Youth Internet Safety Education: Aligning Programs With the Evidence Base

David Finkelhor1, Kerryann Walsh2, Lisa Jones1, Kimberly Mitchell1, and Anne Collier3

Abstract

Background: This review critically examines the messages of youth internet safety education programs in the light of research about both the dynamics of internet dangers and the efficacy of youth prevention education. Methods: Using terms “internet safety education” and “digital citizenship,” a Google search identified 12 multi-topic safety programs. Review articles were identified via Google Scholar for six forms of online harm to youth that have been targeted by many of these programs: cyberbullying (19 articles); online sexual exploitation (23 articles); sexting (19 articles); online fraud, hacking, and identity theft (6 articles); online suicide and self-harm promotion (18 articles); and internet overuse or addiction (15 articles). Findings: There appear to be mismatches between dynamics revealed in the research about internet harms and the messages emphasized in educational programs, particularly on the issues of sexual exploitation and sexting. Overall, the review literature also suggests major advantages to integrating internet safety into already well-established and evidence-based programs currently addressing related off-line harms, for example, programs focusing on general bullying, dating abuse, or sexual abuse prevention. The advantages stem from four factors: (1) the considerable overlap between online harms and similar off-line harms, (2) the apparent greater prevalence of off-line harms, (3) the evidence that the same risk factors lie behind both online and off-line harms, and most importantly, (4) the substantially superior evidence base for the longer standing programs developed originally around the off-line harms.

Keywords
cybersafety, online safety, digital citizenship, technology education

There have been an increasing number of educational programs developed and marketed to help young people navigate new digital technologies. These have been developed by a variety of organizations including technology companies such as Google (2019), child protection agencies (National Center for Missing & Exploited Children, 2019), along with independent not-for-profits focusing on media and technology (Common Sense Media, 2017, 2019; PBS Kids, 2019). Characterizing these programs is difficult, owing to heterogeneity in the topics covered, with some, but not all, labeled under the umbrella concept of digital citizenship, which refers broadly to education initiatives aiming to teach responsible and safe use of digital technologies (Jones & Mitchell, 2015; Moreno et al., 2013).

From a research vantage point, two challenges face these education-focused prevention efforts. First, there is a limited research base about the dynamics of some of the online dangers, so that program developers are not always clear about how the harms arise, for whom, under what circumstances, and for what reasons. Second, there is an extremely limited literature on what kinds of program messages and skills have the potential to protect children and youth from specific harms. Although dissemination of programs has intensified, few have been evaluated using rigorous empirical methods.

This review explores two issues. What does current research show about the dynamics of the technology harms (e.g., online sexual exploitation), and what are the implications for the design of prevention education? What does the broader evaluation literature on prevention in related areas suggest to maximize successful messaging and skill building for these programs? The review grows out of the findings of independently conducted but related research projects that were commissioned by the World Health Organization and

1 Crimes Against Children Research Center, University of New Hampshire, Durham, NH, USA
2 Faculty of Education, Queensland University of Technology, Brisbane, Queensland, Australia
3 The Net Safety Collaborative, Salt Lake City, UT, USA

Corresponding Author:
David Finkelhor, Crimes Against Children Research Center, University of New Hampshire, 125 McConnell Hall, 15 Academic Way, Durham, NH 03824, USA.
Email: david.finkelhor@unh.edu
the Australian Office of the eSafety Commissioner (Walsh et al., 2019).

Using terms “internet safety education” and “digital citizenship,” a Google search identified 12 multi-topic safety programs (Table 1). Review articles were identified via Google Scholar for six forms of online harm to youth that have been targeted by many of these programs: cyberbullying (19 articles); online sexual exploitation (23 articles); sexting (19 articles); online fraud, hacking, and identity theft (6 articles); online suicide and self-harm promotion (18 articles); and internet overuse or addiction (15 articles). These will be the prime topics for this review.

## Table 1. Internet Safety and Digital Citizenship Programs With Selected Content Areas.

<table>
<thead>
<tr>
<th>Program</th>
<th>Cyberbullying</th>
<th>Sex Solicitation</th>
<th>Sexting</th>
<th>Fraud/ Hacking</th>
<th>Self-Harm/ Suicide</th>
<th>Overuse/ Addiction</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Be Internet Awesome</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="https://beinternetawesome.withgoogle.com/en_us">https://beinternetawesome.withgoogle.com/en_us</a></td>
</tr>
<tr>
<td>Cyberscivics</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td><a href="https://www.cyberscivics.com/">https://www.cyberscivics.com/</a></td>
</tr>
<tr>
<td>Cybersmart</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td><a href="http://cybersmart.org/workshops/">http://cybersmart.org/workshops/</a></td>
</tr>
<tr>
<td>Digital Citizenship Common Sense Media</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td><a href="https://www.commonsense.org/education/digital-citizenship/curriculum">https://www.commonsense.org/education/digital-citizenship/curriculum</a></td>
</tr>
<tr>
<td>eSafety Australia</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td><a href="https://www.esafety.gov.au/educators/classroom-resources">https://www.esafety.gov.au/educators/classroom-resources</a></td>
</tr>
<tr>
<td>FBI Safe Internet Surfing</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td><a href="https://sos.fbi.gov/en/">https://sos.fbi.gov/en/</a></td>
</tr>
<tr>
<td>iSafe</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td><a href="https://www.isafe.org/">https://www.isafe.org/</a></td>
</tr>
<tr>
<td>NetSmartz</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td><a href="https://www.missingkids.org/netsmartz/home">https://www.missingkids.org/netsmartz/home</a></td>
</tr>
<tr>
<td>ThinkUKnow</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
<td><a href="https://www.thinkuknow.co.uk/">https://www.thinkuknow.co.uk/</a></td>
</tr>
<tr>
<td>Webwise kids</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.webwisekids.org/">http://www.webwisekids.org/</a></td>
</tr>
<tr>
<td>Wired Safety</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td><a href="https://www.wiredsafety.com/">https://www.wiredsafety.com/</a></td>
</tr>
</tbody>
</table>

