Interventions to Prevent and Reduce Cyber Abuse of Youth: A Systematic Review

Faye Mishna, Charlene Cook, Michael Saini, Meng-Jia Wu and Robert MacFadden

Research on Social Work Practice 2011 21: 5 originally published online 11 January 2010
DOI: 10.1177/1049731509351988

Research on Social Work Practice
21(1) 5-14

DOI: 10.1177/1049731509351988
http://rsw.sagepub.com

Interventions to Prevent and Reduce Cyber Abuse of Youth: A Systematic Review

Faye Mishna[1], Charlene Cook[2], Michael Saini[2], Meng-Jia Wu[3] and Robert MacFadden[2]

Abstract

Objectives: The Internet has created a new communication tool, particularly for young people whose use of electronic communication is exploding worldwide. While there are many benefits that result from electronic-based communication, the Internet is concurrently a potential site for abuse and victimization. **Methods:** This paper systematically reviews the effectiveness of cyber abuse interventions in increasing Internet safety knowledge and decreasing risky online behavior. **Results:** Significant results were found between pre- and posttest scores related to Internet safety knowledge. Most results related to risky online behavior were not significant. **Conclusions:** Results provide evidence that participation in psychoeducational Internet safety interventions is associated with an increase in Internet safety knowledge but is not significantly associated with a change in risky online behavior.

Keywords

abuse, field of practice, adolescents, population, youth, systematic review, literature review

Introduction

The rapid growth of electronic- and computer-based communication and information sharing during the last decade has changed individuals' social interactions, learning strategies, and choice of entertainment. The Internet has created a new communication tool, particularly for young people whose use of instant messaging, social networking Web sites, YouTube, e-mail, chat rooms, and webcams, among others, is exploding worldwide. While there are enormous benefits that result from electronic-based communications such as social and academic support, identity exploration, and cross-cultural interactions, the Internet is, however, concurrently a potential site for abuse and victimization (Mitchell, Finkelhor, & Wolak, 2003), whereby young people can fall victim to sexual perpetrators, stalkers, exploiters, and peers who bully online. Recent large-scale cross-sectional studies on the prevalence of cyber abuse demonstrate that this is a growing problem, in which commonly recognized forms of child maltreatment (sexual and emotional abuse) are being pursued via the Internet (Berson, Berson, & Ferron, 2002; Mitchell, Finkelhor, & Wolak, 2001; Mitchell et al., 2003; Ybarra & Mitchell, 2004a, 2004b). These findings have been supported by studies around the world, suggesting that the prevalence of cyber abuse of children and youth is growing dramatically (Aloysius, 2001; Arnaldo & Finnström, 1998; Cowburn & Dominelli, 2001; Durkin & Low, 1998; Finkelhor, Mitchell, & Wolak, 2000; Sellier, 2001), with detrimental short- and long-term effects on the psychosocial functioning of the children and youth involved.

Cyber abuse is an umbrella term that encompasses online abusive interpersonal behaviors including online bullying, stalking, sexual solicitation, and problematic exposure to pornography. Cyber bullying, also known as electronic bullying or online social cruelty (Kowalski & Limber, 2007), includes "willful and repeated harm inflicted" (Hinduja & Patchin, 2008) toward another. Cyber bullying is unique in its use of electronic communication technology as the means through which to threaten, harass embarrass, or socially exclude (Hinduja & Patchin, 2008; Patchin & Hinduja, 2006; Williams & Guerra, 2007). Cyberstalking is the use of the Internet to target victims and ranges from constant unwanted contact to threats of violence and can escalate into attempts to control

[1] Margaret and Wallace McCain Family Chair in Child and Family, University of Toronto, Factor-Inwentash Faculty of Social Work, Toronto, Ontario, Canada
[2] University of Toronto, Factor-Inwentash Faculty of Social Work, Toronto, Ontario, Canada
[3] Research Methodology, School of Education, Loyola University Chicago, Chicago, Illinois

Corresponding Author:
Faye Mishna, Margaret and Wallace McCain Family Chair in Child and Family, University of Toronto, Factor-Inwentash Faculty of Social Work, 246 Bloor Street West, Toronto, Ontario M5S 1A1, Canada.
Email: f.mishna@utoronto.ca

an individual's behavior (Philips & Morrissey, 2004). Sexual solicitation involves requests to engage in sexual activities/talk or to provide personal sexual information, where the requests are unwanted and/or constitute an illegal relationship (vis-a-vis age of consent restrictions; Mitchell, Wolak, & Finkelhor, 2007). Problematic exposure to pornography involves either (a) exposure to pictures of people who are naked or having sex, without having expected or looked for the pictures, while engaged in activities such as conducting searches or opening e-mail (Mitchell, Wolak, et al., 2007); or (b) compulsively seeking pornography such that the behavior interferes with the youth's life or leads to the commission of criminal offences (i.e., viewing child pornography; Quayle & Taylor, 2006). A comprehensive synthesis of the literature completed at Harvard University details risks associated with Internet activity for children and youth and highlights concerns related to cyber bullying, sexual solicitation, and exposure to problematic content (Schrock & Boyd, 2008).

The prevalence rates of cyber bullying typically range across studies from approximately 10–35% (Agatston, Kowalski, & Limber, 2007; Hinduja & Patchin, 2008; Kowalski & Limber, 2007; Li, 2007; Patchin & Hinduja, 2006; Williams & Guerra, 2007), although some research has found significantly higher rates (Juvonen & Gross, 2008; Raskauskas & Stoltz, 2007). Students who were cyber bullied have reported feelings of sadness, anxiety, and fear, and an inability to concentrate, thus affecting their grades (Beran & Li, 2005, 2007).

