Campbell Systematic Reviews
2009:2
First published: 26 August, 2009
Last updated: 9 July, 2009

Interventions for Children, Youth, and Parents to Prevent and Reduce Cyber Abuse

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

THE CAMPBELL COLLABORATION

Colophon

Title	Interventions for children, youth, and parents to prevent and reduce cyber abuse.
Institution	The Campbell Collaboration
Authors	Mishna, Faye Cook, Charlene Saini, Michael Wu, Meng-Jia MacFadden, Robert
DOI	10.4073/csr.2009.2
No. of pages	54
Last updated	9 July, 2009
Citation	Mishna F, Cook C, Saini M, Wu M-J, MacFadden R. Interventions for children, youth, and parents to prevent and reduce cyber abuse. Campbell Systematic Reviews 2009:2 DOI: 10.4073/csr.2009.2
Copyright	© Mishna et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.
Keywords	
Support/Funding	This systematic review was funded by Bell Canada and co-sponsored by SFI Campbell, The Danish National Centre for Social Research and The Campbell Collaboration.
Potential Conflicts of Interest	There are no known conflicts of interest.

Corresponding author	Faye Mishna, PhD, RSW Professor Associate Dean of Research Factor-Inwentash Faculty of Social Work Margaret and Wallace McCain Family Chair in Child and Family University of Toronto 246 Bloor Street West Toronto, Ontario M5S 1A1 Canada (416) 978-1385 f.mishna@utoronto.ca

Campbell Systematic Reviews

The Campbell Collaboration (C2) was founded on the principle that systematic reviews on the effects of interventions will inform and help improve policy and services. C2 offers editorial and methodological support to review authors throughout the process of producing a systematic review. A number of C2's editors, librarians, methodologists and external peer-reviewers contribute.

The Campbell Collaboration
P.O. Box 7004 St. Olavs plass
0130 Oslo, Norway
www.campbellcollaboration.org

Table of contents

Executive summary/Abstract

BACKGROUND

The Internet has created a new communication tool, particularly for young people whose use of e-mail, websites, instant messaging, web cams, chat rooms, social networking sites and text messaging is exploding worldwide. While there are many benefits that result from electronic based communication, the Internet is, however, concurrently a potential site for abuse and victimization, whereby young people can fall victim to sexual perpetrators, stalkers, exploiters, and peers who bully online. Interventions regarding cyber abuse have been developed in response to a growing emphasis on protecting children and youth from online dangers.

OBJECTIVES

To examine the effectiveness of cyber abuse interventions in increasing Internet safety knowledge and decreasing risky online behaviour.

SELECTION CRITERIA

The scope of this review is experimental and quasi-experimental prevention and intervention strategies that target children ages 5 to 19 years old and/or their parents, utilize a control group, and examine an outcome related to cyber abuse such as Internet safety knowledge, risky online behaviour, or exposure to inappropriate online content.

SEARCH STRATEGY

We searched the following databases : 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; Dissertation Abstracts International (DAI). We also handsearched Youth and Society; Journal of Interpersonal Violence; Annual Review of Sex

Research; Computers in Human Behavior; Computers & Education; and Journal of Adolescent Health. Additionally, we contacted experts in the field and searched for grey literature.

DATA COLLECTION AND ANALYSIS

Two screeners reviewed abstracts and full-text of all articles. Three articles met all inclusion criteria, and effect sizes and z-tests were calculated for all relevant outcomes.

MAIN RESULTS

Significant z-tests were found between pre-and post-test scores on measures related to Internet safety knowledge such as managing online risk and identifying online predators. Most z-tests related to pre- and post- measures of risky online behaviour were not significant, including disclosing one's name, participating in open chat rooms, or emailing strangers.

REVIEWERS' 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 behaviour. The need for further research in this field is highlighted.

1 Background

1.1 DEFINITION OF CYBER ABUSE

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 e-mail, websites, instant messaging, web cams, chat rooms, social networking sites and text messaging is exploding worldwide. There is evidence, for example, that young people's use of the Internet is now a preferred pastime over watching television (Kaynay & Yelsma, 2000; Nie & Hillygus, 2002).

While there may be many benefits that result from electronic based communication, 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, 2003; Ybarra & Mitchell, 2004a, 2004b). These findings have been supported by studies from 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 a wide range of activities including cyber bullying, cyber stalking, cyber sexual solicitation, and cyber pornography. Cyber bullying includes the use by peers of email, cell phones, text messages, and Internet sites to threaten, harass, embarrass, socially exclude, or damage reputations and friendships. Cyber stalking, as an extension of the physical form of stalking, is where individuals utilize electronic mediums such as email, cell phones, text messages, and Internet sites to pursue, harass or contact another in an unsolicited fashion. Cyber sexual solicitation is the use of electronic media such as email, cell phones, text messages, and Internet sites by adults to identify, "groom,"

and entice children and youth to perform sexual acts online or offline. Cyber pornography includes the production and dissemination of and exposure to graphic sexual content through technology, such as email, cell phones, text messages, and Internet sites.

1.2 PREVALENCE AND IMPACT OF CYBER ABUSE

Prevalence studies have highlighted the extent of the impact of cyber abuse in the lives of children and youth. A recent and comprehensive synthesis of the literature completed at Harvard University details the risks associated with Internet activity for children and youth, and particularly highlights concerns related to sexual solicitation, cyber bullying, and exposure to problematic content (Schrock & Boyd, 2008). This review draws heavily on the results of the Youth Internet Safety Survey, a US nationally representative telephone survey of 1500 youth between the ages of 10 and 17 who use the Internet regularly. The Youth Internet Safety Survey was first conducted in 2000 and subsequently updated in 2005 (Finkelhor et al., 2000; Wolak, Mitchell, & Finkelhor, 2006). The Youth Internet Safety Survey highlighted exposure to cyber pornography as well as experience with cyber sexual solicitation and cyber bullying.

With respect to cyber pornography, 34 percent of youth reported being exposed to sexual content online that they did not want to see in 2005, an increase from 25 percent in 2000. Cyber stalking through online harassment also increased, to nine percent of youth Internet users in 2005 from six percent in 2000. While a smaller proportion of youth Internet users received unwanted sexual solicitations in 2005 (13 percent) than in 2000 (19 percent), the number of youth Internet users receiving aggressive sexual solicitations – in which sexual solicitors made or attempted to make offline contact with youth – remained the same. Most disturbingly, the already low rate at which authorities were informed about online sexual solicitation decreased during the period between 2000 and 2005, with nine percent of incidents of solicitation reported in 2000, compared to only five percent in 2005 (Wolak et al., 2006).

In 2002, the National Centre for Missing and Exploited Children conducted a survey of 1,501 youths, ages 10 to 17, with similar results. One in five of the youth were found to have received a sexual solicitation over the Internet in that year. Three percent had received an aggressive sexual solicitation (offered to meet somewhere, called on the telephone, or received money or gifts), and one in four reported unwanted exposure to nude pictures or people engaged in sex. Results of the survey also indicated that less than 10 percent of these approaches were ever reported to police and only 40 percent of the incidents were mentioned to parents (Magid, 1998).

Cyber bullying is defined as "the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group, that is intended to harm others" (Belsey, 2008). Cyber bullying includes the use of email, cell phones, text messages, and Internet sites to threaten, harass embarrass, or socially exclude (Patchin & Hinduja, 2006; Williams & Guerra, 2007). Cyber bullying further encompasses the use of an electronic medium to sexually harass between peers (Hinduja & Patchin, 2008; Shariff & Johnny, 2007), including distributing unsolicited text or photos of a sexual nature or peer-to-peer requests for sexual acts either online or offline. The findings of the Youth Internet Safety Survey are that approximately one in five youth reported experience with online harassment within the past year (Ybarra & Mitchell, 2004a). A study conducted in a Canadian city found that about 70 percent of students reported hearing about incidents of cyber-bullying, 21 percent had been bullied several times, and 3 percent reported engaging in this form of bullying (Beran & Li, 2005). A considerable percentage of youth who identified being bullied online also reported that they were targets of traditional bullying, whereas other youth reported being victims of online harassment but not of traditional bullying. Three percent of the youth reported being both aggressors and targets, four percent reported being targets only and 12 percent reported acting aggressively towards others online. A study by the Cyberspace Research Unit at the University of Central Lancashire found that of the one in four young people who reported being bullied through email or text messaging approximately one-third will never tell anyone about the harassment (O' Connell, Price & Barrow, 2004). This corresponds with the findings that a significant percentage of children who are bullied through traditional methods do not tell anyone (Hanish & Guerra, 2000; Mishna, Pepler, & Wiener, 2006).

Although not identical phenomena, research on traditional bullying can be used as a starting point for examining online bullying (Ybarra & Mitchell, 2004b), leading to concerns regarding the social, emotional and academic impact of cyber bullying on children and youth. Beran and Li (2005) administered a survey asking students about their reactions to cyber bullying. The majority of students reported feelings of sadness, anxiety, and fear, and stated that it affected their ability to concentrate on their school work and to attain good marks. Findings suggest that the effects of traditional bullying may be far-reaching for children who bully and who are victimized, both of whom are at risk of experiencing emotional, social, and psychiatric problems that may persist into adulthood (Craig, 1998; Crick & Bigbee, 1998; Nansel, Overpeck, Pilla, Ruan, Simons-Morton, Scheidt, 2001; O'Connell, Pepler, & Craig, 1999). One significant difference between online and traditional bullying is the perceived anonymity of the child who bullies in the case of online harassment (Ybarra & Mitchell, 2004b).