## Cyberbullying

### Problem

Cyberbullying is a problem with wide recognition and a considerable research base. The term cyberbullying references verbal aggression, hostility, and other attempts to cause harm in online communications and encompasses terms such as flaming, outing, hate speech, online drama, and online harassment (see also Calvete et al., 2010; Pyżalski, 2012). It can include the posting of false profiles, distributing defamatory information, and cyberstalking (Rivers & Noret, 2010). Besides physical threats and threats to home, family, and friendships, it is widely recognized that much of cyberbullying, like face-to-face bullying, has sexual components, including sexual harassment, and homophobic and sexist derogation (Ehman & Gross, 2018). Hate and bias speech is also common (Henry, 2013). Online bullying, harassment, aggression, and stalking also occur in the context of adolescent dating relationships, among school peers, and in relationships started online (Rivers & Noret, 2010; Stonard et al., 2014).

However, cyberbullying is not well defined in the literature or colloquially since criteria such as repetition and power imbalance that are applied in conventional bullying assessment are not typically applied in regard to cyberbullying (Englander et al., 2017; Livingstone & Smith, 2014).

### Scope

Rates of cyberbullying vary widely. A meta-analysis of 72 studies found 15% of youth report cyberbullying victimization compared to 36% who report face-to-face bullying (Modecki et al., 2014). Cyberbullying occurs to both boys and girls to about equal degree, but there are differences by gender with respect to specific cyberbullying behaviors (Sorrentino et al., 2019). Cyberbullying peaks at ages 13–15, somewhat older than conventional bullying (Mitchell, Jones, Turner, Shattuck, & Wolak, 2016; Sorrentino et al., 2019; Tokunaga, 2010).

### Co-occurrence

A key well-substantiated finding is that much cyberbullying occurs in conjunction with off-line bullying and harassment (Sabella et al., 2013; Waasdorp & Bradshaw, 2015). One study found that two thirds of online harassment episodes were connected with off-line episodes (Mitchell, Jones, Turner, Blachman-Demner, & Kracke, 2016).

### Prevention Strategies

There are many educational programs that address cyberbullying to some extent. A recent review found 64 articles reporting...
on programs around the world (Gaffney, Farrington, et al., 2018). Some of the key messages and skills that are taught in programs include the following: establishing norms about what is mean or hurtful, teaching empathy or taking the perspective of another person, skills for de-escalation, skills for disengagement (such as logging off, or not forwarding messages), bystander support and mobilization, reporting, and help-seeking.

Educational programs do appear to be effective at reducing cyberbullying. A meta-analysis found educational programs reduced cyberbullying perpetration by 10%–15% and victimization by 15% (Gaffney, Farrington, et al., 2018). An important qualification is that most of the evaluated cyberbullying interventions in this review were components of or connected to more generic off-line bullying prevention education programs such as Second Step (Frey et al., 2000) or KiVa (Kärnä et al., 2013). It is not clear whether prevention programs directed at cyberbullying alone or presented narrowly as part of internet safety education without more generic bullying prevention are similarly effective.

Thus, the arguments for addressing cyberbullying in conjunction with off-line bullying are strong. Most cyberbullying is connected to off-line bullying, which is more common. The main venue for educational programs is school, where off-line bullying is a problem important to students and school administrators. The programs addressing off-line bullying have a much longer history, level of refinement, and extensive evaluation literature (Della Cioppa et al., 2015). Off-line bullying programs also utilize more modalities to affect bullying than may be available for cyberbullying programs, such as changing school culture, increasing supervision, and various school environmental interventions.

The main argument for stand-alone cyberbullying prevention programming would be that it is a topic that generates a lot of concern from parents and teachers, and their concerns could be a driver for program adoption. There may be a few specific skills that need to be imparted for avoiding or foiling cyberbullying compared to off-line bullying. However, it should be possible to capitalize on the enthusiasm for the topic and to impart the special skills in the context of a more comprehensive bullying approach.

Summary

(1) There is an extensive literature on cyberbullying. (2) Definitions and operationalizations of the concept need work. (3) Cyberbullying is strongly connected to off-line bullying. (4) There are proven effective general bullying prevention programs that appear to be effective in cyberbullying reduction. (5) The programmatic focus should be on adapting existing bullying prevention programs to encompass cyberbullying (if such adaptation is indeed needed) and promoting the dissemination of these integrated programs.

Online Sexual Exploitation

Problem

The key problem generally referenced on this topic has also been referred to as internet predators or solicitors or online-facilitated sexual abuse (May-Chahal et al., 2018). It is generally characterized as adults trying to contact children to recruit them into online or off-line sexual encounters or to obtain sexual images or videos—all of which are criminal offenses (Wolak et al., 2008). Such offences can include livestreaming and blackmauling children and youth for sexual purposes (Broadhurst, 2019).