The Youth Internet Safety Survey, a U.S. nationally representative telephone survey of 1,500 youth between the ages of 10 and 17 years who use the Internet regularly, was conducted in 2000 and in 2005 (Finkelhor et al., 2000; Wolak, Mitchell, & Finkelhor, 2006). In 2005, 34% of youth reported being exposed to online sexual content they did not want to see, an increase from 25% in 2000. While a smaller proportion of youth Internet users received unwanted sexual solicitations in 2005 (13%) than in 2000 (19%), the number of youth receiving aggressive sexual solicitations, in which sexual solicitors made or attempted to make off-line contact with youth, remained constant (4%). The same percentage (4%) reported that online solicitors asked them for nude or sexually explicit photographs of themselves. Depression, substance use, and delinquency are significantly higher among youth who report being bullied or sexually solicited online (Mitchell, Ybarra, & Finkelhor, 2007). The already low rate at which authorities were informed about online sexual solicitation further decreased between 2000 and 2005, with 9% of incidents of solicitation reported in 2000 compared to 5% in 2005 (Wolak et al., 2006).

Although the research is relatively sparse, efforts to document the impact of cyber abuse provide a picture of the significant repercussions of cyber abuse and the vulnerability of children and youth targeted for abuse. Involvement in cyber bullying as perpetrator or as victim negatively affects youth's mental health over and above traditional bullying (Blais, 2008). Thirty-eight percent of youth who experienced online harassment reported emotional distress as a result of the incident (Ybarra, Mitchell, Wolak, & Finkelhor, 2006), and youth who were online aggressors reported struggling with a number of psychosocial difficulties, including problematic relationships with parents, delinquency, and substance use (Ybarra & Mitchell, 2004a). Depressive symptoms were associated with being sexually solicited online (Ybarra, Leaf, & Diener-West, 2004), while an association has been found between depressive symptoms and being harassed online among youth, particularly males (Ybarra, 2004). It is clear that a focus on prevention and intervention efforts is pivotal to ensure the safety of children and youth for whom technology is increasingly an academic and social necessity and way of life.

Method

Criteria for Inclusion and Exclusion of Studies in the Review[1]

Types of studies. Studies were eligible for the review if (a) the study evaluated a prevention or intervention strategy/program that was administered to children and youth between the ages of 5 and 19 years and/or their parents; (b) the prevention or intervention strategy/program targeted outcomes primarily related to children and youth exposed to the Internet or cell phones; (c) the evaluation used an experimental or two-group quasiexperimental research design that included a no treatment or minimal treatment control group (single-group designs will be excluded); (d) the allocation of study participants to treatment or control group used random allocation and the allocation of study participants to quasiexperimental designs was by parallel group design and created through the use of naturally created groups such as classrooms (the studies will vary with respect to the method of constructing the control group and also vary concerning their use of statistical controls to reduce the threat of selection bias); (e) the study included a postprogram measure of knowledge or behavior regarding cyber abuse and online practices (these may have included surveys of Internet knowledge, awareness of the risks associated with online activity, the development of online safety practices, and measures of the frequency of risky online behaviors); and (f) the evaluation was conducted within the last 10 years. There were no restrictions on the language of the study report or the geographical location of the study.

Types of intervention. In order to conduct this systematic review, the prevention and intervention programs were divided into four strategies to address cyber abuse. Specifically, these included (a) technological and software initiatives used with children and adolescents to block or filter access to inappropriate online content; (b) online and off-line cyber abuse preventive interventions for children and youth delivered through any medium (including face-to-face presentations, video games, interactive software, etc.); (c) online and off-line cyber abuse preventive interventions for parents to protect children from cyber abuse; and (d) therapeutic interventions for children and youth who have experienced cyber abuse.

Search Strategy for Identification of Relevant Studies

Several strategies were used to perform an exhaustive search for literature fitting the eligibility criteria. First, a keyword search was performed with a variety of electronic bibliographic databases (see list of keywords and databases below). Second, we performed hand searches of key journals in the field. Third, we contacted experts in the field to request articles meeting our inclusion criteria. Lastly, we completed a gray literature search for relevant articles.

The following bibliographic databases were searched: Psychological Abstracts (PsycINFO, PsycLIT, ClinPsyc-*clinical subset*); MEDLINE; EMBASE; Database of reviews of effectiveness (DARE online); ChildData (child health and welfare); ASSIA (applied social sciences); Caredata (social work); Social Work Abstracts; Child Abuse, Child Welfare & Adoption; Cochrane Collaboration; C2-SPECTR; Social Sciences Abstracts; Social Service Abstracts; and Dissertation Abstracts International (DAI).

To ensure maximum sensitivity and specificity, subject headings and word text were searched in a systematic process. The search strategy included such terms as child, teen, youth, adolescent, student, Internet, child abuse, prevention, intervention, education, school, program, knowledge, filter, block, police, sex, harass, stalk, pornography, victim, threat, exploit, computer, cyber, Web, e-mail, and net.

Hand searches for content, over the last 10 years, were completed with the following journals: *Youth and Society, Journal of Interpersonal Violence, Annual Review of Sex Research, Computers in Human Behavior, Computers & Education*, and *Journal of Adolescent Health*. Ten experts in the field were contacted. Most responded that they were unaware of any relevant articles, and the few articles that were forwarded to us were not eligible for inclusion or were already included in the review.

Gray literature searching involved a search with the following sites: Google; Canadian Evaluation Society Grey Literature Bank; Criminology Grey Literature; Dissertations and Theses; Proceedings from Professional Conferences, including PapersFirst and ProceedingsFirst; and Government Sources, including the Governments of Canada, United States, and the European Union.

