ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/332989526

Internet Safety

Article · May 2019

DOI: 10.1002/9781118978238.ieml0093

CITATIONS
9

READS
20,662

4 authors, including:

Michel Walrave
University of Antwerp
218 PUBLICATIONS **7,064** CITATIONS
SEE PROFILE

Koen Ponnet
Ghent University
394 PUBLICATIONS **9,678** CITATIONS
SEE PROFILE

Joris Van Ouytsel
Arizona State University
105 PUBLICATIONS **3,543** CITATIONS
SEE PROFILE

All content following this page was uploaded by Koen Ponnet on 10 July 2020.

The user has requested enhancement of the downloaded file.

Internet Safety

LIES DE KIMPE
University of Antwerp and Ghent University, Belgium

MICHEL WALRAVE
University of Antwerp, Belgium

KOEN PONNET
Ghent University, Belgium

JORIS VAN OUYTSEL
University of Antwerp, Belgium, and University of Texas Medical Branch, USA

The term "Internet safety" encompasses a set of issues that are, either directly or indirectly, related to the physical and psychological well-being of Internet users. Also referred to as "online safety," "digital safety," or "e-safety," this concept is associated both with the risks individuals face online and with the ways they can protect themselves against those risks. A large body of research within this domain is dedicated to the safety of children and adolescents. One reason for this specific focus is the fact that young people are the most active Internet users. Being online offers them a whole range of opportunities, but at the same time this may confront them with several risks. Adolescents may be particularly vulnerable when facing those online risks as compared to adults, because they are, among other things, more stimulated by short-term rewards than by long-term prospects and because they have a higher tendency to take part in risky behaviors than adults. An additional concern related to this age group is that the way in which they access the Internet differs from previous generations. Most devices that are used to go online have become portable and, therefore, young people spend more and more time alone with their laptops, smartphones, and tablets, in their bedrooms for example. In consequence, children's Internet use is often free of parental supervision.

That most studies focus on young people's online behavior does not mean, however, that adults are insusceptible to online risk. Just like children and adolescents, they are connected to the Internet. They may be less vulnerable to some risks and less prone to taking risks in general, but they are not immune to the potentially negative consequences related to risky Internet use, such as reputational damage or losing money through online scams. Furthermore, some research points out that older Internet users (65- to 90-year-olds) tend to have less experience with various types and functions of technology (Olson, O'Brien, Rogers, & Charness, 2011), implying that older users may be just as vulnerable online as their younger counterparts in some situations.

The International Encyclopedia of Media Literacy. Renee Hobbs and Paul Mihailidis (Editors-in-Chief), Gianna Cappello, Maria Ranieri, and Benjamin Thevenin (Associate Editors).
© 2019 John Wiley & Sons, Inc. Published 2019 by John Wiley & Sons, Inc.
DOI: 10.1002/9781118978238.ieml0093

Over the years, academic researchers from different disciplines (e.g., communication studies, psychology, law), educators, media outlets, and governmental institutions have voiced concerns about the risks people face online on a daily basis and have expressed the need for appropriate interventions in order to minimize the harm some online activities might cause, especially to children. More recently, however, some academics have started to label this increased worry as "moral panic." They claim that the Internet is not as dangerous as generally assumed by public opinion, since not every risk Internet users face will inevitably result in a negative outcome or harm. Nonetheless, they do not deny that some Internet users have negative experiences which result in harm. Therefore, it is important to address these issues so the risks Internet users encounter are minimized without limiting the opportunities the World Wide Web has to offer.

A number of different categorizations are used to classify online risks. One frequently applied categorization is created within the framework of the project EU Kids Online and distinguishes aggressive, sexual, commercial, and value-related risks (Livingstone, Haddon, Görzig, & Ólafsson, 2011). In a second categorization, a distinction can be made between risks related to online content and those related to online contact (Youth Protection Roundtable, 2009). Contact risks assume a direct connection or interaction between offender and victim, while this kind of connection is absent or less visible when facing content risks. Based on the framework derived from EU Kids Online and the Youth Protection Roundtable Toolkit, a categorization is proposed in Table 1 that will be used in the remainder of this entry. It is important to note that overlap may exist between some of these categories (e.g., between aggressive content and some value-related risks). Moreover, some risks may co-occur in specific online contexts (e.g., hate speech could lead to cyberbullying). As such, it is not the scope of this entry to present an exhaustive overview of all risks Internet users may encounter.

Aggression risks

The freedom and anonymity the Internet offers can be used to hurt others through spreading hateful or violent messages, images, and/or videos. Although many types of cyberaggression exist (e.g., flaming, outing, (in)direct harassment), the umbrella term most often used to talk about this variety of online aggression is *cyberbullying*. No consensus exists on the definition of this term, but it can be understood as aggressive or cruel acts carried out by an individual or group against a victim by means of the Internet or other digital technologies (Tokunaga, 2010). Some definitions stress the power imbalance between the victim and the perpetrator, while others emphasize the repetitive nature of the aggressive acts.