Scope

Several youth surveys have asked about online sexual solicitation (Madigan, Villani, et al., 2018; Seto, 2013). Some such studies limit reports to “unwanted” solicitations, but none have clearly delineated the criminal inquiries by adults from what might be unwanted or unsolicited approaches by peers. One study that limited the count to aggressive or distressing solicitations estimated the past year rate among a national U.S. sample of 10- to 17-year-olds as 3% for aggressive and 2% for distressing solicitations (Mitchell, Jones, et al., 2014). A meta-analysis of nine studies on the prevalence of unwanted online sexual solicitation found a mean prevalence rate of 11.5% (Madigan, Villani, et al., 2018). One repeated study also found rates of both unwanted exposure to sexually explicit material and solicitation had declined over time (Jones et al., 2012).

Studies of internet sex crimes against children have shown their dynamics to be somewhat at odds with widely held stereotypes, which have sometimes characterized these crimes as typically involving younger children, deception, abduction, and coercive violence at the hands of internet strangers (Bergen et al., 2014; Wolak et al., 2008). In studies of actual police-reported episodes, most of the victims were aged 12 years or older (Wolak et al., 2008). The majority of the arrestees in internet solicitation crimes were not truly online strangers, but acquaintances from face-to-face environments who used technology to build trust and forge relationships that facilitated their crimes. Deceptions about identity and sexual motives were sometimes present but were not the dominant offender strategies. Instead, victims were more typically teens drawn into sexual relationships with older partners because of flattery and attention, and offers of adventure, sexual instruction, or romance. A majority had multiple sexual encounters with the offenders. Vulnerable youth provided sexual images in exchange for special treatment or status, gifts, money, drugs, or alcohol. A growing literature on this grooming or luring process has identified a variety of different elements and features (Lorenzo-Dus et al., 2016; Quayle & Newman, 2016; Webster et al., 2014; Whittle et al., 2014). In studies of offenders, an important additional subgroup of adult solicitors were identified who were not interested in contact, but only fantasy-
oriented interactions with youth online (Merdian et al., 2018; Seto, 2013).

Co-occurrence
A study of off-line and online peer sexual harassment (including unwanted solicitations) among a U.S. national sample of 791 youth found that a large majority of online sexual episodes were connected to off-line contact as well (Mitchell, Jones, Turner, Blachman-Denner, & Kracke, 2016). A study of over 1,700 Dutch adolescents found high overlap between online and off-line sexual risk-taking among these youth (Baumgartner et al., 2012). In regard to adult solicitors, more than two thirds of adults arrested for internet sex crimes against actual children in the United States were acquaintances from off-line contexts, not strangers met online (Wolak & Finkelhor, 2013; Wolak et al., 2012). There were few differences in the dynamics comparing the online offenders or off-line acquaintances. All this signifies considerable overlap and similarity between internet-mediated and more conventional forms of child sexual abuse.

Prevention Strategies
There is a mismatch between the dominant messages from educational programs and the actual dynamics of most internet sexual exploitation. Some of the most frequent educational messages about internet predators directed at children and youth include: “Remember that people online are often not who they claim to be,” “Don’t communicate online with people you do not know,” “Don’t respond to messages asking for personal or sexual information,” and “Don’t go to meet someone you have only communicated with online” (Davidson et al., 2009).

These messages are inadequate in a number of ways (Wolak et al., 2008; Wurtele, 2017; Wurtele & Kenny, 2016). First, the emphasis on “people you meet online” may mislead about online exploitation at the hands of acquaintances. Second, the programs rarely discuss that many teens use online resources and communication to explore issues of love, romance, and sexuality. For them, warnings about risky sexual conversations and people they do not know may be at odds with their peer norms and developmental interests. If they have communicated online with someone over time who seems interested in them, and with whom they have developed trust and perhaps shared images, a warning about “meeting up” with someone who no longer seems a stranger will not be effective.

A superior logic model for prevention of these criminal online interactions would involve helping youth to make better judgments about healthy romantic or sexual relationships (Wurtele, 2017; Wurtele & Kenny, 2016). Messaging that helps them understand why having a relationship with someone who is considerably older is risky would work better, including the fact that the older person may be committing a crime. Education can help them to distinguish when someone really cares about them from when someone is being sexually exploitative. Yet, such discussions are complicated and involve acknowledging that youth have legitimate curiosity about relationships and sex. These are not topics that all schools and parents are eager to address in an educational program. Moreover, if the important skill set is making good judgments about relationships and sex, this is a topic that is not specific to the internet or digital communications, but something that is best addressed in comprehensive sex and relationship education (Wolak et al., 2008).

The goal of reducing sexual risks online could benefit from the considerable literature on programs trying to influence risky teen sexual behavior in general. The literature on these programs spans both developed (Kirby, 2001; Pound et al., 2016) and developing countries (Kirby et al., 2006). Nonetheless, adult efforts to curb youth sexual behavior have been resisted by youth in almost every generation. The evaluation literature emphasizes that successful influence requires multi-session and multielement programs that give children and youth opportunities to contribute their views to program content (Pound et al., 2016), explore values, discuss relationships, and practice interpersonal skills including how to respond to solicitations (Haberland & Rogow, 2015; Kirby, 2001). Successful initiatives also involve establishing shared understandings between parents and youth regarding what constitutes appropriate and inappropriate sexual behavior (Wurtele & Miller-Perrin, 2014). Warning messages alone are not effective.