Analytic methods: Calculating effect sizes. The effect size (ES) calculated in this study is standardized mean-change measures (Becker, 1988). It represents the magnitude of the difference between pre- and posttest for each outcome and for treatment and control groups separately. In the I-SAFE study, data from five posttests were collected. The duration between pretest and the second posttest (Time 3) was similar to the duration between pre- and posttests in the Missing Project. Therefore, only the data from Time 3 (second posttest) were used to calculate the ESs, in order to allow for comparison. In the Missing program study, the means and standard deviations for males and females for each outcome were merged before calculating the ES so the results could be compared with the I-SAFE study, in which the results were not separated based on gender. The HAHASO program utilized only one posttest data collection point, at approximately 90 days after the pretest. Given the different focus of the HAHASO program, findings from this study were not directly compared to those from the I-SAFE and Missing evaluations.

The comparison between treatment and control groups for each outcome in each study was conducted using z test with pooled standard deviation. z Tests were used because we were comparing two groups (treatment and control groups) with the ''known variances,'' based on the sampling distributions of the ESs (Howell, 2007). A z statistic larger than 1.96 indicates a significant difference on the ESs between two groups.

Results

Critical Review

Our search strategy uncovered 3,029 studies. The abstracts of these studies were reviewed by two screeners to identify relevant studies (i.e., content relevance and the presence of an evaluation). Most articles were irrelevant to the topic at hand and were therefore excluded. Most of the remaining studies were excluded as a result of lacking the necessary research design or outcome measures. Full-text screening by two screeners identified three studies that met our eligibility criteria, an evaluation of the I-SAFE cyber safety program, an evaluation of the Missing cyber safety program, and an evaluation of an in-school cyber bullying intervention (HAHASO). Details of these studies can be found in Table 3. The two former studies were psychoeducational preventive interventions for children and youth oriented to Internet safety knowledge and online risky behavior. One of these studies was conducted in the United States and the other was conducted in Canada. Both studies were evaluative reports funded by national governments. The HAHASO study employed an anti-bullying strategy—Help, Assert Yourself, Humor, Avoid, Self-talk, Own it—in schools in Connecticut to address traditional face-to-face as well as cyber bullying. The HAHASO study was a doctoral dissertation.

All the studies included in this review utilized a pre- and posttest design with a control group. Students were not randomly assigned to treatment or control group, rather assignment was based on segmentation through classrooms. The intervention was provided by a teacher for both the I-SAFE and the Missing program and by the researcher in the HAHASO program. Attrition in the Missing program was approximately 1% in both the treatment and the control group, and attrition in the I-SAFE program was approximately 7% in the treatment group and 3% in the control group. These low levels suggest there is little to no bias due to attrition in the studies. Attrition was not noted in the HAHASO report. The follow-up period in the Missing program was approximately 3 weeks, the follow-up period in the I-SAFE program extended to approximately 9 months, and follow-up in the HAHASO program was approximately 90 days. The use of the same schools for treatment and control groups may have led to diffusion of treatment. This is a

greater possible concern in the Missing program, in which six of the eight schools provided both treatment and control group classes, as compared to the I-SAFE program, in which only 2 of 18 schools provided both treatment and control classes. Diffusion is a particularly important consideration regarding the HAHASO program, as treatment and control groups were both selected from one intermediate school.

While the Missing and I-SAFE studies are broadly similar, key differences in the operationalization of outcome measures precluded the use of meta-analytic techniques. The I-SAFE study focused on measuring Internet safety knowledge obtained by students after the intervention, while the Missing program focused on measuring the change in Internet safety behaviors and attitudes after the intervention. Due to the disparate outcomes, no combined effects were calculated, but ESs were calculated and compared for both studies. Additionally, given that the HAHASO program focused on cyber bullying behavior, findings cannot be directly compared to those from the I-SAFE or Missing program.

Excluded Studies

Other evaluations of psychoeducational interventions regarding Internet safety were excluded for methodological reasons, such as a lack of control group (Brookshire & Maulhardt, 2005; Gray, 2005; KidSmart, 2002; Wishart, Andrews, & Yee, 2005; Wishart, Oades, & Morris, 2007), qualitative data collection (Davidson & Martellozzo, 2004), and other methodological and outcome limitations (Finn & Kerman, 2004). Evaluations of technological interventions were identified in the search but excluded for not being implemented with children/youth or their parents (Greenfield, Rickwood, & Tran, 2001; Hunter, 2000; Richardson, Resnick, Hansen, Derry, & Rideout, 2002).

Types of cyber abuse interventions in included studies. Three of the articles meeting all criteria offered educational prevention interventions oriented toward children and/or youth concerning Internet safety. The first of these interventions, the I-SAFE curriculum, includes five lessons and youth empowerment activities in the areas of cyber community citizenship, cyber security, personal safety, predator identification, and intellectual property. Lessons were provided by teachers during class time, and almost all activities were off-line in nature. The intervention was provided to students in Grades 5–8. The curriculum was developed to be consistent with Bruner's constructive learning theory, which indicates that "learning is an active process in which students construct new ideas or concepts based upon their current/past knowledge" (Chibnall, Wallace, Leicht, & Lunghofer, 2006, p. 5). The curriculum does not require computer-based learning and is very flexible in its implementation. Outcomes included intellectual property knowledge related to legal rights of purchased media and illegally downloading media; Internet safety knowledge related to items such as chat rooms, predators, computer viruses, and plagiarism; risk management related to perceptions that someone the student meets online would try to contact them or harm them; predator identification through perceptions that someone might try to contact them by appearing to be a youth the same age as themselves; sharing of personal information such as the student's name and where they hang out with friends; and inappropriate online behavior such as being on unsuitable Web sites, looking at inappropriate pictures, and telling a friend their password. The I-SAFE curriculum was taught over a period of 1 to 6 weeks, with five lessons taught lasting approximately 40 min each.

