the 2012 NetSmartz internet safety program (for reference)
- One set of index cards with program notes
- Three black pens, for presenter use

Equipment

- One wireless internet-enabled laptop computer, running Microsoft Office
- One microphone
- One amplifier for the microphone
- One digital projector, projecting the image created by the laptop

- One pair of computer speakers to project sound from the laptop
- One 4 gigabyte USB flash drive

Facilities

- R High School cafeteria
 - o Cafeteria features adequate presenter space, seating for subject pool, and audio-visual equipment

Appendix B

Consent Form

Agreement to Participate in Research

Principal Investigator: Scott Kraiterman, Psy.M.

Title of Protocol: Internet Safety Program Survey

1. I am requesting that you participate in a survey for research that intends to investigate the value of an internet safety presentation. It will attempt to assess for knowledge gained in the areas of cyberbullying, specific dangers that exist in the online community, and safe and private online behavior.

2. You will be asked to fill out two surveys about your knowledge in these areas. No previous knowledge about any of these topics is necessary.

3. Completing these surveys involves no risk to you.

4. The program length will vary depending on the number of questions following its presentation. My part of the presentation usually lasts about an hour and a half. Completing each survey typically takes about 5-10 minutes.

5. You have been chosen by the administration of the district of R to attend this program as an in-service presentation for today, February 18, 2013. It will count toward your required in-service hours in the same manner in which every other district sponsored in-service presentation would.

6. You and the other participants in this presentation will benefit if the results are used by the district to improve the quality of internet safety education in the district. You may also benefit from a greater wealth of knowledge about the realm of internet safety as well as gaining tools that can be used in an academic setting.

7. If you would not like to be included in the study, you may wish to not sign this form or fill out the surveys. This will be done at no penalty to you, as participation in the in-service **with or without completing the surveys** will earn you in-service hours. You may still opt out of the survey after completing the first survey and it will not be counted in the study.

8. All those that fill out both surveys and attend this presentation will be included in the study, if they wish. The surveys and presentation may be delivered again during this school year, at which time both groups' surveys will be included in the final research. No more than 100 people will be included in the study.

9. Although the results of this survey may be published, **no identifying information** that could identify you personally will be included. Participants will remain completely anonymous.

10. Questions about any of this research may be directed at Scott Kraiterman, 732-572-2289 x2547. Complaints about the research may be directed at Susan Forman, Chair of the school psychology program at Rutgers' Graduate School of Applied and Professional Psychology, 848-445-3975.

11. The results of the study will be provided, if requested, after June 20, 2013 at skraiterman@pway.org.

12. You will receive a copy of this letter for your records.

It is not expected that any participants in this study feel any adverse or negative effects resulting from participation. However, if you should feel any adverse or negative effects, please contact Scott Kraiterman at 732-572-2289 x2547 or Nancy Boyd-Franklin, Ph.D., at 848-445-3924.

If you have any questions about your rights as a research subject, you may contact the IRB (a committee that reviews research studies in order to protect research participants) by contacting the IRB Administrator at Rutgers University at:

Rutgers University, the State University of New Jersey
Institutional Review Board for the Protection of Human Subjects
Office of Research and Sponsored Programs
3 Rutgers Plaza
New Brunswick, NJ 08901-8559
Tel: 848-932-0150
Email: humansubjects@orsp.rutgers.edu

You may contact the investigator of this survey at:

Scott Kraiterman
School Psychologist/Therapist
732-572-2289 x2547
Email: skraiterman@pway.org

Thank you for participating in this survey!

Sincerely,

Scott Kraiterman, Psy.M.

Participant

Appendix C

Survey (Pre-Assessment and Post-Assessment)

Participant Code: _____

Internet Safety Program Survey

Thank you for filling out our survey! Please answer all questions to the best of your ability. The answers are all anonymous and will never be linked to any individuals.

Please be as honest as you can.