Summary
(1) This problem primarily involves teens who are groomed online and exploited by both online and off-line acquaintances, playing on the teens’ interest in romance, relationships, and their sexual curiosity. (2) Warnings about not giving out personal information and not going to meet strangers are unlikely to be effective. (3) More effective prevention should rather involve teaching youth about healthy and unhealthy relationships and offering comprehensive sex education. (4) There are evidence-based sexuality and relationship programs that are relevant to the problem and should be the foundation for such prevention education. (5) Priority research should be on how to develop effective messages about online safety in the context of such programs, recognizing that influencing teen sexual behavior has always been difficult.

Sexting
Problem
There is a large and growing literature on youth sexting. Some define sexting as the creation, transmission, or exchange of youth-produced self-generated sexual images or messages via the internet and mobile phones (Madigan, Ly, et al., 2018). Others confine the definition to explicit images that would qualify as child pornography (Wolak et al., 2012), also known as child exploitation material or child sexual abuse images (Broadhurst, 2019). However, sexting is a complex and controversial area when it comes to youth safety. The making and
exchange among older youth of sexual images and messages by itself does not fit neatly into the framework of harm and victimization. Some kinds of image sharing, such as between teens in a romantic relationship, can be consensual and nonexploitative, even if adults find it risky or morally problematic.

Nonetheless, part of the sexting spectrum does clearly fit into the harm framework, that is, when images are obtained via coercion or pressure or when they are shared without consent or used to threaten, extort, embarrass, harm, manipulate or extract money or when they cause embarrassment. Mitchell et al. (2012) have termed this abusive sexting component “aggravated sexting,” to distinguish it from sexting that occurs between consenting youth as part of romantic relationships and exploration of sexual interests. However, very little of the literature on sexting makes this clear distinction among types. This is a serious failure because it is apt to confuse a moral or reputational problem with crime and harm.

Another complication is that the term “sexting” is often used in research and discussion to include sexual text messages (Martellozzo et al., 2016), not only imagery, and it also often includes “sexy” or “nearly nude” (but not actually nude) imagery, for example, photographs of youth in underwear or swimwear. This is a problem because sexually explicit images have a different legal status, subjecting minors to possible prosecution for child pornography production, storage, or distribution, depending on jurisdictional laws (Judge, 2012).

Scope
A meta-analysis of 39 studies found 15% of youth sent and 27% received “sexts” (a term that was defined to include sexual text messages and images) and 8% had a sext forwarded without consent, a behavior that approximates “aggravated sexting” (Madigan, Ly, et al., 2018). Among a nationally representative sample of 5,568 U.S. middle and high school students, 5% reported that they had been the victim of sextortion (someone using their sexual image to try to obtain something), while 3% admitted to threatening others who had shared an image with them in confidence (Patchin & Hinduja, 2018).

Aggravated sexting, or the form of sexting that would be considered abusive, has been discussed as occurring in several contexts. First is the context of solicitations for or exchanges of images with adults. Another context is sexual images taken or obtained without consent or under coercion or pressure. A third involves images consensually obtained, but then shared with others or posted without consent. A fourth is when sexual images are consensually obtained and used to humiliate, denigrate, threaten, or extort money or favors, what is sometimes termed “sextortion.” Romantic relationships that end acrimoniously are often a context for this behavior (Wolak & Finkelhor, 2011; Wolak et al., 2018).

Co-occurrence
Aggravated sexting overlaps with bullying, when friends and acquaintances use the images to humiliate and extort. It overlaps with sexual exploitation when the exchange occurs with adults. It overlaps with intimate partner abuse when current or former romantic partners misuse the images (Drouin et al., 2015). The images can migrate into the domain of online traded illegal images, so it can overlap with sexual child abuse image or child exploitation material exchange (Wolak & Finkelhor, 2011).

Prevention Strategies
The main strategies typically utilized by prevention programs around the issue of sexting are to discourage youth from making and sharing such images. This is usually done by trying to impress upon them that they will be unable to ultimately control their usage and that the images may later embarrass them or affect some possible opportunity in their future (e.g., college, job, or relationships). A big emphasis has been to warn youth that they may be subject to prosecution. Some prosecutors have actually undertaken such actions to publicize this reality (Israelsen-Hartley, 2015; Jacobson, 2015). There has been no evaluation about the value of such messages. These messages resemble traditional fear-based, adult warnings about other premature sexual behavior that have not proven very successful because even when adolescents become aware of risks, they do not automatically stop taking them (Livingstone & Smith, 2014).

As mentioned earlier, the literature on influencing teen sexual behavior in general strongly shows that successful influence requires multi-session and multielement programs that begin early, before the onset of sexual exploration (Madigan, Ly, et al., 2018). The literature also emphasizes the role of the normative environment including the attitudes and behaviors of peers, siblings, and family members (Kirby, 2001). Some of the promising prevention strategies, therefore, have included challenging and shifting social norms around sexting for children, youth, and adults (Jørgensen et al., 2019; Patchin & Hinduja, 2019).