The second educational prevention intervention, the Missing program, includes an interactive computer game designed to encourage youth to develop guidelines for safe Internet use. In contrast to the I-SAFE curriculum, the Missing program comprises a specific resource that requires computer-based interaction. Youth playing the game assumed the role of a police officer and solved a series of puzzles to find a missing teenager. Players of the game are able to see how the Internet predator successfully leverages the teenager's vulnerabilities and uses numerous approaches to gain his trust and to lure him away from home (Crombie & Trinneer, 2003). The game stresses that revealing personal information about oneself on the Internet creates possible vulnerabilities regarding Internet victimization. In addition, by highlighting how this Internet predator misrepresented himself, the game intends to emphasize to children that they should not always trust what they are told by individuals they meet online (Crombie & Trinneer, 2003). Therefore, the program targets (a) open chat room conversations, (b) personal e-mail communication with someone met on the Internet, and (3) personal Web page design and is therefore more specific in its focus than the broader I-SAFE curriculum. In addition to the computer game, the Missing program includes a documentary video, posters and brochures, and a guidebook for teachers and parents. Participation in the game was supervised by teachers, and most teachers facilitated supplementary activities such as the development of Internet safety guidelines or those activities supported by the guidebook. The intervention was provided to students in grades 6 and 7. Outcomes included the frequency of personal information disclosure in open chat rooms, personal e-mail communication with individuals they met online, and personal Web pages; attitudes regarding the safety of disclosing personal information online, trusting people met online, and the likelihood that someone on the Internet would try to lure children away from home; and the development of Internet safety guidelines to four Internet-related situations. The Missing program was administered in three to four classes of approximately 40 to 50 min.

The final intervention, the HAHASO program, includes five classes of instruction on the "Help, Assert Yourself, Humor, Avoid, Self-talk, Own it" anti-bullying strategy. The strategy was focused on face-to-face bullying, with an additional element of data collection related to cyber bullying. The control group did not receive any special instruction outside their normal curriculum. Lessons were provided by the researcher during class time, and the strategy focused on both face-to-face as well as cyber bullying. The intervention was provided to students in grades 5 and 6. Outcomes included the prevalence of

bullying incidents and behaviors at school, on the Internet, and on cellular phones; reactions to bullying; and knowledge of social skills (Salvatore, 2006).

Included studies: ESs. The three reports produced 96 ESs for treatment and control groups in total (22 ESs were from the I-SAFE project; 64 ESs were from the Missing program; 10 ESs were from the HAHASO program). The different outcomes measured in the three reports can be found in Table 1. All the ESs presented in Table 1 have been calculated in the way that all the positive ESs indicate the improvement from the pretests to the posttests.

In the I-SAFE project, the largest effect in the treatment group was on the outcome "Internet safety knowledge" ($d^{trt} = 0.88$), indicating that students' knowledge regarding Internet safety increased 0.88 standard deviation from the pretest to the posttest. Cohen (1988) suggested an ES of .2 is small, an ES of .50 is medium, and an ES of .80 is large. Another practical guideline for synthesis is based on empirical examination provided by Lipsey (1990), who found an ES of 0.15 to be small, 0.45 to be moderate, and 0.90 to be large. According to these, the students' knowledge vastly improved. The control group consistently showed smaller ESs on the outcomes reported in this project.

In the Missing program, the ESs for the open chat room behaviors for the treatment group ranged from −0.35 (disclosing the name of one's city) to 0.00 (disclosing a description of one's appearance). The positive ES indicates less disclosure of personal information from the pretests to the posttests. As for the 11 outcomes related to "reporting the likelihood of posting specific personal information on a personal Web page," the effects of the program for the treatment group ranged from 0.18 (a photo of oneself) to −0.05 (gender), indicating that, after involvement in the program, the students generally slightly decreased the likelihood of posting several forms of information about themselves and their families. The increment of posting gender information was very subtle. A similar pattern was found in the control group on these outcomes but the ESs were generally smaller than those from the treatment group. For the 11 outcomes related to Internet safety attitudes, the positive ESs indicated the improvement of safer attitudes in the posttest. In several outcomes, the control group seemed to have safer attitudes than those in the treatment group in the posttest (e.g., "how likely is it that someone online would pretend to be someone else"; $d^{trt} = 0.13$; $d^{ctrl} = 0.29$).

In the HAHASO program, the ESs in the treatment group ranged from 0.62 ("social skills rating scale"—measuring students' positive social behaviors) to 0.00 ("bully/victim questionnaire"—measuring the occurrences of bullying), indicating that students' behavior and perception of bullying had medium to no change from the pretest to the posttest. The largest ES occurred in the control group in "cyberbullying survey" ($d^{ctrl} = 0.88$), which indicates a decrease of bullying from the pretest to the posttest. At the same time, cyber bullying also decreased in the treatment group ($d^{trt} = 0.37$).

In Table 2, the differences between treatment ES and control ES on each outcome were presented in the "ES^{trt}-ES^{ctrl}" column, followed by the z values from the significant tests of the differences in the "z test" column. In the I-SAFE project, the comparisons of the ESs between treatment and control groups on all outcomes were significant at .05 level (z statistics were larger than 1.96), except for the "inappropriate online behavior" outcome. This finding indicates that the treatment group did retain different knowledge compared to the control group. The most significant difference is "Internet safety knowledge" (ES^{trt}-$ES^{ctrl} = 0.78$*). The differences between treatment and control groups, however, are not statistically significant on the "inappropriate online behavior" outcomes ($z = 0.50$), implying that the intervention did not really significantly change the behavior.

In the Missing program, most of the comparisons between treatment and control groups turned out to be nonsignificant at the .05 level. In other words, the ESs differences we observed between treatment and control groups on most of the outcomes could have happened simply by chance. Specifically, the program did not significantly change most of the students' online behavior and attitudes, except for reducing the likelihood of disclosing one's gender, age, school name, and photo.