As with traditional bullying, a systemic-ecological framework is considered essential in order to understand and address cyber abuse, including cyber bullying, cyber stalking, cyber sexual solicitation and cyber pornography (Atlas & Pepler, 1998;

Hanish & Guerra, 2000; Olweus, 1994). This framework builds on the assumption that, since people are embedded in social and environmental contexts, multiple factors invariably contribute to social behavioural patterns (Cairns & Cairns, 1991; Germain & Bloom, 1999). According to this conceptual framework, cyber abuse does not reside solely with the child or youth who experiences cyber abuse or who is victimized, but unfolds in the social context of the peer group, the classroom, the school, the family and the larger community and society as a whole. The victimized child's inability to defend him/herself is integral. Given the belief that protection from abuse is a fundamental human right, others are obliged to intervene (Atlas & Pepler, 1998; Olweus, 1997).

Though 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. Thirty-eight percent of youth who experienced online harassment reported emotional distress as a result of the incident (Ybarra et al., 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, 2000a). 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.

1.3 THE CURRENT STATE OF RESEARCH

A search of peer reviewed journals and the grey literature has uncovered a growing emphasis on protecting children and youth from the dangers of the Internet. Currently, the focus of the literature seems to be education and technological initiatives, with additional focus on the need for greater attention to therapeutic issues (Wolak, Finkelhor, Mitchell & Ybarra, 2008).

In the field of education, several programs have been developed to educate children and youth about the risks of Internet use (Chibnall, Wallace, Leicht, & Lunghofer, 2006; Crombie & Trinneer, 2003; Davidson & Martellozzo, 2005; Gray, 2005; KidSmart, 2002; Wishart, Andrews, & Yee, 2005). Efforts to educate children, youth, and parents regarding the dangers of online activity have received particular emphasis in the prevention and intervention grey literature. Education efforts for children and youth are predominantly administered by teachers and located within school settings (Chibnall et al., 2006; Crombie & Trinneer, 2003; Davidson & Martellozzo, 2005; Gray, 2005; KidSmart, 2002; Wishart et al., 2005). Education efforts have also been extended to parents and caregivers (Finn & Kerman, 2004). In addition to presentations, innovative educational media for use with children and youth include computer games (Crombie & Trinneer, 2003), cyber solicitation

simulations (Davidson & Martellozzo, 2005), and websites (KidSmart, 2002). Preliminary research has also shown that children appear to be responsive to Internet safety messages within the context of drama-based learning (Berson & Berson, 2002; KidSmart, 2002).

Educational efforts are aimed at a range of student ages, with a particular emphasis on middle-school children (Crombie & Trinneer, 2003; Davidson & Martellozzo, 2005; Gray, 2005). Educational efforts have been undertaken in England (Davidson & Martellozzo, 2005; KidSmart, 2002; Wishart et al., 2005), the United States (Chibnall, Wallace, Leicht, & Lunghofer, 2006), and Canada (Crombie & Trinneer, 2003; Gray, 2005). Research to evaluate these educational efforts has focused on assessing outcomes related to children's knowledge of online safety strategies, knowledge of dangers involved in Internet use, and high risk online behaviour.

Technological initiatives have also been developed, including new strategies to block children's access to unapproved websites (Censorware Project, 2000; Richardson et al, 2002; Schneider, 1997) and to filter graphic descriptions and images (Hunter, 2000; Schneider, 1997) The most comprehensive report in this regard is the recent "Enhancing child safety and online technologies: Final report of the Internet safety technical task force" (Internet Safety Technical Task Force, 2008). This report, directed by Harvard University, explores technological approaches to online safety, with a particular focus on social networking sites. While the report does not evaluate the technical merit of the reviewed technologies, the authors highlight the potential for online protections provided through technological innovations (Internet Safety Technical Task Force, 2008). Additional research has been undertaken into the role of technological solutions to cyber abuse. In particular, the efficacy of technological efforts to block websites with sexual or other inappropriate and offensive content has been analyzed (Censorware Project, 2000; Richardson et al, 2002; Schneider, 1997). The importance of filtering software is evident in research noting that children and youth will evade rule based restrictions placed by their parents on Internet use (Livingstone & Bober, 2005). The associations between technological preventions and exposure to sexual materials (Mitchell, Finkelhor, & Wolak, 2003) and Internet harassment (Ybarra & Mitchell, 2004) have also been assessed. Intended outcomes include the ability of technological intervention to filter or block sexual content.

Internet filtering and site blocking have been shown to be reasonably effective in reducing – but not eliminating – the amount of sexual content to which children are exposed online (Hunter, 2000; Mitchell et al., 2003; Schneider, 1997). In addition, software was found to improperly block benign content (Hunter, 2000; Schneider, 1997). The connection between the amount of sexual content that passed through the filter and the amount of benign content improperly filtered was found to be related to the level of block setting used (Richardson et al, 2002). While filtering

software was associated with a decrease in exposure to sexual content, it was not linked to a decrease in Internet harassment (Ybarra & Mitchell, 2004).

The perceptions of filtering and blocking software have been researched with variable results. Research on the perceptions of filter users has highlighted a lack of product understanding, noting that librarians indicated little knowledge of the programs their school libraries utilize (Curry & Haycock, 2001). The receptivity of those more knowledgeable about filtering software has been more positive, with foster parents who were given a software filtering program noting fewer household problems associated with online pornography and violence (Finn & Kerman, 2004). Of particular interest is the benefit of using technological solutions to cyber abuse with, rather than on, children and youth given the tendency among children and youth to evade restrictions unilaterally placed on their Internet use (Livingstone & Bober, 2005).

Internet safety and prevention is a young field beginning to take shape, both through strategies developed to provide Internet safety for children and youth and through empirical research to evaluate the effectiveness of such strategies. Recent web-based evaluations have been located within the grey literature, some of which use quasi-experimental designs with outcome measures to evaluate program efficacy such as children's knowledge of online safety strategies, knowledge of dangers involved in Internet use, and high risk online behaviors. Other programs have reported plans to conduct such evaluations. These developments demonstrate that the field is maturing in both sophistication and rigor. It is imperative that these strategies be systematically reviewed to ensure the field moves in directions that are informed by empirical evidence.

1.4 CONTRIBUTION OF THIS REVIEW

This systematic review will have implications for policy, practice, and research. In particular, the review could influence educational policy and practice as well as future research in cyber abuse prevention and interventions to ameliorate victimization. Evidence regarding the efficacy of prevention and intervention strategies with regards to cyber safety and cyber abuse will be disseminated to child and youth service agencies, children's mental health organizations, public awareness organizations, schools, researchers, policy makers and parents, children and youth. As well, results will be made available to Internet service providers so they can compare these results with their current protection mechanisms and identify gaps and emerging trends. By systematically reviewing the current state of prevention and intervention strategies to address cyber abuse, this review will contribute to a research agenda that develops stringent criteria to best test for program effectiveness.

2 Objectives of the Review

The primary purpose of this review was to conduct a comprehensive examination of the literature in order to collect all the evidence regarding strategies to prevent and intervene with respect to cyber abuse and to systematically review the evidence to determine the best ways to prevent and intervene with cyber abuse and keep children and youth safe. Cyber abuse is defined as the abuse of children or adolescents in the form of bullying, sexual solicitation, stalking, or child pornography, or any other type of physical or emotional harm enabled by the use of the Internet and other forms of information and communication technology, such as text messaging or the use of cellular telephone cameras. Cyber safety is defined as the condition of being safe online, which includes freedom from danger, risk, threat or injury while online. The increase of cyber safety has been explored by means of various approaches to promote cyber safety through prevention and intervention strategies designed to develop knowledge and awareness among children, adolescents and their parents to reduce risky behaviors online.

Specifically, we aimed to:

- Identify the maximum possible number of articles on prevention of and intervention with respect to cyber abuse in relation to children and adolescents published during the past 10 years;
- Synthesize the evidence contained in published and unpublished literature on prevention and intervention to combat cyber abuse; and
- Identify major gaps to guide future research efforts.

In addition we aimed to explicate how cyber abuse is understood in the literature and to assist practitioners and policy makers involved in the early detection and management of cyber abuse involving children and adolescents.

3 Methods

3.1 CRITERIA FOR INCLUSION AND EXCLUSION OF STUDIES IN THE REVIEW

3.1.1 Types of studies

Studies were eligible for the review if 1) the study evaluated a prevention or intervention strategy/program which was administered to children and youth between the ages of 5 and 19 years and/or their parents; 2) the prevention or intervention strategy/program targeted outcomes primarily related to children and youth exposed to the Internet or cell phones; 3) the evaluation used an experimental or two-group quasi-experimental research design which included a no treatment or minimal treatment control group (single-group designs will be excluded); 4) the allocation of study participants to treatment or control group used random allocation and the allocation of study participants to quasi-experimental designs were 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); 5) the study included a post-program 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 6) 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.