A review of parent training programs finds that increased parental communication with youth about sexual matters may not be sufficient, but that parent programs aimed at multiple youth risks are better at altering risky sexual behavior (Downing et al., 2011). More recent research suggests adults’ communication with youth must enable critical thinking around broader topics of respect in sexual relationships, coercion and consent, and personal boundaries (Albury et al., 2017). Additionally, emerging areas of research point toward elements of bystander (or upstander) education (Van Ouytsel et al., 2019) and teaching self-regulation (Houck et al., 2018). There is also a relevant literature about the prevention of abuse in teen dating relationships, and a number of programs have been identified that have positive influence on attitudes and knowledge (De La Rue et al., 2017). It is not known to what extent these programs have been modified to include sexting prevention.
Summary

(1) There is a large literature about sexting. (2) There is limited systematic distinction made in the literature between sexting that is malicious, criminal, and exploitative and sexting that may be part of consensual relationships. (3) Prevention strategies based on warnings and scare tactics are unlikely to be effective. (4) The problem intersects with teen sexual risk-taking in general, relationship violence, bullying, and off-line sexual exploitation. (5) Prevention strategies might best start with evidence-based programs addressing these intersecting problems.

Online Fraud, Hacking, and Identity Theft

Problem

Dangers such as fraud, identity theft, hacking, and malicious attacks on computers, computer software, smartphone applications, and wearable technology dominate discussions of internet dangers in general, but they are less frequently raised in relation to child victims specifically. Because youth are sometimes relatively inexperienced and naive users, they may have particular vulnerabilities to fraud.

There is no widely accepted categorization of cyber-fraud crimes (Gercke, 2012). The largest category of offenses against all citizens, according to an inventory at the U.S. FBI Internet Crime Complaint Center, are complaints of online commercial transactions where sellers do not send merchandise or buyers do not send payment, as well as a related category of buyer overpayment that is not rectified. There are also a number of categories that entail fraudulently obtaining passwords, account information, identities, and credit cards. It is hard to know how many of these result in actual financial losses, although they can be very disruptive for victims even without financial losses. There are categories that concern getting a victim to spend or pay money for a fraudulent purpose or cause. Then there are categories that may not be directly financial but represent malicious acts toward a person’s computer, technology resources, or online activities, for example, ruining software or hardware or making it impossible to access certain accounts. This is akin to vandalism and may have similarities to harassment or cyberbullying. It is likely that young people experience all these types of victimization and may come to experience more as their possessions are increasingly connected to the internet.

Scope

Some survey evidence about technology-mediated fraud and hacking is available. In one U.S. survey, 12% of 15- to 17-year-olds said someone hacked into their accounts and stole information, and 6% said someone stole or coercively obtained their password (Lenhart et al., 2016). A survey by a private security firm of U.S. households claimed over a million children were affected by identity fraud, resulting in losses totaling US $2.6 billion and families paying over US$540 million out of pocket (Pascual & Marchini, 2018).

Co-occurrence

Among the various offenses we cover in this review, identity theft and hacking have a fairly confined internet nexus. That is, the interactions tend to start and play out primarily in the digital environment. Fraud that occurs in online interaction may or may not be linked to off-line interactions.

Prevention Strategies

There is a large quantity of activity aimed at preventing online fraud, hacking, and identity theft through legislation, law enforcement, commercial and banking institutions, and the design of software, websites, and internet architecture (United Nations Office on Drugs and Crime, n.d.). Little of this is specific to youth victims.

There are also public education efforts targeted at the general population (Norton Security Center, n.d.). In addition, many youth-oriented internet safety and cyber-citizenship programs contain content directed at avoiding cyber-fraud. These include trainings on how to create secure passwords, exhortations about not giving out personal information, and encouragement to ask for permission from parents when responding to various online commercial offers and opportunities. Some programs explain to youth how to recognize various kinds of scams. They also discuss viruses and malware and the online environments where such vandalism is likely to lurk (Common Sense Media, 2017). Little of this has been evaluated.

This seems one area where the necessary judgments, avoidance skills, and safety practices are directly situated in and perhaps exclusive to the technology and internet context, so it may be one of the topics that fits most naturally into standalone technology education (see, for example, Weinstein, 2019) and broader internet safety (see, for example, UK Council for Child Internet Safety, 2018).

Summary

(1) There is extremely little research or advocacy on the topics of online fraud, hacking, and identity theft specifically related to youth victims. (2) This is likely a serious problem, based on the small amount of research and the fact that this problem affects a large part of the general population. (3) The skills and strategies needed for prevention may be specific to online behavior and technologies and may not have as many off-line analogs as some other internet safety topics.

Suicide and Self-Harm Promotion

Problem

Concern has been raised about websites where youth can find encouragement and instruction about how to take their own lives, cut or injure themselves, or engage in harmful eating
regimes, conducive to anorexia and bulimia (Luxton et al., 2012). Systematic reviews emphasize a mixture of findings, highlighting both negative and positive effects from such website exposure (Daine et al., 2013; Dyson et al., 2016; Marchant et al., 2017). Some studies found normalization of harmful behavior and instruction in techniques of harm and concealment. Others found support and encouragement for restraint and help-seeking.

Scope
Surveys have asked youth about exposure to suicide and self-harm sites. The pan-European EU Kids Online Survey of 17,000 9- to 16-year-olds reported 7% viewing self-harm and 4% viewing suicide content online in the past 12 months (Görzig, 2016). The 12-month rate for exposure to self-harm sites in a U.S. sample of 10- to 17-year-old youth was 1% in 2011 (Mitchell, Wells, et al., 2014).