In the HAHASO strategy project, the largest ES difference between treatment and control groups was in the rating of "social skills" (ES^{trt}-$ES^{ctrl} = 0.58$), yet the difference is not significant ($z = 1.49$). The rest of ESs was all negative, which indicates that control groups had more changes between the pre- and posttests than the treatment groups. However, none of the difference between treatment and control groups is significant.

There are a few limitations to this analysis. The number of statistical tests performed in this analysis increases the risk of type I error. Additionally, the differences between included studies precluded the completion of a meta-analysis.

Discussion and Applications to Social Work

The aim of this review was to examine all available evidence regarding cyber abuse prevention and intervention initiatives. Based on this comprehensive search of available studies, it is clear that this is an emerging area of research that is only beginning to take form. Results so far provide evidence that participation in cyber abuse prevention and intervention strategies is associated with an increase in Internet safety knowledge. The findings suggest, however, that participation in cyber abuse prevention interventions may not be significantly related to Internet risk attitudes and behavior. Similar to other public health issues, cyber abuse knowledge may not always lead to behavior change. It is important to note, however, that many of the changes reported in the treatment group regarding Internet behavior were in the desired direction, although they were not significant. Therefore, it may be that there was insufficient evidence of an effect in these cases. Additionally, participation in a school-based anti-bullying strategy was not significantly

Table 1. The Effect Size (ES) and the Standard Error (SE) of Each Outcome, and the Sample Sizes (N) for Treatment and Control Groups for the I-SAFE, the Missing Program, and HAHASO Projects[a]

	Treatment		Control	
	ES	*SE*	ES	*SE*
I-SAFE (US)	*N* = 796-1,199		*N* = 528-738	
Intellectual property knowledge: Media	0.46	0.0304	0.05	0.0369
Intellectual property knowledge: Theft	0.21	0.0293	−0.11	0.0371
Internet safety knowledge	0.88	0.0340	0.10	0.0369
Managing risk	0.22	0.0292	0.00	0.0369
Predator identification	0.25	0.0294	−0.15	0.0371
Personal information	0.24	0.0293	0.04	0.0369
Computer virus	0.41	0.0301	0.20	0.0373
Mentoring	0.07	0.0290	0.27	0.0376
E-mail protocol	0.04	0.0355	−0.04	0.0435
Inappropriate online behavior	0.16	0.0291	0.14	0.0371
Comfort level with online acquaintances	0.17	0.0291	0.07	0.0369
Missing Program (Canada)	*N* = 57–181		*N* = 55–157	
1. Open chat room behaviors and E-mailing strangers				
Going to open chat rooms	0.14	0.1168	0.10	0.1166
Disclosing one's name	0.06	0.2087	−0.19	0.1942
Disclosing one's gender	0.07	0.2088	−0.44	0.1981
Disclosing one's age	0.24	0.2116	−0.24	0.1916
Disclosing a description of one's appearance	0.00	0.6803	0.12	0.1896
Disclosing the name of one's city	0.35	0.2148	−0.00	0.1890
Disclosing the name of one's school	0.13	0.2093	0.06	0.1891
Disclosing one's personal e-mail address	0.06	0.2087	−0.16	0.1902
Disclosing one's instant messaging (IM) number/nickname	0.15	0.2097	−0.09	0.1894
E-mailing strangers	0.20	0.1191	0.14	0.1201
2. Reported likelihood of posting specific personal information on a personal Web page				
Full name	0.09	0.1107	0.04	0.1126
Gender	−0.05	0.1105	−0.03	0.1125
Age	0.14	0.1117	0.07	0.1126
A description of one's personal appearance	0.12	0.1108	0.05	0.1133
The name of one's city	0.16	0.1111	0.08	0.1134
Street address	0.13	0.1109	0.06	0.1126
School name	0.07	0.1106	−0.20	0.1143
E-mail address	0.15	0.1124	0.09	0.1135
IM number/nickname	0.00	0.1104	−0.03	0.1133
A photo of oneself	0.18	0.1113	−0.02	0.1125
A photo of one's family	0.09	0.1113	0.11	0.1136
3. Internet safety-related attitudes (*high scores indicates safer attitudes)				
How truthful are people when talk online	0.13	0.1102	0.00	0.1125
How likely is it that someone online would pretend to be someone else	0.13	0.1102	0.29	0.1148
How likely is it that someone online would try to manipulate you	0.24	0.1113	0.24	0.1142
How much can one trust people online	0.00	0.1098	0.03	0.1125
How long do you have to know people met online before trusting them a little	0.14	0.1103	0.19	0.1143
How long do you have to know people met online before trusting them a lot	0.19	0.1107	0.20	0.1143
How likely is it that someone online would try to lure you away from home	0.37	0.1141	0.23	0.1140
How likely is it that someone online would try to lure someone your age away from home	0.06	0.1099	0.04	0.1125
How risky is it to disclose personal information in an open chat room	0.16	0.1111	0.16	0.1132
How risky is it to disclose personal information in e-mail to someone met online	0.22	0.1111	0.04	0.1140
How risky is it to disclose personal information on a personal Web page	0.11	0.1114	0.20	0.1182
HAHASO strategy	*N* = 6		*N* = 6	
Revised Olweus Bully/Victim Questionnaire E01-Senior (RBVQ)	0.00	0.4082	−0.02	0.4083
Cyberbullying Survey	0.37	0.4219	0.88	0.4801
Internal—Bully-Victimization Distress Scale	0.19	0.4118	−0.43	0.4268
External—Bully-Victimization Distress Scale	0.15	0.4107	0.49	0.4318
Social Skills Rating Scale	0.62	0.4463	0.04	0.4084

a. Impacts on internet safety knowledge, risk behavior, and cyber bullying outcomes (effect sizes).