1. How many hours a day do you spend online? _____

2. What social networking sites (Facebook, Tumblr, reddit, etc.) do you use regularly?

3. Do you have computers at home? If so, where are they located within the home and who is the primary user of each one?

4. Are you currently sharing any of the following information on ANY social networking sites? (check all that apply)

a. Full name _____

b. Cell phone number _____

c. Home address _____

d. Names of family members _____

e. School information _____

f. Job information _____

g. Others notable personal inclusions (please list)

5. Please answer the following questions to the best of your ability.

a. A student in your school comes to you and reports an incident of what you believe to be cyberbullying. What advice do you provide that student on how to respond? Please list as many responses as you can.

b. Think about a social networking website like Facebook. What privacy controls are good for students to activate in order to help them stay as safe and private as possible?

c. Think about usernames and passwords that a person may utilize online. What are some safe practices that a student can use when creating or changing usernames or passwords that could help them stay as safe and private as possible?

d. What are some changes you can make RIGHT now to your online behavior that could help improve your own online safety?

e. Name as many websites or types of website tools as you can that are frequented by online predators.

f. Name as many methods as you can that online predators use to "groom" or entrap children.

g. Name as many ways that you can that a typical student can take to immediately decrease their exposure to online predators.

Thank you very much!

Scott Kraiterman, Psy.M.

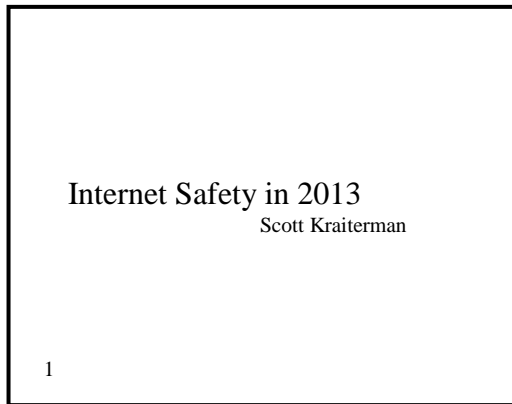
Appendix D

Internet Safety Program Slides

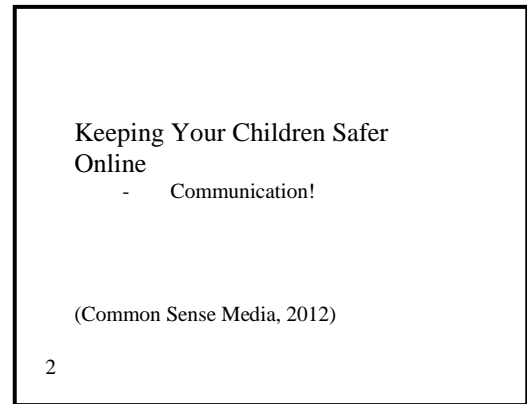
(For the full presentation, see

<https://drive.google.com/file/d/0B0c5GnsUFUJDQ1RBanBkVzhBUWM/view?usp=sharing.>)

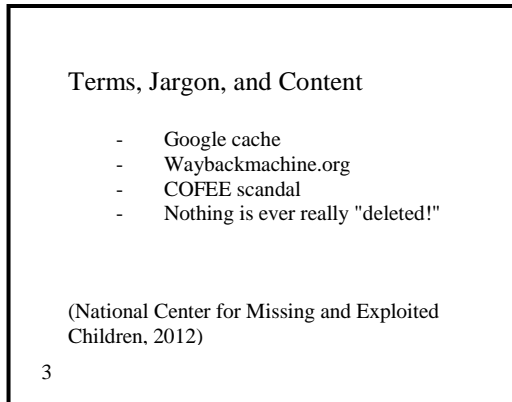
Slide 1



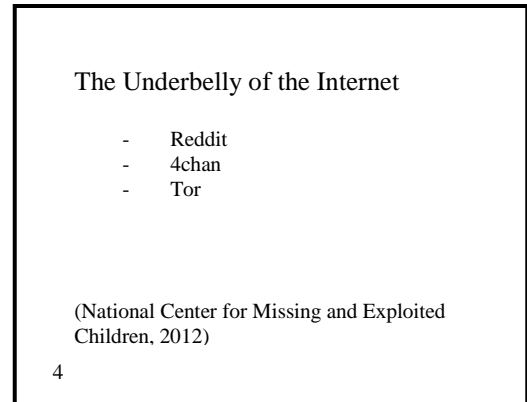
Slide 2



Slide 3



Slide 4



Slide 5

Online

- Cell Phones
- Laptops
- Gaming Devices

(National Center for Missing and Exploited Children, 2012)

5

Slide 6

- Gmail
- Myspace
- Facebook
- Google
- Disney Club Penguin
- RuneScape
- AIM
- iTunes

(National Center for Missing and Exploited Children, 2012)

6

Slide 7

Youtube!