Operational definition of cyber abuse included cyber bullying, cyber stalking, cyber sexual solicitation and cyber pornography. Whenever possible, we coded these types of cyber abuse separately in the analysis. To be included in the review, evaluations must have included children and youth exposed to the Internet or cell phone and/or their parents, however, we were flexible regarding the amount of exposure to the Internet. Regarding the control group, our preliminary search found that evaluations of cyber abuse prevention and intervention strategies mostly used control groups that received no treatment. But we planned to code for different types of control groups, including groups receiving some other treatment.

3.1.2 Types of participants

The population comprised of children and adolescents who use the Internet or cell phones and are therefore vulnerable to being victimized by cyber abuse, children and adolescents who have been victimized through cyber means, and children and adolescents who have been perpetrators of cyber abuse. School-aged children and adolescents were included in this review (we had an expected age range of 5-19 years old). Based on previous research that has identified the importance of parental involvement and parental monitoring to reduce cyber abuse (Chibnall, Wallace, Leicht, & Lunghofer, 2006), we also planned to include studies that use a sample of parents, although it was our intention to treat these studies separately in the analysis.

3.1.3 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

1. Technological and software initiatives used with children and adolescents to block or filter access to inappropriate online content;
2. Online and offline cyber abuse preventive interventions for children and youth delivered through any medium (including face-to-face presentations, video games, interactive software, etc);
3. Online and offline cyber abuse preventive interventions for parents to protect children from cyber abuse;
4. Therapeutic interventions for children and youth who have experienced cyber abuse.

We searched for all potential prevention and intervention studies based on technological, psychoeducational, and therapeutic interventions to prevent cyber abuse. Technological measures included the use of any of the following with children and adolescents: installation of firewalls; installation of antivirus or anti-Trojan software; installation of a key logger; and installation of privacy filters. Psychoeducational measures included: both online prevention strategies and traditional “offline” strategies with the primary goal to protect children and adolescents from becoming victimized through cyber abuse. The term “online” refers to web-based prevention strategies found on various Internet sites. “Offline,” in contrast, refers to direct contact with children and youth and their parents by informing them of strategies to protect against cyber abuse. Therapeutic interventions included both online and offline strategies to help individuals who have been involved in cyber abuse as either victimized or as abusing others. It was important to differentiate the various strategies because the primary goal and timing

of each may be different (e.g., in therapeutic approaches, counseling or therapy occurs after the child or adolescent has been victimized, or has victimized others, unlike preventive strategies, which aim to improve the conditions so that cyber abuse does not occur in the first place).

Two reviewers categorized the type of prevention or intervention based on the above definition of terms. In situations in which the reviewers did not agree on a selected category, the conflict was resolved by a third party (see Selection of Articles).

3.1.4 Types of outcome measures

The primary outcomes of interest for this systematic review included: 1) cyber abuse of children and adolescents; 2) risky behaviors by children and adolescents; 3) knowledge related to cyber abuse; and 4) negative impact on psychological state among those who have been victimized by cyber abuse. These outcomes were considered separately based on the type of prevention/intervention subgroup:

1. The outcome for technological and software initiatives include an assessment of child and youth exposure to inappropriate web-based content.
2. The outcomes for online and offline preventive interventions for children and youth focused on an assessment of knowledge of cyber safety post-intervention and of whether any measured change in knowledge influences future events of cyber abuse and/or risky behaviors while online. A change of mean scores on these measures were compared to the change of means for the control groups.
3. The outcomes for preventive interventions for parents focused on an assessment of knowledge of technology and increased monitoring to reduce children's exposure to cyber abuse post-intervention and on whether any change in monitoring influences future events of cyber abuse and/or risky behaviors while online.
4. The outcomes for therapeutic interventions for children and youth affected by cyber abuse included an assessment of risky online behaviors post intervention, as well as an assessment of adverse outcomes experienced by those victimized by cyber abuse.

3.2 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 grey literature search for relevant articles.

3.2.1 Literature search strategy for identification of appropriate studies

Bibliographic databases:

1. Psychological Abstracts (PsycINFO, PsycLIT, ClinPsyc-clinical subset)
2 MEDLINE
3. EMBASE
4 Database of reviews of effectiveness (DARE online),
5. ChildData (child health and welfare)
6. ASSIA (applied social sciences)
7. Caredata (social work)
8. Social Work Abstracts
9. Child Abuse, Child Welfare & Adoption
10. Cochrane Collaboration
11. C2-SPECTR
12. Social Sciences Abstracts
13. Social Service Abstracts
14. Dissertation Abstracts International (DAI)

To ensure maximum sensitivity and specificity, subject headings and word text were searched in a systematic process. Searches for MEDLINE are as follows (search was modified according to the specific database).

1. Child/
2. Internet/
3. “exp” Internet
4. Child Abuse/
5. "exp" Child Abuse
6. Prevention/
7. “exp” Prevention
8. Intervention/
9. “exp” Prevention
10. “3” AND “5”
11. “3” AND “7”
12. “3” AND “9”
13 ((AB=(child$ or teen$ or youth or adolescen$ or student or kid)) and (AB=(saf$ or prevent$ or educat$ or school$ or program$ or knowledge or reduc$ or train$ or filter$ or block$ or polic$ or intervention)) and (AB=(sex$ or harass$ or stalk$ or porn$ or flash$ or abus$ or bull$ or cim$ or victim$ or erot$ or pedophil$ or paedophil$ or molest$ or rape$ or torment or smut$ or cruel$ or evil$ or viol$ or solicit$ or maltreat$ or decep$ or deceiv$ or offen$ or threat$ or exploit$ or perver$ or gossip$ or bad mouth or bash or insult$ or expos$ or

explicit)) and (AB=(cyber$ or comput$ or internet or web or email or net or webcam)).mp.
14. “12” or “13”

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.

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

3.3 SELECTION OF ARTICLES

Our search strategy uncovered 3029 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. Full-text of studies that appeared to meet the initial criteria were retrieved and further assessed. Articles in conflict at initial screening were passed into full-text review. Most of the remaining studies were excluded due to 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). The two former studies were psychoeducational preventive interventions for children and youth oriented to Internet safety knowledge and online risky behaviour. 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.

3.4 CRITERIA FOR DETERMINATION OF INDEPENDENT FINDINGS

Multiple ESs were calculated within each study. However, the outcomes of I-SAFE focused on knowledge retention whereas the outcomes of the Missing Program focused on the change of behavior and attitudes. The outcomes of each study were not similar enough to combine and the potential dependence problem in most of the meta-analyses with multiple ESs from each study does not pertain. Further, as it was focused on a different outcome – cyber bullying rather than cyber safety knowledge and behaviour – the HAHASO study explored different outcomes than those examined by the I-SAFE or Missing evaluations.

3.5 ASSESSMENT OF METHODOLOGICAL QUALITY

All of the studies included in this review utilized a pre- and post-test design with a control group. Students were not randomly assigned to treatment or control group; rather assignment was based on segmentation through classrooms. Attrition in the Missing program was approximately 1% in both the treatment and 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 three weeks, the follow-up period in the I-SAFE program extended to approximately nine months, and follow-up in the HAHASO program was approximately ninety 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 out of eight schools provided both treatment and control group classes, as compared to the I-SAFE program, in which only two out of eighteen 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.

3.6 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-test and post-test for each outcome and for treatment and control groups separately. The formulas for treatment and control groups are:

$g^{trt} = \frac{(\bar{Y}^{trt} - \bar{X}^{trt})}{S_X^{trt}}$ and $g^{ctrl} = \frac{(\bar{Y}^{ctrl} - \bar{X}^{ctrl})}{S_X^{ctrl}}$, where

g^{trt} : the standard deviation of the change from before intervention (pre-test) to post intervention (post-test).

$\bar{Y}^{trt}$: the post-test mean of the treatment group;

$\bar{X}^{trt}$: the pre-test mean of the treatment group;

S_X^{trt} : the standard deviation of the treatment group on the pre-test; and

g^{ctrl}, $\bar{Y}^{ctrl}$, $\bar{X}^{ctrl}$, and S_X^{ctrl} are parallel statistics for the control group.

A g^{trt} of 0.1 indicates that students in the treatment group averagely improved 0.1 standard deviation from pre-test to post-test on the outcome of interest. In the I-SAFE study, data from five post-tests were collected. The duration between pre-test and the second post-test (Time 3) was similar to the duration between pre- and post-tests in the Missing Project. Therefore, only the data from Time 3 (second post-test) were used to calculate the ESs, in order to allow for comparison. In the Missing Program study, the means and standard deviations for male and females for each outcome were merged before calculating the ES so the results can be compared with the I-SAFE study, in which the results were not separated based on gender. The HAHASO program utilized only one post-test data collection point, at approximately ninety days after the pre-test. Given the different focus of the HAHASO program, findings from this study are not directly compared to those from the I-SAFE and Missing evaluations.

All the *g*s were corrected for small-sample bias (Hedges & Olkin, 1985). The unbiased value for the *i*th ES in the treatment group, denoted as d_i^{trt}, is defined

$d_i^{trt} = \{1 - [\frac{3}{4n_i - 5}]\} g_i^{trt}$,

where n_i is the sample size of the treatment group on the outcome *i*. The same formula was applied to the control group by simply changing the superscript "*trt*" to "*ctrl*" in the formula above.