Table 2. The ES Differences Between Treatment and Control Groups (ES^{trt}-ES^{ctrl}) and the z Test Results for Testing the ESs Differences Between Treatment and Control Groups on Each of the Outcomes Studied in the I-SAFE, the Missing Program Projects, and the HAHASO Strategy Project

	ES^{trt}-ES^{ctrl}	*Z* test
I-SAFE (US)		
Intellectual property knowledge: Media	0.41*	12.26*
Intellectual property knowledge: Theft	0.32*	9.85*
Internet safety knowledge	0.78*	22.10*
Managing risk	0.22*	6.86*
Predator identification	0.40*	12.27*
Personal information	0.20*	6.04*
Computer virus	0.20*	6.16*
Mentoring	−0.20*	−6.08*
E-mail protocol	0.09*	2.19*
Inappropriate online behavior	0.02	0.50
Comfort level with online acquaintances	0.10*	3.06*
Missing Program (Canada)		
1. Open chat room behaviors and e-mailing strangers		
Going to open chat rooms	0.04	0.31
Disclosing one's name	0.25	1.26
Disclosing one's gender	0.52*	2.55*
Disclosing one's age	0.48*	2.37*
Disclosing a description of one's appearance	−0.11	−0.22
Disclosing the name of one's city	0.35*	1.71
Disclosing the name of one's school	0.07	0.35
Disclosing one's personal e-mail address	0.22	1.11
Disclosing one's instant messaging (IM) number/nickname	0.24	1.22
E-mailing strangers	0.07	0.56
2. Reported likelihood of posting specific personal information on a personal Web page		
Full name	0.05	0.42
Gender	−0.03	−0.24
Age	0.07	0.67
A description of one's personal appearance	0.07	0.64
The name of one's city	0.08	0.68
Street address	0.07	0.65
School name	0.27	2.38*
E-mail address	0.05	0.49
IM number/nickname	0.04	0.32
A photo of oneself	0.20	1.78
A photo of one's family	−0.02	−0.22
3. Internet safety-related attitudes		
How truthful are people when talk online	−0.13	−1.14
How likely is it that someone online would pretend to be someone else	0.16	1.43
How likely is it that someone online would try to manipulate you	0.01	0.06
How much can one trust people online	0.04	0.32
How long do you have to know people met online before trusting them a little	0.05	0.46
How long do you have to know people met online before trusting them a lot	0.01	0.08
How likely is it that someone online would try to lure you away from home	−0.14	−1.19
How likely is it that someone online would try to lure someone your age away from home	−0.02	−0.22
How risky is it to disclose personal information in an open chat room	0.01	0.05
How risky is it to disclose personal information in e-mail to someone met online	−0.18	−1.60
How risky is it to disclose personal information on a personal Web page	0.09	0.77
HAHASO strategy		
Revised Olweus Bully/Victim Questionnaire E01-Senior (RBVQ)	−0.02	−0.04
Cyberbullying Survey	−0.51	−1.23
Internal—Bully-Victimization Distress Scale	−0.24	−0.64
External—Bully-Victimization Distress Scale	−0.33	−0.87
Social Skills Rating Scale	0.58	1.49

* $p < .05$.

Table 3. Included Articles

Articles meeting all inclusion criteria

Author	Location	Type of Intervention	Time of Study	Sample Size	Population
Chibnall et al. (2006)	Kentucky, Oklahoma and Nebraska, United States	In school administration of the i-safe curriculum	2004–2005	Treatment group = 1328; control group = 771	Grades 5–8 students
Crombie & Trinneer (2003)	British Columbia, Canada	In school administration of the Missing Internet Safety computer program	2002	Treatment group = 181; control group = 157	Grades 6 and 7 students
Salvatore (2006)	Connecticut, United States	In school administration of the "Help, Assert Yourself, Humour, Avoid, Self-talk, Own it" anti-bullying strategy (including cyber bullying)	2005	Treatment group = 138; control group = 138	Students in grades 5 and 6

related to change in the number of incidents of cyber bullying experienced by students.

Specifically, results from the I-SAFE project provide evidence that psychoeducational prevention and intervention strategies are associated with an increase in Internet safety knowledge, which encompasses knowledge of such items as Internet predators, and moderated chat rooms. Findings also suggest that students in the control group increased knowledge regarding how to manage risk while online, including the identification of Internet predators and the safety of divulging personal information. Students who received the intervention were also more likely to discuss online risks with friends or siblings. An increase in knowledge and discourse regarding online safety is an important finding that highlights the value of the I-SAFE project. Despite these increases in knowledge, however, students who received the intervention were not significantly less likely to engage in inappropriate online behavior such as browsing inappropriate sites, giving out their e-mail address to individuals met online, or providing personal passwords to others. Students receiving the intervention did report that they would wait longer to provide personal information to someone they had met online.

Results from the Missing program suggest that participation in the intervention did not significantly change Internet-related safety attitudes or the likelihood of posting most personal information on a personal Web page. While students who received the intervention indicated they were less likely, in communication with strangers, to disclose their gender, age, and name of their city, there was no change in the likelihood of disclosing one's name, description of appearance, personal e-mail address, or school name. Additionally, students who received the intervention were not significantly less likely to participate in open chat rooms and to e-mail strangers.

Results from the HAHASO program suggest that participation in a school-based anti-bullying intervention did not change the number of reported cyber bullying incidents experienced by participants.

The generalizability of these findings to all children and youth is influenced by the narrow age range of participants (grades 5 to 8). No information is provided regarding the applicability of these interventions to younger or older children and youth.