(video)

(National Center for Missing and Exploited Children, 2012)

7

Slide 8

Risky Online Behaviors

- Sending or posting provocative images
- Sharing passwords with friends
- Embarrassing or harassing people
- Posting personal information
- Clicking on pop-ups

(National Center for Missing and Exploited Children, 2012)

8

Slide 9

Bullying + Technology = Cyberbullying

- eww! what is she wearing?

(National Center for Missing and Exploited
Children, 2012)

9

Slide 10

General Bullying

- "A person is bullied when he or she is exposed, repeatedly and over time, to negative actions on the part of one or more other persons, and he or she has difficulty defending himself or herself."

(Olweus, 1994)

10

Slide 11

New Jersey: Harassment, Intimidation, and Bullying in 2013

"Harassment, intimidation or bullying" means any gesture, any written, verbal or physical act, or any electronic communication, whether it be a single incident or a series of incidents, that is reasonably perceived as being motivated either by any actual or perceived characteristic, such as race, color, religion, ancestry, national origin, gender, sexual orientation, gender identity and expression, or a mental, physical or sensory disability, or by any other distinguishing characteristic, that takes place on school property, at any school-sponsored function, on a school bus, or off school grounds as provided for in section 16 of P.L.2010, c.122 (C.18A:37-15.3), that substantially disrupts or interferes with the orderly operation of the school or the rights of other students and that:

a. a reasonable person should know, under the circumstances, will have the effect of physically or emotionally harming a student or damaging the student's property, or placing a student
in reasonable fear of physical or emotional harm to his person or damage to his property;
b. has the effect of insulting or demeaning any student or group of students; or
c. creates a hostile educational environment for the student by interfering with a student's education or by severely or pervasively causing physical or emotional harm to the student."

New Jersey Department of Education, (2013)
(Anti-Bullying Bill of Rights Act, 2010)

11

Slide 12

Cyberbullying

- Evolution in communication
- Technology increases access
- Online communities
- Perceived anonymity
- Those that bully others - increased risk of cyberbullying!

(Hinduja and Patchin, 2008)
(Hinduja and Patchin, 2009)

12

Slide 13

Cyberbullying

- Electronic aggression in the form of harassment, teasing, mean comments, rumor spreading and threats
 - o IM
 - o Text messaging
 - o Email
 - o Chat rooms
 - o Blogs
 - o Web sites
 - o Social networking sites
 - o Picture and video clips
 - o Internet gaming

(Hinduja and Patchin, 2009)
(David-Ferdon and Hertz, 2007)

13

Slide 14

Challenges of cyberbullying

- Difficult to define and operationalize
- One text message - repeated aggressions over time?
- Where does the power imbalance exist?
- Anonymity
- Can continue outside the school day

(Hinduja and Patchin, 2009)
(David-Ferdon and Hertz, 2007)

14

Slide 15

Cyberbullying

- Spreading rumors and gossip
- Posting pictures of someone without consent
- Stealing passwords to assume someone else's identity
- Threatening or harassing with offensive language

(Hinduja and Patchin, 2009)
(National Center for Missing and Exploited Children, 2012)

15

Slide 16

Information Acceleration

(National Center for Missing and Exploited Children, 2012)

16

Slide 17

Signs of Cyberbullying

- A cyberbullying victim might:
 - o Stop using the computer or cell phone
 - o Act nervous when receiving an e-mail, IM, or text
 - o Seem uneasy about going to school
 - o Withdraw from friends and family

(National Center for Missing and Exploited Children, 2012)
(Hinduja and Patchin, 2009)

17

Slide 18

- Block or ban the bully from contacting your child
- Set up a new account
- Save the messages for evidence

(National Center for Missing and Exploited Children, 2012)

18

Slide 19

**Report to the website, school,
bully's parents, or law
enforcement**

(National Center for Missing and Exploited Children, 2012)

19

Slide 20

Cyberbullying Behaviors

- Quickly switch screens, or close programs when you walk by
- Use the computer at all hours of the night
- Get unusually upset if they cannot use the computer
- Laugh excessively while online
- Avoid discussions about what they are doing
- Use multiple online accounts or use an account that is not their own

(National Center for Missing and Exploited Children, 2012)

20

Slide 21

Cyberbullying
- "You Can't Take it Back"

(National Center for Missing and Exploited Children, 2012)

21

Slide 22

(NetSmartz Workshop video)

(National Center for Missing and Exploited Children, 2012)

22

Slide 23

Consequences of Cyberbullying

(National Center for Missing and Exploited Children, 2012)

23

Slide 24

Don't just be a bystander!