We also calculated the standard error (SE) of the unbiased ES (d_i^{trt} for the treatment group), which is

$SE(d_i^{trt}) = \sqrt{\frac{2(1-r_i)}{n_i} + \frac{(d_i^{trt})^2}{2n_i}}$.

r_i is the pre-test-post-test correlation for the *i*th sample. Since the correlation is rarely reported unless the study was interested in that specific relationship, a conservative value of .5 was used for calculating all variances for the ESs from

treatment and control groups. Again, the same formula was used to calculate the variance of the unbiased ES for the control group by switching the superscript "*trt*" to "*ctrl*" in the formula above.

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). The z-test is calculated as

$$z = \frac{ES^{trt} - ES^{ctrl}}{S(ES_{pooled})}$$

.

The $S(ES_{pooled})$ is the pooled standard deviation of the effect sizes (aka. The pooled standard error), which is calculated as weighting SEs of treatment and control groups by their degrees of freedom. Specifically,

$$S(ES_{pooled}) = \sqrt{\frac{(N^{trt}-1)*(SE^{trt})^2 - (N^{ctrl}-1)*(SE^{ctrl})^2}{(N^{trt}+N^{ctrl}-2)}}$$

.

A z statistic larger than 1.96 indicates a significant difference on the ESs between two groups.

3.7 HOMOGENEITY TESTS AND MODERATOR ANALYSIS

Due to the conceptual differences between the three studies included in the current synthesis, we did not combine the ES across the three studies. The homogeneity test was therefore not applied (not to say the homogeneity test is meaningless when there are only three studies and the degrees of freedom is 2). The moderator analysis was not necessary since the outcomes from the three studies were not similar enough to conduct a more conventional meta-analysis.

Our analyses mainly focused on the interpretation of the ESs extracted from both studies systematically. We tried to link the findings across studies and come up with a broader conclusion regarding the effectiveness of cyber abuse interventions.

4 Results

4.1 DESCRIPTION OF ELIGIBLE STUDIES

The basic research design for included studies was an intervention and control group design with an outcome measure of interest, such as Internet safety knowledge, risk behavior, or cyber bullying. All studies used the natural segmentation of classes within schools to construct the control group. The intervention was provided by a teacher for both the I-SAFE and Missing program, and by the researcher in the HAHASO program. Baseline measures were collected in all studies.

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 effect sizes were calculated and compared for both studies. Additionally, given that the HAHASO program focused on cyber bullying behaviour, findings cannot be directly compared to those from the I-SAFE or Missing program.

4.2 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, & Rideout, 2002). Excluded studies are detailed in Appendix A.

4.3 TYPES OF CYBER ABUSE INTERVENTIONS

Three of the articles meeting all criteria offered educational prevention interventions oriented towards 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 offline in nature. The intervention was provided to students in grades five to eight. As the goal of I-SAFE is to "provide students with the awareness and knowledge they need to recognize and avoid dangerous, destructive, or unlawful Internet behavior and use the Internet appropriately" (Chibnall et al., 2006), it is clear that the focus of the I-SAFE program extends beyond cyber safety. 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 et al., 2006). The intention of the program is to encourage students to select and transforms information, constructs hypotheses, and makes decisions. Though this theory does not explicitly include Internet safety, the theory was congruent with the program developers' intent to have students develop their own perspectives through thinking about their own online behavior and talking with each other (Chibnall et al., 2006). The curriculum does not require computer-based learning, and is very flexible in its implementation. Outcomes include: 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; managing risk 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 kid their age; sharing personal information such as the student's name and where they hang out with friends; and inappropriate online behaviour such as being on inappropriate websites, looking at inappropriate pictures, and telling a friend their password. The I-SAFE curriculum was taught over a period of one to six weeks, with five lessons taught lasting approximately 40 minutes 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 & Trineer, 2003). The game highlights 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 highlight to children that they should not always trust what they are told by individuals they meet online (Crombie & Trineer, 2003). Therefore, the program targets (1) open chat rooms conversations, (2) 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 six and seven. The theoretical approach of the Missing program is not detailed. Outcomes included: the frequency of personal information disclosure in open chat rooms, personal email 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 minutes.

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 five and six. The specific theoretical approach underpinning the "Help, Assert Yourself, Humor, Avoid, Self-talk, Own it" curriculum is not detailed. Outcomes included: the prevalence of bullying incidents and behaviours at school, on the Internet, and on cellular phones; reactions to bullying; and knowledge of social skills (Salvatore, 2006).

4.4 IMPACTS ON INTERNET SAFETY KNOWLEDGE, RISK BEHAVIOR, AND CYBER BULLYING OUTCOMES (EFFECT SIZES)

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

I-SAFE (US)	Treatment (N=796-1199)		Control (N=528-738)	
	ES	SE	ES	SE
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

TABLE 1 (Cont'): 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

Missing Program (Canada)	Treatment (N=57-181)		Control (N=55-157)	
I. Open Chat Room Behaviours and E-mailing Strangers	ES	SE	ES	SE
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

TABLE 1 (Cont'): 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

Missing Program (Canada) cont'	Treatment (N=57-181)		Control (N=55-157)	
II. Reported Likelihood of Posting Specific Personal Information on a Personal Web Page	ES	SE	ES	SE
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

TABLE 1 (Cont'): 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

Missing Program (Canada) cont'	Treatment (N=57-181)		Control (N=55-157)	
III. 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 email 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

TABLE 1 (Cont'): 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

HAHASO strategy	Treatment (N=6)		Control (N=6)	
	ES	SE	ES	SE
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

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 pre-tests to the post- tests. A Forest plot for each project (I-SAFE, Missing Program, and Hahaso Program) on each group (treatment and control) was provided in the appendix.

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 pre-test to the post-test. Cohan (1988) suggested an ES of .2 is small, an ES of .50 is medium, and an ES of .8 is large. Another practical guideline for synthesis is based on empirical examination provided by Lipsey (1990), who found an effect size of 0.15 to be small, 0.45 to be moderate, and 0.90 to be large. According to the rule of thumb, the students' knowledge vastly improved. The control group consistently showed smaller ESs on the outcomes reported in this project. The negative ESs found in the control group indicated the decrease from the pre-tests to the post-tests. For example, the ES of -0.15 on "predator identification" indicates that students' knowledge on possible actions of predators decreased 0.15 standard deviation from the pre-test to the post-test in the control group.

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 info from the pre-tests to the post-tests. Some negative values were found in the control group indicate a worsening of behavior from the pre-tests to the post-tests. For example, the largest ES of on "Disclosing one's gender" in the control group (dctrl = -0.44) indicates that students increased dangerous behavior (disclosing gender) 0.44 standard deviation in the chat rooms from the pre-test to the post-test. 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 post-test. Above medium effects were found both in treatment and control groups on "how likely is it that someone online would try to manipulate you" (d^{trt} = 0.24; d^{ctrl} = 0.24) and "how likely is it that someone online would try to lure you away from home" (d^{trt} = 0.37; d^{ctrl} = 0.23). Similar results were also found in other outcomes, such as, "how much can one trust people online" (d^{trt} = 0.00; d^{ctrl} =

0.03), "how long do you have to know people that you met online before trusting them a lot" (d^{trt} = 0.19; d^{ctrl} = 0.20), "how likely is it that someone online would try to lure someone your age away from home" (d^{trt} = 0.06; d^{ctrl} = 0.04), "how risky is it to disclose personal information in an open chat room" (d^{trt} = 0.16; d^{ctrl} = 0.16). In several outcomes, the control group seemed to have safer attitudes than those in the treatment group in the post-test (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 pre-test to the post-test. The largest ES happened in the control group in "cyberbullying survey" (d^{ctrl} = 0.88), which indicates a decrease of bullying from the pre-test to the posttest. At the same time, cyber bullying also decreased in the treatment group (d^{trt} = 0.37).

The differences between treatment and control groups on the ESs of each outcome will be tested statistically in the next section.

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.

I-SAFE (US)	ES^{trt}-ES^{ctrl}	Z-test
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)	ES^{trt}-ES^{ctrl}	Z-test
I. Open Chat Room Behaviours 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
II. 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
III. 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 email 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	ES^{trt}-ES^{ctrl}	Z-test
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

*$p<.05$

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*). However, the differences between treatment and control groups 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 non-significant at the .05 level. In other words, the ESs differences between treatment and control groups we observed on most of the outcomes could have happened simply by chance. Specifically, the program did not significantly change most of 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 indicate that control groups had more changes between the pre- and post- tests 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. Forest plots are provided in Appendix C to facilitate an interpretation of the results given these limitations.

5 Discussion

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. However, it is important to note that many of the changes reported in the treatment group regarding Internet behaviour were in the desired direction, though 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 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 knowledge regarding the identification of Internet predators and knowledge about 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. However, despite these increases in knowledge, students who received the intervention were not significantly less likely to engage in inappropriate online behavior such as browsing inappropriate sites, giving out their email 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 to disclose their gender, age, and name of their city in communication with strangers, there was no change in the likelihood of disclosing one's name, description of appearance, personal email address, or school name. Additionally, students who received the intervention were not significantly less likely to participate in open chat rooms and email 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 five to eight). 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 needs to be placed on actually decreasing risky online behaviors.