The results of this systematic review are timely given the increasing interest in combating cyber abuse. The findings highlight that cyber abuse is a complex issue and that although important, changing attitudes may not be sufficient to change behavior of children and youth with respect to risky online behavior. Developers of cyber abuse programs must create prevention and intervention strategies that do more than increase awareness of the potential threats of the Internet. Emphasis must be placed on actually decreasing risky online behaviors.

Additionally, the importance of educating parents, caregivers, and teachers about the potential risks associated with online activities must be underlined. Parents need to become more knowledgeable and adept regarding technology and require greater understanding about both opportunities and risks presented by the Internet. Parents and other significant adults in children's lives also require effective strategies to engage with their children regarding online activity. Educational initiatives for parents must include a contextualized understanding of the importance of technology in the lives of children and youth in order to build an appreciation of the complexity of online risk behavior.

Despite the attention provided to cyber abuse by the media and the public, there is a surprising and discouraging paucity of rigorous cyber abuse prevention and intervention evaluations. Additional research is vital to greater understanding in this important field. The research implication growing out of this review is that additional research is necessary to explore the link between Internet safety knowledge generation and risky online behavior. While research that can clearly delineate the impact of psychoeducational interventions on Internet safety knowledge is important, the link between psychoeducational interventions and risky online behavior change remains unclear. Further research is also necessary to explore the impact of these forms of interventions on younger children as well as older youth, given that the studies in this review focused only on middle school children in grades 5 to 8. Additionally, research that explores the use of technological interventions with children and youth is necessary to explore opportunities to reduce risk through software filtering and blocking programs. Lastly, research that explores anti-bullying strategies

with a greater focus on cyber bullying is vital in order to examine opportunities to reduce cyber bullying among children and adolescents.

Note

1. For more detail regarding methodology and results, please see the full review on the Campbell Collaboration Web site: http://www.campbellcollaboration.org/library.php

Authors' Note

This paper was invited and accepted by the Editor and is based on a completed Campbell Collaboration Systematic Review. The complete review may be found at: http://www.campbellcollaboration.org/library.php. The Campbell Collaboration mechanism for extensively processing, reviewing, and approving systematic reviews replaced the journal's usual blind peer system. The authors of other approved Campbell and Cochrane Collaboration Systematic Reviews are encouraged to contact the editor about the possibility of this journal publishing a version of their review.

Declaration of Conflicting Interests

The author(s) declared no conflicts of interest with respect to the authorship and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research and/or authorship of this article: Bell Canada and the Campbell Collaboration, and SFI Campbell, The Danish National Centre for Social Research.

References

Agatston, P., Kowalski, R., & Limber, S. (2007). Students' perspectives on cyber bullying. *Journal of Adolescent Health*, *41*, S59-S60.

Aloysius, C. (2001). The media response: A journalist's view of the problem in Asia. In C. A. Arnaldo (Ed.), *Child abuse on the Internet: Ending the silence* (pp. 157-162). Paris: Berghahn Books and UNESCO.

Arnaldo, C. A., & Finnström, A. (1998). Youth and communication. In U. Carlsson & C. von Feilitzen (Eds.), *Children and media violence* (pp. 35-41). Göteborg: The UNESCO International Clearinghouse on Children and Violence on the Screen.

Becker, B. J. (1988). Synthesizing standardized mean-change measures. *British Journal of Mathematical and Statistical Psychology*, *41*, 257-278.

Beran, T., & Li, Q. (2005). Cyber-harassment: A study of a new method for an old behavior. *Journal of Educational Computing Research*, *32*, 265-277.

Beran, T., & Li, Q. (2007). The relationship between cyberbullying and school bullying. *Journal of Student Wellbeing*, *1*, 15-33.

Berson, I. R., Berson, M. J., & Ferron, J. M. (2002). Emerging risks of violence in the digital age: Lessons for educators from an online study of adolescent girls in the United States. *Meridian: A Middle School Technologies Journal*, *5*, 1-32.

Blais, J. (2008). *Chatting, befriending, and bullying. Adolescents' Internet experiences and associated psychosocial outcomes.* Unpublished dissertation, Queen's University.

Brookshire, M., & Maulhardt, C. (2005). *Evaluation of the effectiveness of the NetSmartz program: A study of Maine public schools*. Retrieved December 9, 2008, from http://www.netsmartz.org/pdf/gw_evaluation.pdf

Chibnall, S., Wallace, M., Leicht, C., & Lunghofer, L. (2006). *I-safe evaluation. Final Report*. Caliber Association, Fairfax. Retrieved December 8, 2008, from http://www.ncjrs.gov/pdffiles1/nij/grants/213715.pdf

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum.

Cowburn, M., & Dominelli, L. (2001). Masking hegemonic masculinity: Reconstructing the paedophile as the dangerous stranger. *British Journal of Social Work*, *31*, 399-415.

Crombie, G., & Trinneer, A. (2003). *Children and Internet safety: An evaluation of the Missing Program. A report to the Research and Evaluation Section of the National Crime Prevention Centre of Justice Canada.* Ottawa: University of Ottawa.

Davidson, J. C., & Martellozzo, E. (2004). *Educating children about sexual abuse and evaluating the Metropolitan Police Safer Surfing Programme.* London, UK: Metropolitan Police.

Durkin, K., & Low, J. (1998). Children, media and aggression: Current research in Australia and New Zealand. In U. Carlsson & C. von Feilitzen (Eds.), *Children and media violence* (pp. 107-124). Göteborg: The UNESCO International Clearinghouse on Children and Violence on the Screen.