(National Center for Missing and Exploited Children, 2012)

24

Slide 25

Talk to your kids!

- Pay attention.
- Take action.

(National Center for Missing and Exploited Children, 2012)

25

Slide 26

**Who are they talking to?
What are they talking about?
What are they sharing online?**

(National Center for Missing and Exploited Children, 2012)

26

Slide 27

Facebook Friends

(National Center for Missing and Exploited Children, 2012)

27

Slide 28

Friend Requests

(National Center for Missing and Exploited Children, 2012)

28

Slide 29

Talk to your kids!

- Pay attention.
- Take action.

(National Center for Missing and Exploited Children, 2012)

29

Slide 30

When can your comments get you into trouble?

- "Teenager fired for complaining about her job on Facebook."

(National Center for Missing and Exploited Children, 2012)

30

Slide 31

Usernames

(National Center for Missing and Exploited Children, 2012)

31

Slide 32

Live Hunt

- Originally completed in 2009
- Updated in 2013

32

Slide 33

Google search
- "webcam cap girl"

33

Slide 34

Google search
- "alina_____"

34

Slide 35

MySpace
- "ALINA_____"

35

Slide 36

MySpace
- "ALINA_____"
(continued)

36

Slide 37

PHOTOLOG

- "Last photos of alina _____"

37

Slide 38

Google maps

- "Saukville, WI"

38

Slide 39

MySpace

- "ALINA _____'s blog"
 - o "The Best People I Know)

39

Slide 40

Facebook

- "Kristen _____"
- "Port Washington High"

40

Slide 41

Port Washington High School
- Port Washington, WI

41

Slide 42

Facebook search

- "Kristen _____'s Friends"
 - o "Alina _____"
 - o Port Washington High
 - o Saukville, WI

42

Slide 43

Facebook

- "Jimmy Dugan"
- "Saukville, WI"
- "Port Washington High"

43

Slide 44

Facebook

- "Alina _____"
- Full profile

44

Slide 45

Facebook

- Living
- Relationship
- Family

45

Slide 46

Facebook

- "New phone, need numbers"

46

Slide 47

Linkedin

- "Alina _____"
- Work experience

47

Slide 48

Twitter

- "Alina _____"
- @alina_____

48

Slide 49

Myspace
- "Alina" (current)

49

Slide 50

Photobucket
- "alina_____"

50

Slide 51

Stickam
- "alina_____"
- AIM
- Email

51

Slide 52

Whitepages search
- "Alina _____"
- "Angela _____"
- "David _____"

52

Slide 53

Whitepages

- "Angela _____"
- Phone number
- Address

53

Slide 54

Google maps

- "Angela _____"
- Address
- Satellite view

54

Slide 55

Google maps

- "Angela _____"
- Address
- Street view

55

Slide 56

Google maps

- "Angela _____"
- Address
- Satellite view

56

Slide 57

Google search

- "webcam cap girl"

57

Slide 58

Google maps

- "Angela _____"
- Address
- Street view

58

Slide 59

Privacy Settings

- Friends Only
 - o My status, photos, and posts
 - o Family and relationships
 - o Photos and videos I'm tagged in
 - o Birthday
 - o Permission to comment on your posts
 - o Contact information

(National Center for Missing and Exploited Children, 2012)

59

Slide 60

Sexting

- Sending sexual messages, pictures, or videos through cell phones

(National Center for Missing and Exploited Children, 2012)
(NSPCC, 2012)

60

Slide 61

1 in 6 teens ave received a "sext."

(National Center for Missing and Exploited Children, 2012)

61

Slide 62

Your Photo Fate

(National Center for Missing and Exploited Children, 2012)

62

Slide 63

(NetSmartz video)

(National Center for Missing and Exploited Children, 2012)

63

Slide 64

Consequences of Sexting

(National Center for Missing and Exploited Children, 2012)

64

Slide 65

"Can I see what you've been posting online?"

(National Center for Missing and Exploited Children, 2012)

65

Slide 66

What comes to mind when you think of online predators?

(National Center for Missing and Exploited Children, 2012)

66

Slide 67

Pedophile or Predator?

(National Center for Missing and Exploited Children, 2012)

67

Slide 68

"She's with him?"