6 Reviewers' Conclusions

6.1 IMPLICATIONS FOR PRACTICE

Cyber abuse remains a new and relatively unexplored phenomenon. The pervasiveness of online risks underlines the importance of focusing preventive and intervention programs/strategies for all children and youth, as there are inevitable concerns of online activity even for those children and youth who are not typically considered to be vulnerable. Further, there is a great need to develop and evaluate interventions with those children and youth who are more vulnerable and experience greater risk as this review did not find any such existing evaluations. . Although little clinical knowledge appears to exist in this area, the growing nature of this phenomenon demands greater attention.

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 the 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.

6.2 IMPLICATIONS FOR RESEARCH

Despite the attention provided to cyber abuse by 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 five to eight. Additionally, research that explores the use of technological interventions with children and youth is also 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 to examine opportunities to reduce cyber bullying among children and adolescents.

7 Plans for Updating the Review

The review will be updated every two years.

8 Acknowledgements

This review was supported by Bell Canada and co-sponsored by SFI Campbell, The Danish National Centre for Social Research and The Campbell Collaboration.

9 References

Aloysius, 2001
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*, Berghahn Books and UNESCO, Paris, pp.157–62.

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

Atlas & Pepler, 1998
Atlas, R. & Pepler, D. (1998). Observations of bullying in the classroom. *Journal of Educational Research, 92*(2), 86-99.

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

Belsey, 2008
Belsey B. (2008). Available at: http://www.cyberbullying.ca Accessed July 16, 2008.

Beran & Li, 2005
Beran, T. & Li, Q. (2005). Cyber-harassment: A study of a new method for an old behavior. *Journal of Educational Computing Research, 32*(3), 265-277.

Berson & Berson, 2002
Berson, I. & Berson, M. (2002). Evolving a Community Initiative to Protect Children in
Cyberspace Final Report. University of South Florida. Retrieved December 8, 2008 from: http://www.fmhi.usf.edu/institute/pubs/pdf/cfs/cybersafetyfinalreport.pdf

Berson, Berson & Ferron, 2002

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: AMiddle School Technologies Journal, 5*(2), 1-32.

Brookshire & Maulhardt, 2005
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

Cairns & Cairns, 1991
Cairns, R.B., & Cairns, B.D. (1991). Social cognition and social networks: A developmental perspective. In D. Pepler & K. Rubin (Eds.), *The development and treatment of childhood aggression* (pp. 249-278). Hillsdale, NJ: Lawrence Erlbaum Associates.

Chibnall, Wallace, Leicht & Lunghofer, 2006
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, 1988
Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences, 2nd ed. Hillsdale, NJ: Erlbaum.

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

Crick & Bigbee, 1998
Crick, N.R., & Bigbee, M.A. (1998). Relational and Overt Forms of Peer Victimization: A Multiinformant Approach. *Journal of Consulting and Clinical Psychology, 66*(2), 337-347.

Crombie & Trinneer, 2003
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.

Curry & Haycock, 2001
Curry, A., & Haycock, K. (2001) Filtered or unfiltered? *School Library Journal, 47*(2), 45-47.

Davidson & Martellozzo, 2005

Davidson. J., & Martellozzo, E. (2005). *Educating Children about Sexual Abuse and Evaluating the Metropolitan Police Safer Surfing Programme.* London, UK: Metropolitan Police.

Durkin & Low, 1998
Durkin, K. & Low, J. (1998) Children, media and aggression: Current research in Australia and New Zealand, in U. Carlsson and C. von Feilitzen (eds), *Children and media violence*, The UNESCO International Clearinghouse on Children and Violence on the Screen, Göteborg, pp.107–24.

Finkelhor, Mitchell & Wolak, 2000
Finkelhor, D., Mitchell, K., & 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 & Kerman, 2004
Finn, J., & Kerman, B. (2004). Internet risks for foster families online. *Journal of Technology in Human Services, 22*(4), 21-38.

Germain & Bloom, 1999
Germain, C.B., & Bloom, M. (1999). *Human behavior in the social environment: An ecological view* (Second Edition). New York: Columbia University Press.

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

Greenfield, Rickwood & Tran, 2001
Greenfield, P., Rickwood, P. & Tran, H. (2001). Effectiveness of Internet filtering software products. Retrieved December 8, 2008 from: http://www.acma.gov.au/webwr/aba/newspubs/documents/filtereffectiveness.pdf

Hanish & Guerra, 2000
Hanish, L.D., & Guerra, N.G. (2000). Children who get victimized at school: What is known? What can be done? *Professional School Counseling, 4*(2), 113-119.

Hedges & Olkin, 1985
Hedges, L. V., & Olkin, I. (1985). Statistical methods for meta-analysis. Orlando, FL: Academic Press.

Hinduja, & Patchin, 2008
Hinduja, S. & Patchin, J. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior*, 29(2), 129-156.

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

Hunter, 2000
Hunter, C.D. (2000). Internet filter effectiveness - testing over- and underinclusive blocking decisions of four popular web filters. *Social Science Computer Review, 18*(2), 214-22.

Internet Safety Technical Task Force (2008).
Internet Safety Technical Task Force (2008). Enhancing child safety and online technologies. Final report of the Internet safety technical task force. Retrieved July 7, 2009 from: http://cyber.law.harvard.edu/pubrelease/isttf/

Kaynay & Yelsma, 2000
Kaynay, J.M., & Yelsma, P. (2000). Displacement effects of online media in the socio-technical contexts of households. *Journal of Broadcasting and Electronic Media, 4*(2), 215-229.

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

Livingston & Bober, 2005
Livingstone, S., & Bober, M. (2005). UK children go online: final report of key project findings. Retrieved December 8, 2008 from: http://www.lse.ac.uk/collections/children-go-online/

Lipsey, 1990
Lipsey, M. W. (1990). *Design Sensitivity: Statistical Power for Experimental Research*. Thousand Oaks, CA: Sage Publications.

Magid, 1998
Magid, L.J. (1998). Child safety in the information highway. National Center for Missing and Exploited Children. Retrieved December 8, 2008 from: http://www.safekids.com/child_safety.htm

Mishna, Pepler & Wiener, 2006
Mishna, F., Pepler, D., & Wiener, J. (2006). Factors associated with perceptions and responses to bullying situations by children, parents, teachers and principals. *Victims and Offenders, 1*(3), 255-288.

Mitchell, Finkelhor & Wolak, 2001

Mitchell, K.J., Finkelhor D., & Wolak J. (2001) Risk factors for and impact of online sexual
solicitation of youth. *JAMA, 285*(23), 3011-3014.

Mitchell, Finkelhor & Wolak, 2003
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*(3), 330-358.

Nansel, Overpeck, Pilla, Ruan, Simons-Morton & Scheidt, 2001
Nansel, T.R., Overpeck, M., Pilla, R.S., Ruan, W.J., Simons-Morton, B., & Scheidt, P. (2001).
Bullying behaviors among US youth: Prevalence and association with psychosocial adjustment. *Journal of the American Medical Association, 285*, 2094–2100.

National Centre for Missing & Exploited Children, 2002
National Center for Missing & Exploited Children (2002). Education & resources: Statistics and commonly asked questions [On-line]. National Center for Missing & Exploited Children. Retrieved December 8, 2008 from: http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=2810

Nie & Hillygus, 2002
Nie, N. H., & Hillygus, D. S. (2002). Where Does Internet Time Come From?: A Reconnaissance. *IT & Society, 1*(2), 1-20.

O'Connell, Price & Barrow, 2004
O' Connell, R., Price, J, & Barrow, C. (2004). Cyber Stalking, Abusive Cyber Sex and Online Grooming: A Programme of Education For Teenagers. Lanchasire, UK: Cyberspace Research Unit, University of Central Lanchasire.

O'Connell, Pepler & Craig, 1999
O'Connell, P., Pepler, D., & Craig, W. (1999). Peer involvement in bullying: Insights and challenges for intervention. *Journal of Adolescence, 22*, 437-452.
Olweus, 1994
Olweus, D. (1994). Annotation: Bullying at school: Basic facts and effects of a school based intervention program. J*ournal of Child Psychology and Psychiatry and Allied Disciplines, 35*(7), 1171-1190.

Olweus, 1997
Olweus, D. (1997). Bully/victim problems in school: Facts and intervention. *European Journal of Psychology of Education. Special Issue: Children with special needs, 12*(4), 495-510.

Patchin & Hinduja, 2006
Patchin, J. & Hinduja, S. (2006). Bullies move beyond the school yard: A preliminary look at
cyberbullying. *Youth Violence and Juvenile Justice,* 4(2), 148-169.

Richardson, Resnick, Hansen & Rideout, 2002
Richardson, C., Resnick, P., Hansen, D. & Rideout, V. (2002). Does pornography blocking software block access to health information on the Internet? *Journal of the American Medical Association,* 288(22), 2887-2894.

Sellier, 2001
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.173–75). Paris: Berghahn Books and UNESCO.

Scheider, 1997
Schneider, K. (1997). A Practical Guide to Internet Filters. *Neal Schuman Publishing*. Clifton Park, New York.

Shariff & Johnny, 2007
Shariff, S. & Johnny, L. (2007). Cyber-libel and cyber bullying: Can schools protect student reputations
and free expression in virtual environments? *McGill Journal of Education*, 16, 307-342.