Finkelhor, D., Mitchell, K. J., & Wolak, J. (2000). *Online victimization: A report on the Nation's youth*. National Center for Missing & Exploited Children. Retrieved December 8, 2008, from http://www.unh.edu/ccrc/pdf/jvq/CV38.pdf

Finn, J., & Kerman, B. (2004). Internet risks for foster families online. *Journal of Technology in Human Services*, *22*, 21-38.

Gray, S. (2005). *Internet safety and the intermediate student*. Unpublished dissertation, Royal Roads University.

Greenfield, P., Rickwood, P., & Tran, H. C. (2001). *Effectiveness of Internet filtering software products*. A report for NetAlert and the Australian Broadcasting Authority. Retrieved December 8, 2008, from http://www.acma.gov.au/webwr/aba/newspubs/documents/filtereffectiveness.pdf

Hinduja, S., & Patchin, J. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior*, *29*, 129-156.

Howell, D. C. (2007). *Statistical methods for psychology* (6th ed.). Pacific Grove, CA: Duxbury.

Hunter, C. D. (2000). Internet filter effectiveness—testing over- and underinclusive blocking decisions of four popular web filters. *Social Science Computer Review*, *18*, 214-222.

Juvonen, J., & Gross, E. F. (2008). Extending the school grounds?—Bullying experiences in cyberspace. *Journal of School Health*, *78*, 496-505.

KidSmart. (2002). Childnet's Kidsmart Schools Internet Safety Project. Retrieved December 8, 2008, from http://www.childnet-int.org/downloads/kidsmart-summary.pdf

Kowalski, R., & Limber, S. (2007). Electronic bullying among middle school students. *Journal of Adolescent Health*, *41*, S22-S30.

Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior*, *23*, 1777-1791.

Lipsey, M. W. (1990). *Design sensitivity: Statistical power for experimental research.* Thousand Oaks, CA: SAGE.

Mitchell, K. J., Finkelhor, D., & Wolak J. (2001). Risk factors for and impact of online sexual solicitation of youth. *JAMA*, *285*, 3011-3014.

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2003). The exposure of youth to unwanted sexual material on the Internet: A National survey of risk, impact, and prevention. *Youth & Society*, *34*, 330-358.

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2007). Trends in youth reports of sexual solicitations, harassment and unwanted exposure to pornography on the Internet. *Journal of Adolescent Health*, *40*, 116-126.

Mitchell, K. J., Ybarra, M., & Finkelhor, D. (2007). The relative importance of online victimization in understanding depression, delinquency, and substance use. *Child Maltreatment*, *12*, 314-324.

Patchin, J., & Hinduja, S. (2006). Bullies move beyond the school yard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, *4*, 148-169.

Philips, F., & Morrissey, G. (2004). Cyberstalking and cyberpredators: A threat to safe sexuality on the Internet. *Convergence: The International Journal of Research into New Media Technologies*, *10*, 66-79.

Quayle, E., & Taylor, M. (2006). Young people who sexually abuse: The role of the new technologies. In M. Erooga & H. Masson (Eds.), *Children and young people who sexually abuse others: Current developments and practice responses* (2nd ed). New York: Routledge.

Raskauskas, J., & Stoltz, A. D. (2007). Involvement in traditional and electronic bullying among adolescents. *Developmental Psychology*, *43*, 564-575.

Richardson, C. R., Resnick, P. J., Hansen, D. L., Derry, H. A., & Rideout, V. J. (2002). Does pornography blocking software block access to health information on the Internet? *Journal of the American Medical Association*, *288*, 2887-2894.

Salvatore, A. (2006). An anti-bullying strategy: Action research in a 5/6 intermediate school. *Dissertation Abstracts International Section A: Humanities and Social Sciences*, *67*(3-A), 891.

Schrock, A., & Boyd, D. (2008). *Online threats to youth: Solicitation, harassment, and problematic content*. Research Advisory Board Report for the Internet Safety Technical Task Force. Berkman Centre for Internet & Society at Harvard University. Retrieved July 9, 2009, from http://cyber.law.harvard.edu/pubrelease/isttf/

Sellier, H. (2001). The world citizens' movement to protect innocence in danger. In C. A. Arnaldo (Ed.), *Child abuse on the Internet: Ending the silence* (pp. 173-175). Paris: Berghahn Books and UNESCO.

Williams, K. R., & Guerra, N. G. (2007). Prevalence and predictors of Internet bullying. *Journal of Adolescent Health*, *41*, S14-S21.

Wishart, J. M., Andrews, J., & Yee, W. C. (2005). *Evaluation of the 'Getting to Know IT All' presentation as delivered in UK schools during November 2005.* Bristol: University of Bristol.

Wishart, J. M., Oades, C. E., & Morris, M. (2007). Using online role play to teach Internet safety awareness. *Computers & Education*, *48*, 460-473.

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2006). *Online victimization of youth: Five years later.* Washington, DC: National Center for Missing and Exploited Children.

Ybarra, M. L. (2004). Linkages between depressive symptomatology and Internet harassment among young regular Internet users. *Cyberpsychology & Behavior*, *7*, 247-257.

Ybarra, M. L., Leaf, P. J., & Diener-West, M. (2004). Sex differences in youth-reported depressive symptomatology and unwanted Internet sexual solicitation. *Journal of Medical Internet Research*, *6*, e5.

Ybarra, M. L., & Mitchell, K. J. (2004a). Youth engaging in online harassment: Associations with caregiver-child relationships, Internet use, and personal characteristics. *Journal of Adolescence*, *27*, 319-336.

Ybarra, M. L., & Mitchell, K. J. (2004b). Online aggressor/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry*, *45*, 1308-1316.

Ybarra, M. L., Mitchell, K. J., Wolak, J., & Finkelhor, D. (2006). Examining characteristics and associated distress related to Internet harassment: Findings from the second youth Internet safety survey. *Pediatrics*, *118*, 1169-1177.