(National Center for Missing and Exploited Children, 2012)

68

Slide 69

"She's with him?" (continued)

(National Center for Missing and Exploited Children, 2012)

69

Slide 70

(photo graphic)

(National Center for Missing and Exploited Children, 2012)

70

Slide 71

What puts children more at risk?

(National Center for Missing and Exploited Children, 2012)

71

Slide 72

Survivor Diaries

(National Center for Missing and Exploited Children, 2012)

72

Slide 73

(NetSmartz video)

(National Center for Missing and Exploited Children, 2012)

73

Slide 74

Signs of Grooming

- Check if your child is
 - o Receiving gifts through the mail
 - o Making calls to unknown numbers
 - o Turning away from friends and family
 - o Spending a lot of time online
 - o Getting upset when he or she can't get online
 - o Minimizing the screen or turning off the monitor when you come into the room

(National Center for Missing and Exploited Children, 2012)

74

Slide 75

Report to CyberTipline®

- Anyone who sends your child photos or videos containing obscene content
- Anyone speaking to your child in a sexual manner
- Anyone who asks your child to meet in person

How to Report

- Visit www.cybertipline.com
- Call 1-800-THE-LOST®

(National Center for Missing and Exploited Children, 2012)

75

Slide 76

Communicate. Monitor. Report.

- "What do you know about online predators?"
- "What would you do if someone asked to meet you in person?"

(National Center for Missing and Exploited Children, 2012)

76

Slide 77

Teach your child how to use technology responsibly.

(National Center for Missing and Exploited Children, 2012)

77

Slide 78

- Anti-virus software
- Filtering programs
- Monitoring software
- Parental supervision

(National Center for Missing and Exploited Children, 2012)

78

Slide 79

Establish rules for your child's Internet use.

- What sites can they visit?
- Who can they talk to?
- How much time can they spend online?

79

Slide 80

Monitor laptop activity.

80

Slide 81

Monitor mobile technologies.

(National Center for Missing and Exploited Children, 2012)

81

Slide 82

- "What's your favorite thing to do online?"
- "Show me the funniest YouTube video."
- "Let's play your favorite online game."

(National Center for Missing and Exploited Children, 2012)

82

Slide 83

NetSmartz.org

- Activities
- Discussion Starters
- Games
- Read about the issues
- Safety Pledges
- Tip Sheets
- Videos

(National Center for Missing and Exploited Children, 2012)

83

Slide 84

Help people in your community.

- Tell your friends about these resources
- Encourage your PTA to set up presentations
- And talk to your child's school about using NetSmartz

(National Center for Missing and Exploited Children, 2012)

84

Slide 85

Thank you!

Contact me at:

- scottkr@gmail.com

85

Slide 86

References

- Anti-Bullying Bill of Rights Act. P.L. 122 § N.J.S.A. 18A:37-13 (2010, Amended 2012)
- Common Sense Media (2013). Privacy and internet safety. Common Sense Media Inc. Retrieved from <https://www.commonsensemedia.org/privacy-and-internet-safety>
- David-Ferdon, C., Hertz, M. (2007). Electronic media, violence, and adolescents: an emerging public health problem. *Journal of Adolescent Health*, 41(6), Supplement: S1-S5
- Hinduja, S. & Patchin, J. W. (2009). *Bullying beyond the Schoolyard: Preventing and Responding to Cyberbullying*. Thousand Oaks, CA: Sage Publications.
- Hinduja, S. & Patchin, J. W. (2008). Cyberbullying: an exploratory analysis of factors related to offending and victimization. *Deviant Behavior*, 29(2): 129-156.

86

Slide 87

References (continued)

- National Center for Missing & Exploited Children (2012). NetSmartz internet safety presentation: Educate parents & communities. NetSmartz Workshop. Retrieved from <http://www.netsmartz.org/Presentations>
- New Jersey Department of Education (2013). Keeping our kids safe, healthy & in school: Harassment, intimidation, and bullying (HIB). State of New Jersey Department of Education. Retrieved from <http://www.state.nj.us/education/students/safety/behavior/hib>
- National Society for the Prevention of Cruelty to Children (NSPCC) (2012). Children, young people and 'sexting': summary of a qualitative study. London: NSPCC.
- Olweus, D. (1994). Bullying at school: basic facts and effects of a school based intervention program. *Journal of Child Psychology and Psychiatry*, 35(7): 1171-1190.

87