Although everyone can become a victim of cyberbullying, research is mostly conducted among children and teenagers. Because differences in both definition and measurement exist, it is difficult to estimate the prevalence of cyberbullying within this age group. On average, between 20% and 40% of young people have been cyberbullied at least once (Tokunaga, 2010). The number of cyberbully victims has even increased during the past decade (Jones, Mitchell, & Finkelhor, 2012). This is not very surprising, since young people have become active users of social media and the Internet. As a result, an important part of their social life now occurs online. The increase in

Table 1 Categorization of online risks.

	Content risks	*Contact risks*
Aggression	Violent or hateful content	Cyberbullying Cyberstalking
Sexual	Pornography	Sexting Sextortion Online grooming
Value-related	Incorrect or harmful information on • suicide • self-harm • anorexia • racism • hate speech • …	Incorrect or harmful advice on • suicide • self-harm • anorexia • racism • hate speech • …
Commercial	Gambling Copyright infringement Hybridization of commercial content and entertainment	Harvesting personal data Spam Phishing Identity theft

Source: Based on Livingstone et al. (2011); Youth Protection Roundtable (2009).

the number of cyberbully victims should thus be seen as a shift in or expansion of the bullying context, rather than as an increase in the number of bullied children. The majority of cyberbully victims are upset by this experience. Depending on the frequency, length, and severity of the aggressive acts, experiencing cyberbullying is associated with psychological problems (e.g., depression, social anxiety), affective disorders (e.g., detachment), and academic problems (e.g., drop in grades, increased absences). On a more aggregated level, cyberbullying is linked to negative school climate. It is suggested that the harm caused by cyberbullying is potentially more severe when compared to offline bullying as it can easily happen anonymously, may be witnessed by a wider audience, and can occur at any time, 24 hours a day. It should be mentioned, however, that apart from the latter, these features are not unique to the cyberbullying context (e.g., spreading rumors is a form of anonymous offline bullying) (Heirman et al., 2016).

A specific form of cyberbullying is *cyberstalking*, or the repeated and unwanted pursuit of an individual using electronic devices. These digital technologies can be used by stalkers both to collect information about their victim and to reach out to him or her. The difference between cyberbullying and cyberstalking is that stalkers do not by definition wish to cause harm, although they usually do. It is assumed that the perpetrator often wants to initiate a love relationship or friendship with the victim. Other possible motivations are jealousy and revenge. Stalking victims may suffer from psychological (e.g., inner unrest, anger, depression) and social problems (e.g., mistrust toward others). In contrast to offline stalking, cyberstalking has been barely examined. One study showed that 6.3% of people stated to have been a cyberstalking victim for at least 2 weeks (Dreβing, Bailer, Anders, Wagner, & Gallas, 2014).

Next to interpersonal forms of aggression, Internet users may be confronted with *violent content*. In this case, the aggressive message is not directed straight at the user. Violent and hateful images, videos, or texts can be a depiction of reality but can also be displayed within forms of entertainment, such as games. The latter have been studied quite extensively in the past, especially since gaming is very popular among youths. For instance, research has demonstrated that violent video game play is associated with aggression, both in the short and long term (Willoughby, Adachi, & Good, 2012). Therefore, it is not unthinkable the same link exists between other types of online violence and aggressive behavior or, for example, between online violence and radical ideologies (see below).

Sexual risks

The Internet also serves as a platform for the distribution of sexually explicit content, such as online *pornography*. When (young) Internet users face this potentially age-inappropriate and/or unsolicited content, this can be upsetting. One study found that 14% of young people (9- to 16-year-olds) were confronted with sexual content within the 12 months prior to the survey (Livingstone et al., 2011), while other research indicates that 23% (10- to 17-year-olds) saw pornography unwillingly in the past year (Jones et al., 2012). The older teenagers get, the more likely it is they have seen sexual images online. A fifth to a quarter of them reported to have been very upset after seeing this explicit content (Livingstone & Smith, 2014). Younger children are more likely to be bothered than older children.