United Nations, 1989
United Nations General Assembly. (1989). Convention on the Rights of the Child. Document A/RES/44/25(12 December) 1989.

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

Wishart, Andrews & Yee, 2005
Wishart, J., 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, Oades & Morris, 2007
Wishart, J., Oades, C. & Morris, M. (2007). Using online role play to teach Internet safety awareness. *Computers and Education,* 48, 460-473.

Wolak, Finkelhor, Mitchell & Ybarra, 2008

Wolak, J., Finkelhor, D., Mitchell, K & Ybarra, M. (2008). Online predators and their victims: Myths, realities, and implications for prevention and treatment. *American Psychologist,* 63(2), 111-128.

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

Ybarra, 2004
Ybarra M.L. (2004). Linkages between depressive symptomatology and Internet harassment among young regular Internet users. *Cyberpsychology & Behavior, 7*(2), 247-257.

Ybarra, Lead & Diener-West, 2004
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*(1), e5.

Ybarra & Mitchell, 2004a
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 & Mitchell, 2004b
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*(7), 1308-1316.

Ybarra, Mitchell, Wolak & Finkelhor, 2006
Ybarra, M., Mitchell, K., Wolak, J. & Finkelhor, D. (2006). Examining characteristics and associated distress related to internet harassment: Findings from the second youth internet safety survey. *Pediatrics,* 118 (4), 1169-1177.

10 Appendix A: Excluded Articles

Relevant Articles Not Meeting All Inclusion Criteria					
Author, Publication Date	Location	Reasons for Not Including	Intervention	Population and Sample Size	Results
Brookshire, M. & Maulhardt, C. (2005).	Maine, United States	No control group.	NetSmartz – Internet Safety Educational Program	Students aged 9-14 (n= 122)	Increases in Internet safety knowledge.
Davidson. J. & Martellozzo, E. (2004).	London, UK	Data is qualitative in nature, collected by focus groups with students.	Safer Surfing – Internet Safety Program	Students aged 10-13 (n=200)	Students who participated in the program expressed more knowledge regarding Internet safety.

Finn, J. & Kerman, B. (2004).	Connecticut, Massachusetts, Rhode Island, United States	No relevant outcomes for intervention type (parent education), no baseline data collected for control group, temporal measurement issues.	One-hour educational program on Internet safety provided to foster parents, and use of Net-Nanny software.	Foster parents (n=74) and foster children (n=63)	Overall, few Internet related safety issues were reported in sample (research project was not specifically oriented to Internet safety). No outcomes were reported related to changes in knowledge of technology or Internet monitoring among foster parents. Among the small number that reported Internet difficulties, fewer incidences of exposure to violence or pornography reported by treatment group. However, measurement of exposure includes time periods prior to study implementation (and therefore prior to Net-Nanny utilization).
Gray, S. (2005).	British Columbia, Canada	No control group.	Internet safety unit delivered in school.	Grades 4-7 students (n=188)	Increases in Internet safety knowledge.
Greenfield, P., Rickwood, P. & Tran, H. (2001).	Australia	Not implemented with children/youth or their parents. No control group.	n/a – an evaluation of Internet filtering programs	Fourteen Internet filtering programs evaluated	Varying results across multiple usability, performance and effectiveness criteria.
Hunter, C. (2000).	Pennsylvania, United States	Not implemented with children/youth or their parents. No control group.	n/a – an evaluation of Internet filtering programs	Four Internet filtering programs evaluated	Filters blocked some benign content and were not entirely successful in blocking objectionable material.

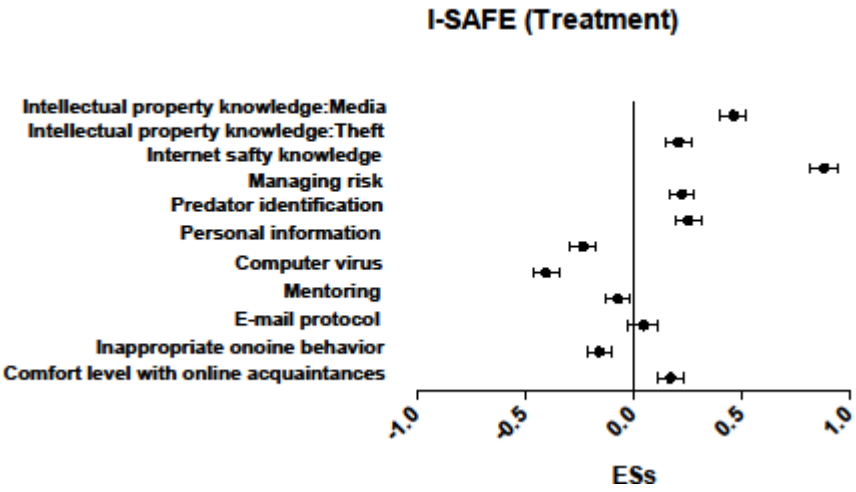
KidSmart. (2002).	United Kingdom	Cross-sectional review of pilot study. No control group.	Childnet's KidSmart Internet safety program	Parents and teachers, unknown sample size	Internet safety education needs to be provided to teachers, students and parents. Students are particularly responsive to drama-based learning.
Richardson, C., Resnick, P., Hansen, D. & Rideout, V. (2002).	Michigan, United States	Not implemented with children/youth or their parents. No control group.	n/a – an evaluation of Internet filtering programs	Six filtering programs were evaluated	Filters blocked some benign health-related content and were not entirely successful in blocking pornography.
Wishart, J., Andrews, J. & Yee, W.C. (2005).	United Kingdom	Cross-sectional review of program. No control group.	Getting to Know IT all – e-safety campaign	Students in years 7-9 (n=657)	Students indentified increases in e-safety knowledge as an important element of the presentation.
Wishart, J. M., Oades, C. E., & Morris, M. (2007).	United Kingdom	No control group.	Net Detectives, an online Internet safety role play.	Students in years 4-7, in role play observation (n=98) and follow up questionnaires (n=192)	Students reported increases in Internet safety.

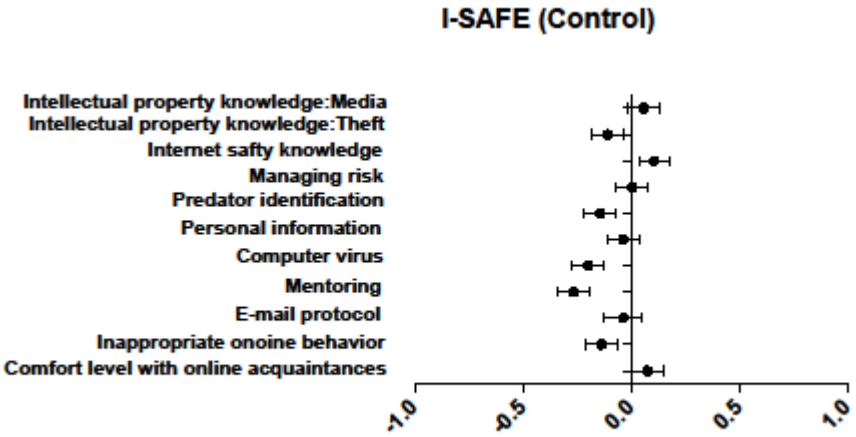
11 Appendix B: Included Articles

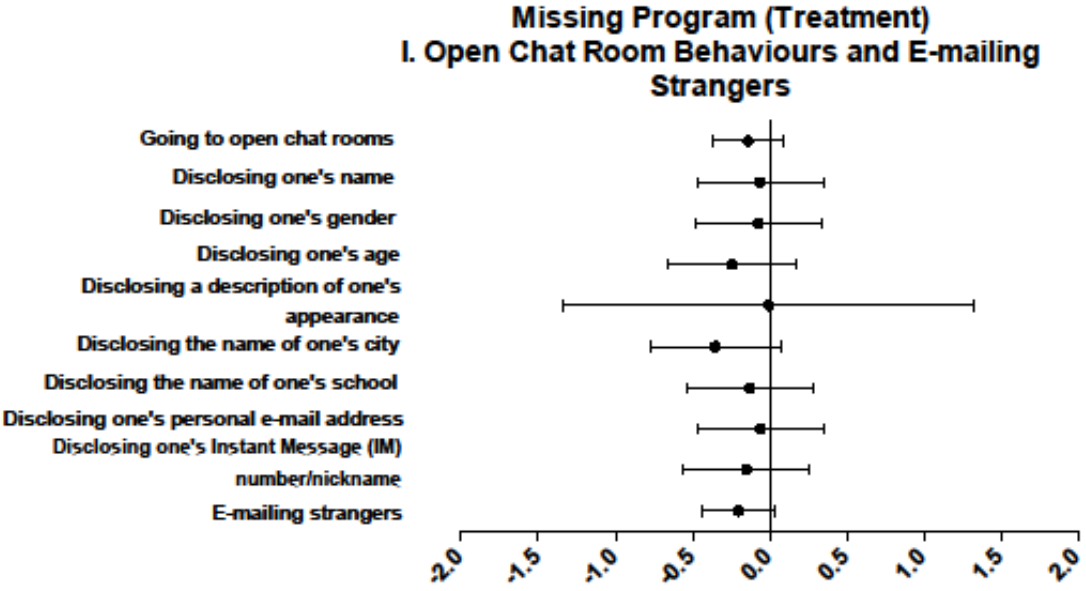
Articles Meeting All Inclusion Criteria					
Author	Location	Type of Intervention	Time of Study	Sample Size	Population
Chibnall, S. et al. (2006).	Kentucky, Oklahoma and Nebraska, United States	In school administration of the i-safe curriculum	2004-2005	Treatment group = 1328 Control group = 771	Grade 5-8 students
Crombie, G. & Trineer, A. (2003)	British Columbia, Canada	In school administration of the Missing Internet Safety computer program	2002	Treatment group = 181 Control group = 157	Grade 6 and 7 students
Salvatore, A. (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