Several dynamics have been associated with these self-harms. One is of depressed, bullied, and suicidal youth who learn about ways to take their lives and perhaps even encouragement to do so from tormentors or even similarly inclined persons who might be frequenting online pro-suicide sites (Luxton et al., 2012). A second dynamic is of anxious, depressed, eating-disordered, or otherwise vulnerable youth who learn and discuss coping strategies that involve self-injury on sites where they and others share stories and get support. A third dynamic involves youth who get caught up in self-injury through online contests around risky behavior where they may be urged to harm themselves (Bisaria, 2017).

Co-occurrence
A key element in much of the literature is that the youth most affected by online self-harm influence are those with some preexisting vulnerability, that is, youth who might be engaging in self-harm even in the absence of online influence. Suicide and self-harm are off-line activities that have strong roots in off-line dynamics including family problems, peer rejection, trauma exposure, social isolation, and mental health issues (Abdelraheem et al., 2018). Some studies find association between self-harm site exposure and internet overuse, sexual risk-taking, and bullying victimization (Marchant et al., 2017; Mitchell & Ybarra, 2007). There is also a suggested co-occurrence of suicide ideation with serious forms of bullying and cyberbullying (Hinduja & Patchin, 2010, 2019). It is well-established that even if youth are getting harmful online influence, there are generally strong and determinative off-line contributors as well (Harris et al., 2009).

Prevention Strategies
The general literature on suicide and self-harm prevention is extremely relevant to this internet component of the problem. A review of programs to prevent suicide and self-harm among high-risk youth concludes that programs can be successful, and successful programs tend to be multisystemic, intensive, and have family involvement (Brent et al., 2013). This suggests that broad-based universal digital literacy education will not provide the kinds of intensive and therapeutic support that are required to prevent and address self-harm and protect high-risk youth.

The main messages in youth suicide prevention programs involve teaching coping skills and stress management, dispelling myths about suicide, alerting youth to signs and symptoms, promoting help-seeking, and mobilizing bystanders to act on behalf of self-harming or suicidal friends (Brent et al., 2013). There is also a literature about self-harm prevention, but most of the studies are individual therapeutic approaches such as dialectical behavioral therapy and mentalization therapy (Hawton et al., 2015; Ouirin et al., 2015).

Given that children and youth are more likely to seek support from peers and informal networks than health care professionals (Michelmore & Hindley, 2012), it may be that suicide and self-harm prevention content belongs best in universal child and youth mental health promotion and school health curricula. These will help mobilize informal support; create positive, caring, and inclusive school environments; and connect children and youth with local helplines and mental health services. Additionally, the literature also points to the need for effective school-based screening and referral systems with capacity to identify and reach vulnerable children and youth (Joshi et al., 2015).

Summary
(1) Self-harm and suicide ideation are serious problems in the youth population, but the role of the internet is not clearly established, as it may exert both an aggravating and a mitigating influence. (2) Those vulnerable to negative, self-harm internet influence tend to have histories of off-line adversities including depression, anxiety, family problems, and bullying victimization. (3) There are well-established and evidence-based self-harm and suicide prevention programs, but little of this is incorporated or even necessarily suitable for incorporation in internet safety education.

Internet Overuse/Addiction
Problem
There is a large literature and considerable international concern about young people overusing technology and the internet. But at the same time, there is controversy over whether (or under what conditions) it should be classified as a mental health or behavioral problem (Aarseth et al., 2017; Markey & Ferguson, 2017; Saunders et al., 2017). There are also pervasive definitional issues. Much of the literature references the problem as internet gaming disorder, but there is also a recognition that the overuse often encompasses off-line digital games and also other online nongaming activities. Various terms have been used for the broader concept such as internet addiction, cyberspace addiction, internet addiction disorder, online
addiction, net addiction, pathological internet use, and high internet dependency (Byun et al., 2009).

Clinical descriptions portray individuals who spend 10 or more hours per day gaming and who experience disorders due to consequent sleep deprivation, day–night reversal, dehydration, malnutrition, seizures, and pressure sores, as well as irritability, physical aggression, depression, and a range of social, academic, and vocational problems (Saunders et al., 2017). The World Health Organization has designated gaming disorder with off-line and online variants as a clinical entity in the International Classification of Diseases (World Health Organization, 2016). It is listed as a potential but not yet official diagnosis in the Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition (American Psychiatric Association, 2013) used in American mental health practice.

Scope

Since there is controversy and debate about how to define a pathological level of use, and whether the available assessment tools are useful at specifying it, estimates about prevalence vary considerably. One conservative assessment placed the population prevalence of gaming disorder at under 1% of those youth who play games (Przybylksi et al., 2016), but the prevalence of the disorder in 37 cross-sectional studies ranged widely from 0.7% to 27.5% with higher rates of 10%–15% in East Asian countries (Saunders et al., 2017).

Co-occurrence

In studies of clinical populations, the strongest predictors of addiction are mental health conditions—Attention-Deficit/ Hyperactivity Disorder (ADHD), depression, anxiety, and impulsivity (Hyun et al., 2015; Mitchell et al., 2007). Trauma memories among males and problems with affect regulation among females appeared to increase the risk of problematic internet use during late adolescence (Schimmenti et al., 2017). Overuse has also been associated with bullying victimization (Boniell-Nissim & Sasson, 2018). A systematic review found a complex array of risk factors such as social isolation, impaired social functioning, poor academic performance, truancy, and school disengagement (Paulus et al., 2018). This again suggests schools as important venues for prevention, screening, and early intervention, as well as tie-ins with bullying prevention.