Teenagers and adults can also produce sexual content themselves. When they send these self-produced sexualized texts, photos, or videos to each other via cell phones or the Internet, this is called *sexting*. Because a variety of definitions and measurements of sexting exist, estimates of prevalence differ widely. The rates depend highly on the nature of the content (nearly nude, nude, or explicit; text, photo, or video), the role the individual takes on (receiver or creator), and the age of the sample. Results therefore range from 2.5% to 25% for minors and from 30% to 54% for adults (Döring, 2014). Although some consider sexting to be a normal part of sexual experience, individuals who engage in sexting should be aware of the risks linked to this specific online contact. Once a sexual message or image is sent, it is difficult to control what happens with it and who will be able to see it. When a sexting message reaches unintended audiences, this content can cause reputational damage or can be abused by (cyber)bullies. In addition, sexting can put individuals at risk of *sextortion*. This is a type of blackmail in which the offender obtains sexually explicit material created by the victim and uses it to pressure him or her to perform sexual acts or to pay a certain amount of money. By threatening to reveal this intimate content to friends or family, offenders try to achieve their goals. Because it is assumed a lot of sextortion cases stay unreported, it is difficult to estimate its prevalence.

Similar to sextortion are concerns related to adults approaching children online with the intent to sexually abuse them, also known as *online grooming*. Social media platforms and mobile applications offer sexual predators a whole range of new and

easy tools to contact young people. Although this risk should be taken seriously, the moral panic surrounding this topic may not be in proportion to the number of online grooming victims. First of all, it is assumed that children are more frequently groomed by acquaintances in an offline setting than by strangers on the Internet (Livingstone & Smith, 2014). It is further true that young people do not always know who they are chatting with online, but according to the EU Kids Online study only 9% of young people actually arrange a face-to-face meeting with a stranger. It happens even less frequently that youngsters go to such meetings alone or without telling another person. Over half of these meetings are with people related to their own friendship circle. When meeting an unknown person face-to-face, 11% of the European youths claimed this encounter made them feel upset or uncomfortable. This equals about 1% of all young Internet users (Livingstone et al., 2011), which indicates that only a relatively small proportion of youths experience real harm as a result of meeting strangers.

Value-related risks

While risks related to digital forms of aggression and sexual risks have received ample research attention, less is known about value-related risks. These risks are related to the harmful content and untrustworthy information that can easily be found online and that can negatively affect the values a person holds regarding him- or herself, a group of individuals, or society as a whole. For example, there are numerous sites available on *suicide* and *nonsuicidal self-injury* (NSSI), respectively depicting and discussing different ways to end one's own life and ways to inflict self-harm. These sites are easily accessible. The majority do not explicitly encourage harmful behaviour, however, but use a neutral tone (Lewis & Knoll, 2015). Some even promote help-seeking (Mok, Ross, Jorm, & Pirkis, 2016).

Still, it should be considered that being confronted with information on suicide methods or self-injury may pose a risk to vulnerable individuals, although this is not the case by default. Research has shown that suicide-related Internet use is associated with an increase in suicidal thoughts (Mok et al., 2016). This result may imply that processing tips and advice on suicide and NSSI indeed leads to an increase in destructive thoughts or can even reinforce harmful behavior. However, this observation may just as well suggest that the Internet is used as a tool to seek help when suffering from suicidal ideation or self-harm tendencies. The interactive features of suicide and NSSI websites, such as chatrooms, may offer individuals who seek help a virtual space where they can give each other emotional support. More research is necessary to fully understand the motivations of the Internet users who visit these types of webpages.

"Pro-ana" sites, which portray anorexia as a lifestyle choice instead of a disease, have the same twofold nature. They may offer support to people with an eating disorder, but this doesn't mean the websites are completely beneficial and that they cannot be potentially harmful to the site's users. One study on pro-anorexia sites, for example, (Bardone-Cone & Cass, 2007) showed that respondents who viewed a pro-ana

website perceived themselves as heavier than those exposed to other websites. These findings suggest that taking part in this type of unsafe community can be perceived as harmful.

Research discussing value-related risks is scarce. Therefore it is difficult to gauge how many people visit websites with such content. The EU Kids Online survey offers some insight into this topic by showing that up to 5% of teenagers have already visited a suicide site, 7% have been confronted with a self-harm site, and 10% have seen pro-ana websites (Livingstone et al., 2011). Little is known, however, about other ways in which unhealthy messages are spread, for instance through social networking sites. It is equally unclear what kind of short- and long-term effects being exposed to value-related risks might have on Internet users.

The Internet is also used by violent ideological groups to spread *hateful or even aggressive messages*. Within these groups, a set of beliefs is shared that considers violence as a justified way to achieve group goals. Often their hate is directed toward people with a different race, religion, or sexual orientation. With their ideology, these groups offer a clear framework that makes sense of the world and reduces ambiguity, which makes membership very attractive to some individuals. Believed to be especially vulnerable to this type of reasoning are (young) people in search of an identity and a sense of belonging. Depending on how often and how long certain messages are consulted, exposure to hateful or racist content can shape belief systems. Moreover, it is feared that exposure will in some cases lead to the mobilization of supporters to become involved in extreme actions, online or even offline. In this respect, it is worrying that in Finland 67.4% of 15- to 18-year-olds (Näsi, Räsänen, Hawdon, Holkeri, & Oksanen, 2015) and in the United States 65.4% of 18- to 36-year-olds were exposed to hate materials online in the 3 months prior to the study (Costello, Hawdon, Ratliff, & Grantham, 2016). One fifth of the latter group was even confronted with content calling for violence. Time spent online and specific attitudes like (a lack of) trust in the government were closely related to their likelihood of exposure. In this regard, it is remarkable that there is still a lot of uncertainty about a possible connection between exposure to hateful online content and the engagement in violent extremism or the adoption of a radical ideology.