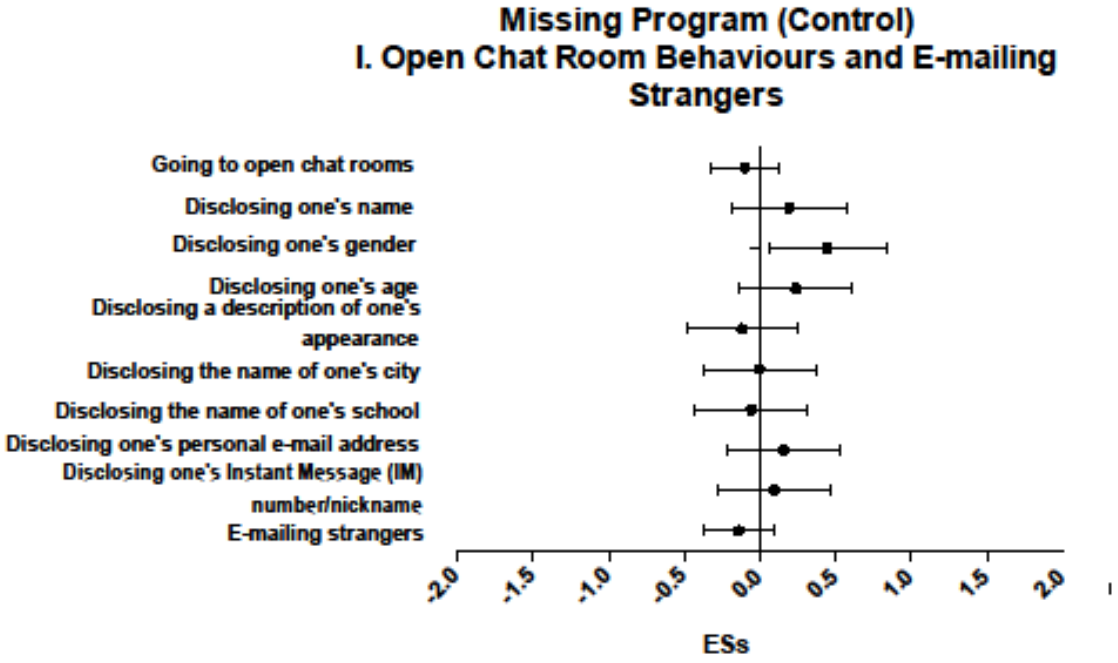
12 Appendix C: Forest Plots

I-SAFE project

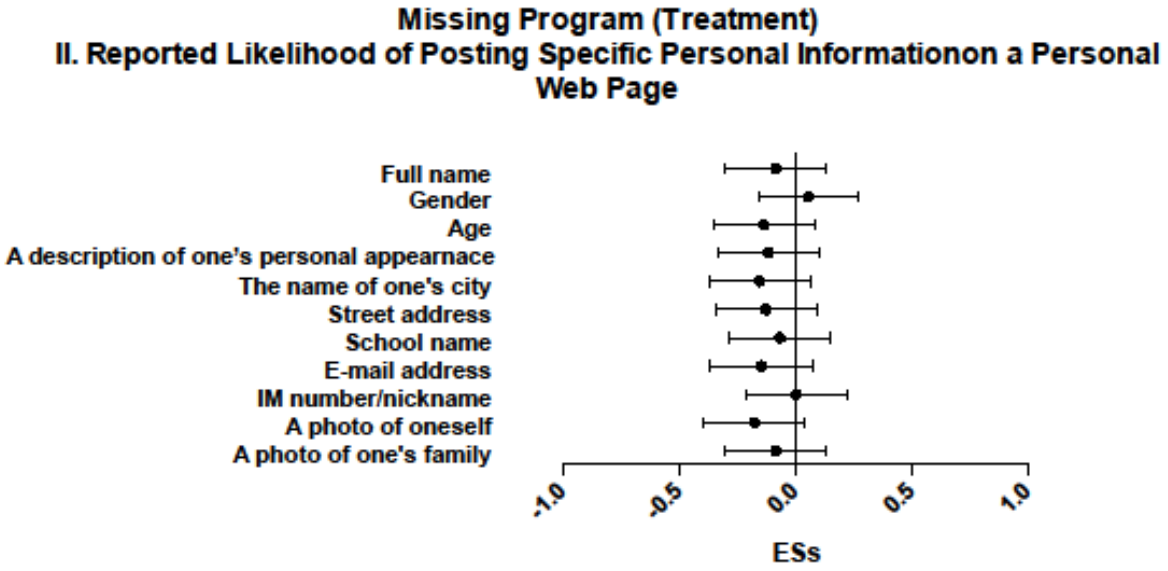


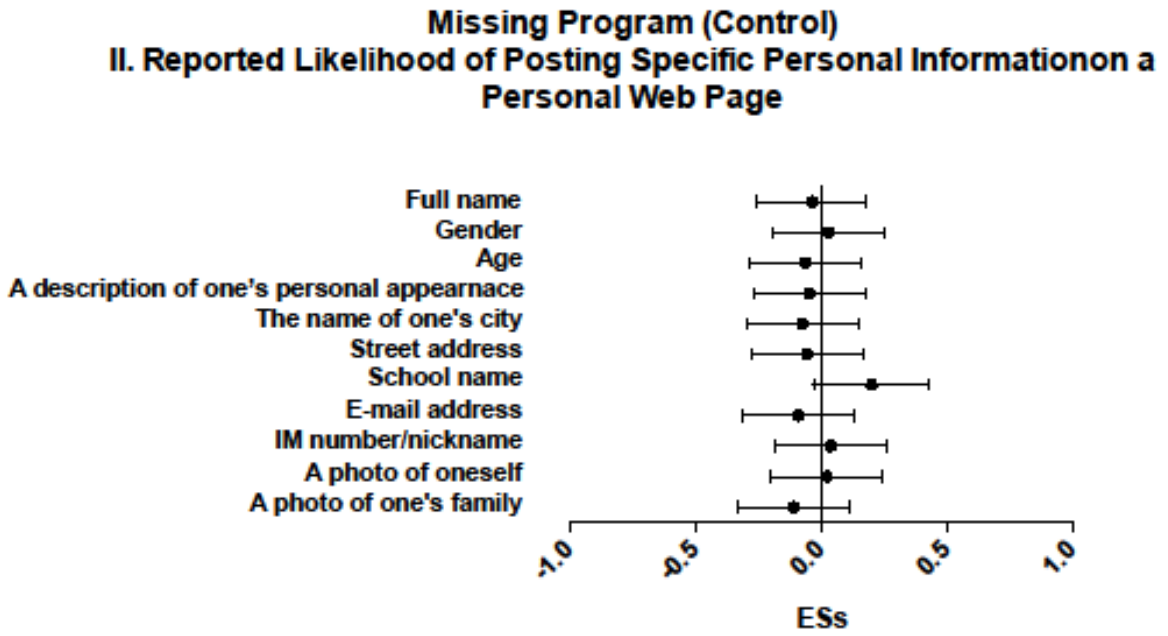


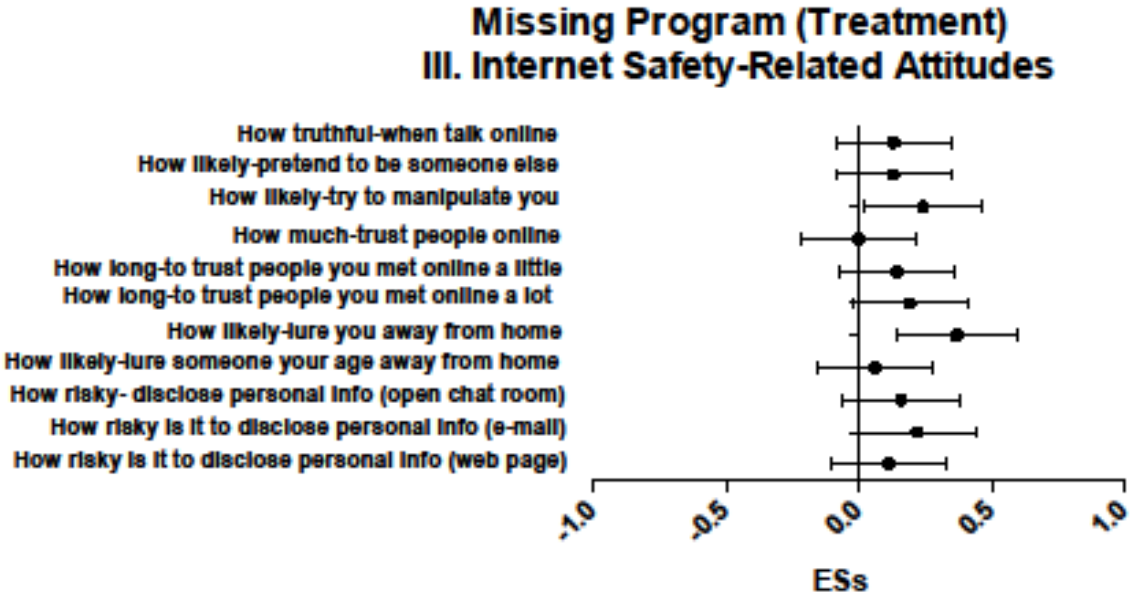

Missing Program (Treatment)
I. Open Chat Room Behaviours and E-mailing Strangers
Going to open chat rooms
Disclosing one's name
Disclosing one's gender
Disclosing one's age
Disclosing a description of one's appearance
Disclosing the name of one's city
Disclosing the name of one's school
Disclosing one's personal e-mail address
Disclosing one's Instant Message (IM) number/nickname
E-mailing strangers
-2.0
-1.5
-1.0
-0.5
0.0
0.5
1.0
1.5
2.0