Prevention Strategies

Efforts to counteract overuse are most developed in East Asian countries such as Korea and China. Psychoeducational programs lasting 3–6 weeks for school-age children provide information about the dangers of overuse, self-control techniques, limit-setting and time management skills, and alternative activities. A review based on 13 quantitative outcome studies found mixed results for such efforts (King et al., 2018). Some of the more successful programs appear to have a broad mental health approach and are directed at high-risk youth (Deng et al., 2013; Joo & Park, 2010).

Other prevention tools that have been tried include promoting usage guidelines for children—such as maximum “screen times,” no devices in the bedroom, and no devices before bedtime, although these initiatives have been directed mainly toward increasing children’s physical activity via reducing sedentary time with digital devices (see World Health Organization, 2019). Family factors and parental mediation are related to overuse (Kalmus et al., 2015; Schneider et al., 2017). Parents are being advised to enforce restrictions on their children’s digital use, and a variety of tools have been developed to assist parents with this task (e.g., Family Online Safety Institute, 2019). Internet and gaming companies are being urged to warn consumers about risks and provide referral services. China had a policy making online gaming unavailable during certain hours of the day (King et al., 2018).

Summary

(1) There is a growing research and prevention literature on internet overuse/addiction that is being led particularly by Asian countries where the problem may be more frequent. (2) Findings on co-occurrence and outcomes studies suggest that integration with general physical and mental health promotion may be valuable. (3) There is some research that parental mediation to establish limits may be associated with overuse avoidance.

Other Topics

The foregoing has not been a comprehensive review of topics addressed in youth internet safety education programs. Among the other topics these programs sometimes cover are privacy (Livingstone et al., 2019) and reputation, ethics and empathy, content and copyright, and digital etiquette. Many programs designate themselves as “digital citizenship” (Common Sense Media, 2017) or “digital intelligence” (DQ Global Standards Report, 2019) rather than “safety” programs (Walsh et al., 2019). Nonetheless, the topics we have reviewed have some commonality in being harms to youth that have prompted persistent concern and some research. To some extent, these six safety topics also lie behind discussions of privacy, reputation, ethics, empathy, digital etiquette, and other more abstract concerns such as what it means to be a “good digital citizen” because the serious harms generally envisioned under these topics typically converge on victimization or perpetration of bullying, fraud, hacking, sexual image misuse, or exploitation.

Online and Off-Line Prevention Integration

Nonetheless, an important question raised by the way various internet safety topics are packaged into diverse programs is whether they belong together as a technology-related ensemble or whether they may have more in common with and should be combined with related off-line harm and victimization.
prevention. Our review of the literature on online harms to children leans toward the following recommendation: *Most prevention education programs on internet harms are best carried out through integrated and comprehensive programs that focus on both off-line and online risks and dynamics conjointly.*

Thus, programs to combat cyberbullying should address both conventional school bullying and cyberbullying. Programs to combat online solicitation should address both conventional sexual abuse and its online forms. Programs to combat sexting and sextortion should also deal with conventional dating and relationship violence and abuse. Programs about online suicide and self-harm should be part of general suicide prevention and mental health risk reduction. This is different from much of current practice where educators are creating stand-alone internet safety programs that focus on discrete internet portions of these problems.

The logic behind the *integrated approach* to internet safety is bolstered by several important findings from our review:

1. Most problems described as internet harms have roots and manifestations in both the off-line and online contexts and have similar dynamics in both contexts.
2. The comparable off-line forms of these harms such as sexual exploitation and bullying are generally more pervasive than their related online forms.
3. Studies have found that the risk factors associated with online problems are similar to those of off-line exposure and that there are few unique online risk factors, suggesting that integrated focus on general risk should be effective with online behavior.
4. The evidence basis for effectiveness is much better developed for programs in the off-line than the online exposure domain. In fact, there is scant literature on the efficacy of stand-alone online safety programs. Therefore, the likelihood of success is much greater if developers start with the existing evidence-based, off-line-oriented programs and add internet-oriented content to them, as opposed to building new, stand-alone, untested online prevention programs.

Here are more details on these assertions.

First, most of the online harms under consideration in internet safety education are strongly connected to off-line contexts. For cyberbullying, studies show that half or more of episodes of cyberbullying and harassment are committed by off-line acquaintances and are extensions of conflict and bullying that are often rooted in the off-line school, family, or neighborhood environment (Sabella et al., 2013; Waasdorp & Bradshaw, 2015). One study found that two thirds of online harassment episodes were linked to off-line episodes (Mitchell, Jones, Turner, Shattuck, & Wolak, 2016). For sexual solicitation, more than two thirds of offenders arrested for internet sex crimes against children in the United States that involved digital grooming were actually acquaintances from off-line contexts, not strangers met online (Wolak & Finkelhor, 2013; Wolak et al., 2012). There were few differences in the dynamics of grooming between the two groups.

In regard to sexting, in a survey of 1,600 victims who had had a sexual image sent or made nonconsensually that was then subject to threats and extortion, 60% of victims said the perpetrator was an off-line acquaintance (Wolak & Finkelhor, 2016), often an ex-boyfriend or girlfriend. This puts aggravated sexting in the context of off-line dating abuse and bullying, both of which are, in turn, related to each other (Wincentak et al., 2017; Zych et al., 2019). Finally, research shows that youth who are attracted to online self-harm and suicide sites are youth with off-line adversities ranging from family problems, bullying, and psychiatric disorders (Abdelraheem et al., 2018). So, the overlap between online and off-line dynamics is considerable.

Second, to the extent that there are comparable measures of online and off-line exposures to similar forms of harm, the *off-line exposures* tend to be more numerous. For example, one large meta-analysis found cyberbullying less than half the rate of conventional bullying (15% vs. 36%; Modecki et al., 2014). For another example, in the United States arrests for sexual exploitation involving online communication constituted less than 5% of the arrests for sex offenses against children overall (Wolak et al., 2009).

Third, risk factors for online and off-line harms are similar. In a factor analytic study of over 19,000 youth aged 10–16 who were part of the EU Kids Online consortium, the results showed that vulnerability to online risks is best explained by a conjoint factor that predicted vulnerability to both online and off-line risks (Görzig, 2016). In another large study of bullying prevention in Colorado, there were no predisposing factors for online risk alone (Williams & Guerra, 2007). The implication is that programs that address more general risk predispositions should be effective in preventing online as well as off-line dangers.

Finally, perhaps the most persuasive argument for an integrated approach to internet safety is that the evidence base is so much better developed in efforts to prevent off-line harms of a related nature (Della Cioppa et al., 2015). Meta-analyses have identified over 100 evaluations of bullying prevention programs and have found them to be successful in reducing bullying (Gaffney, Ttofi, & Farrington, 2018; Ttofi & Farrington, 2011). The one extensive meta-analysis to address prevention of online harm also found reductions in cyberbullying, but the majority of the programs in the review were preexisting off-line bullying or integrated programs addressing both off-line and online forms (Gaffney et al., 2019).

Meta-analysis has also identified 24 evaluations of school-based sexual abuse prevention programs (Walsh et al., 2015) and concluded that they increase knowledge, protective behaviors, and disclosure. Meta-analyses have identified two dozen evaluated programs to prevent teen dating abuse (De La Rue et al., 2017; Ting, 2009). Programs have been shown to change knowledge and attitudes but have not been shown yet to affect victimization or perpetration.

There have also been dozens of sexual risk-taking prevention programs in a variety of international contexts that have been evaluated and reviewed in meta-analyses (Kirby, 2001;
Marseille et al., 2018; Mason-Jones et al., 2016; Song et al., 2000). The conclusions are mixed, showing actual outcomes such as pregnancy and HIV infection difficult to influence. Nonetheless, the considerable efforts in this area leave many insights about more effective approaches that can be built upon to possibly influence risky internet sexual activities.

The literature on self-harm and suicide prevention does indicate success in accomplishing these goals and has considerable guidance on components of successful programming (Brent et al., 2013; Ougrin et al., 2015). In regard to overuse and addiction, some of the more successful programs to reduce internet overuse appear to have a broad mental health approach borrowed from generic programs (Deng et al., 2013; Joo & Park, 2010; King et al., 2018). There is a large foundation of evaluated programs, mostly from off-line contexts, that can be the basis of an integrated approach to online risks.

**Summary**

The argument for integrated prevention does not deny that there may be internet-specific skill sets that are valuable for young people to learn. However, the literature on internet harms and their risk factors points to a strong interconnection between online and off-line dangers and dynamics. It also points to common risk factors in the lives and environments of youth. The existence, sophistication, and longer history of programs directed at related off-line risks also points to these programs as the place to start for the development of protections against internet dangers. We urge that efforts to prevent internet harms be oriented to building upon programs and materials that have been developed for related off-line risks. This is in contrast to the current movement to build new and stand-alone programs addressing online safety as a separate problem.

**Implications for Practice, Policy and Research**

Our review of the literature on online harms to children leans toward the following recommendation: Most prevention education programs on internet harms are best carried out through integrated and comprehensive programs that focus on both off-line and online risks and dynamics conjointly.

**Declaration of Conflicting Interests**

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

**Funding**

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This project was supported with funding from Facebook and the World Health Organization.

**ORCID iD**

David Finkelhor https://orcid.org/0000-0001-7008-4252
Kerryann Walsh https://orcid.org/0000-0003-2672-2688
Kimberly Mitchell https://orcid.org/0000-0003-1974-1637

**References**


Author Biographies

David Finkelhor is Director of Crimes Against Children Research Center and professor of sociology at the University of New Hampshire. He has been studying the problems of child victimization, child maltreatment, and family violence since 1977.

Kerryann Walsh is a professor in the Faculty of Education at Queensland University of Technology. Her research focuses on school-based programs for prevention of child victimization, prevention of harm to children in child- and youth-serving organizations, and education and training for child protection. She was an academic advisor to Australia’s Royal Commission into Institutional Responses to Child Sexual Abuse.

Lisa Jones is a research associate professor of psychology at the University of New Hampshire. She has been conducting research on issues of child victimization epidemiology and prevention for over 20 years. Her current work focuses on technology-based child victimization, hate and bias crime victimization, and commercial sexual exploitation of children.

Kimberly Mitchell is a research associate professor of psychology at the University of New Hampshire. Her research focuses on childhood violence and adversity exposure with an emphasis on identifying innovative ways to inform prevention efforts and promoting well-being. She has particular expertise in technology-involved victimization, drug-endangered children, self-directed violence, bias victimization, and firearm violence.

Anne Collier is a writer and advocate who has been chronicling the public discussion about youth and digital media since 1997. She is the founder and executive director of national nonprofit organization The Net Safety Collaborative (TNSC), creators of a social media helpline for U.S. schools.