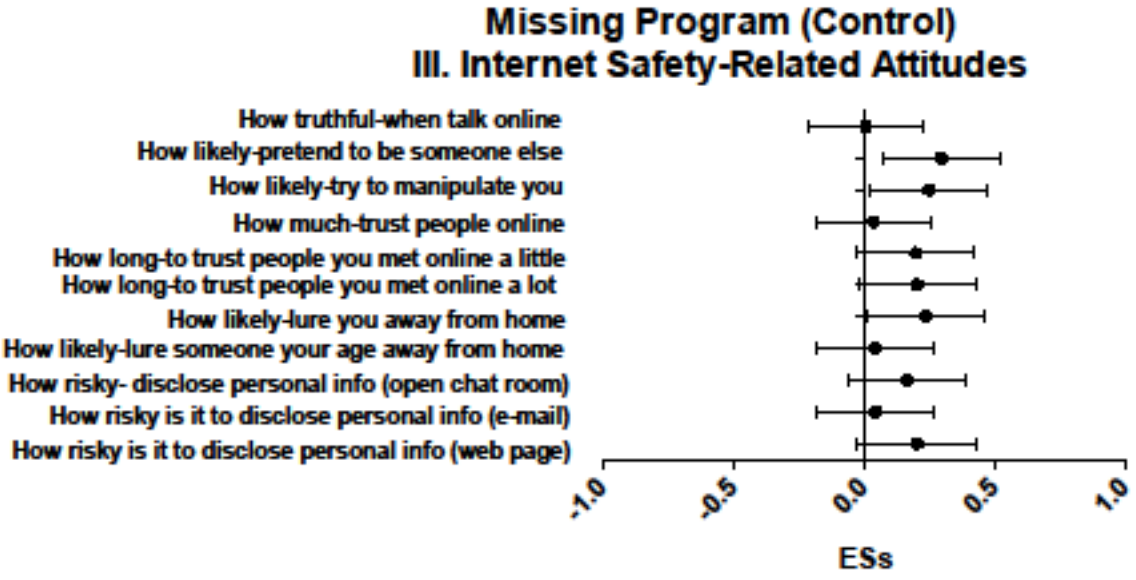

Missing Program (Control)
I. Open Chat Room Behaviours and E-mailing Strangers
Going to open chat rooms
Disclosing one's name
Disclosing one's gender
Disclosing one's age
Disclosing a description of one's appearance
Disclosing the name of one's city
Disclosing the name of one's school
Disclosing one's personal e-mail address
Disclosing one's Instant Message (IM) number/nickname
E-mailing strangers
-2.0
-1.5
-1.0
-0.5
0.0
0.5
1.0
1.5
2.0
ESs

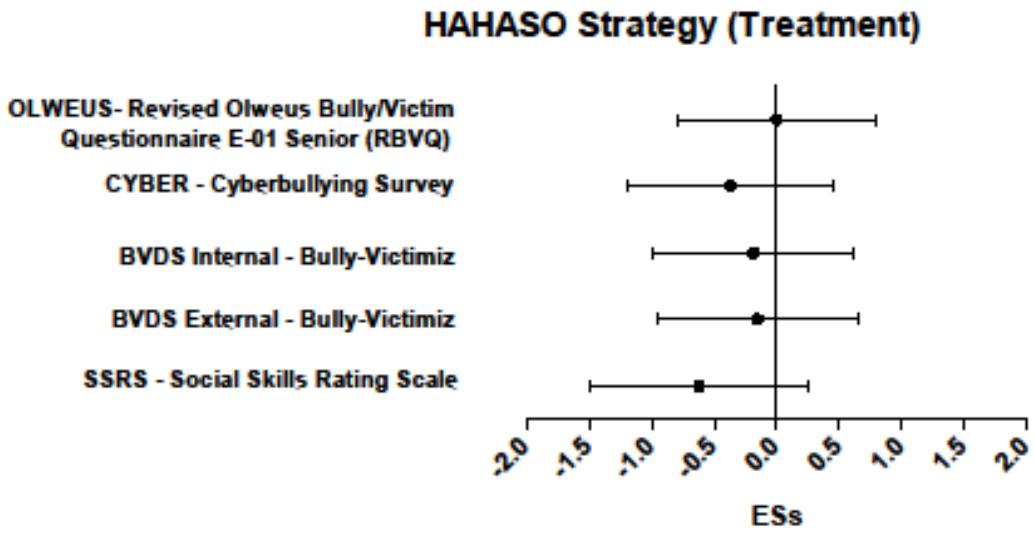
Missing Program: II. Reported Likelihood of Posting Specific Personal Information on a Personal Web Page

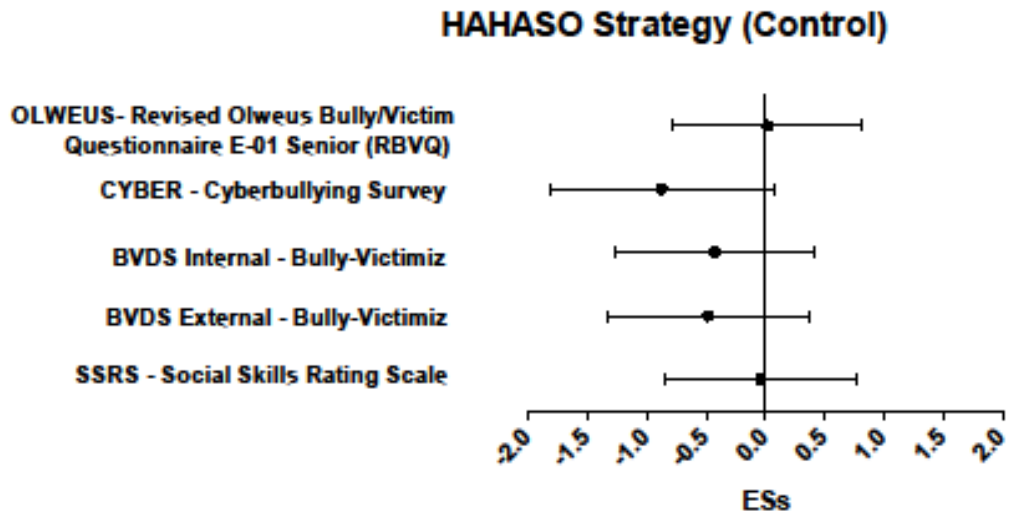





Missing Program (Treatment)
III. Internet Safety-Related Attitudes
How truthful-when talk online
How likely-pretend to be someone else
How likely-try to manipulate you
How much-trust people online
How long-to trust people you met online a little
How long-to trust people you met online a lot
How likely-lure you away from home
How likely-lure someone your age away from home
How risky- disclose personal info (open chat room)
How risky is it to disclose personal info (e-mail)
How risky is it to disclose personal info (web page)
-1.0
-0.5
0.0
0.5
1.0
ESs


Missing Program (Control)
III. Internet Safety-Related Attitudes
How truthful-when talk online
How likely-pretend to be someone else
How likely-try to manipulate you
How much-trust people online
How long-to trust people you met online a little
How long-to trust people you met online a lot
How likely-lure you away from home
How likely-lure someone your age away from home
How risky- disclose personal info (open chat room)
How risky is it to disclose personal info (e-mail)
How risky is it to disclose personal info (web page)
-1.0
-0.5
0.0
0.5
1.0
ESs


HAHASO Strategy (Treatment)
OLWEUS- Revised Olweus Bully/Victim Questionnaire E-01 Senior (RBVQ)
CYBER - Cyberbullying Survey
BVDS Internal - Bully-Victimiz
BVDS External - Bully-Victimiz
SSRS - Social Skills Rating Scale
-2.0
-1.5
-1.0
-0.5
0.0
0.5
1.0
1.5
2.0
ESs


HAHASO Strategy (Control)
OLWEUS- Revised Olweus Bully/Victim Questionnaire E-01 Senior (RBVQ)
CYBER - Cyberbullying Survey
BVDS Internal - Bully-Victimiz
BVDS External - Bully-Victimiz
SSRS - Social Skills Rating Scale
-2.0
-1.5
-1.0
-0.5
0.0
0.5
1.0
1.5
2.0
ESs