Commercial risks

Businesses and other commercial actors have developed several ways to *harvest personal data* from Internet users. Cookies, for example, which are web-tracking and information-gathering tools, are used to save personal data from the users of a specific website (e.g., which buttons are clicked, which pages are visited). On the one hand, these data can be used to personalize advertisements and other content, which makes them more relevant for the consumer. On the other hand, however, this data collection often takes place in a (for the Internet user) nontransparent way. Although it is sometimes possible to decline cookies, this may result in the inability to consume (some of) a website's content. Consumers are thus left with little choice. The same holds for social network sites (SNS): without the disclosure of at least some personal

information it is impossible to enjoy the benefits related to SNS. These practices can be perceived as an invasion of consumers' privacy. Moreover, people are often uninformed about how the collected data are used exactly.

A specific concern exists surrounding the collection of personal data from young people. Since children and teenagers influence family purchase decisions and often have pocket money of their own to spend, they are an attractive demographic for advertisers. The fact that young people are avid Internet users makes it easy for commercial actors to target them online and collect their personal details. It is questioned, however, to what extent young people are able to assess whether they are consuming advertisements and whether their personal data are being collected. This may be problematic, especially when they are confronted with *hybridizations between marketing content and entertainment*, such as "advergames" or online games containing brand communication. Because the persuasive intent of these games is less obvious, the games might make young people more susceptible to the commercial messages as compared to other forms of advertising. It might also affect their decisions regarding the disclosure of personal data.

If individuals do not carefully manage personal data, this can have unwanted consequences. For instance, one may receive *spam*, which can be defined as all unsolicited e-mail communication, ranging from unsolicited advertising, through inappropriate (sexual) content, up to fraudulent messages. The latter can be part of a *phishing attack*, in which dishonest individuals or criminal organizations try to collect personal financial information (e.g., passwords, credit card numbers), often while pretending to be a trusted company. If Internet users fall for this con, this can result in *identity theft* and the loss of large amounts of money.

Lastly, some commercial risks directly resulting from Internet users' own conduct should be discussed. One of them is the usage of *illegal copies of software and media files*, that is, the illegal downloading or streaming of copyrighted music, movies, games, or e-books. Although those copyright infringements negatively affect the financial situation of individual creators and the creative industry as a whole, some consider illegal downloading, sharing, and streaming an acceptable practice. In theory, however, digital piracy is a crime and copyright violators risk fines or even imprisonment.

Also, *gambling sites* can have negative consequences for their users. This relatively new branch within the gambling industry, which encompasses all forms of wagering and gambling through devices connected to the Internet, has proven to be rather hard to study. As online gamblers are not easy to reach, most research uses purposive sampling strategies to collect information. Therefore, the prevalence rate of online gambling is difficult to estimate. One survey in the United Kingdom, however, indicated that 14% of the respondents had gambled online in the past year (Wardle, Moody, Griffiths, Orford, & Volberg, 2011). It is noteworthy that younger people are more likely to use online gambling methods. This might be explained by the fact that some websites do not ask for a user's age. Moreover, studies show that problem gambling appears more frequently among those who use the Internet to gamble compared to those who do not. In practice, problem gambling can have several negative consequences: evidently it can cause financial problems, but it can also lead to interpersonal and mental health problems (e.g., stress, anxiety).

Intervention

While a growing body of literature focuses on specific online safety issues, evidence-based interventions are lacking to successfully reduce online risks and harm. Several possible approaches have, however, been developed. Most often, *awareness campaigns* created by (inter)national governmental organizations are used (e.g., ThinkUKnow, an online safety campaign launched in the United Kingdom and Australia). Campaigns offer the option to reach both minors and adults and can stimulate public debate and raise awareness about Internet safety. At the same time, it isn't always clear to what extent these campaigns also contribute to behavioral change.

Additionally, *legislative initiatives* have been taken in the past to enforce a decrease in online risks. An important part of these initiatives deals with the regulation of data collection and privacy. A well-known example in this context is the Children's Online Privacy Protection Act (COPPA), created in the United States to regulate the online collection of personal data from children. The European Union has similar data protection rules. These do not specifically focus on online data collection, however, but are applicable in a digital context. Moreover, legislation is also issued on hate speech, violent content, or pornography that can be implemented in the online environment.

Other stakeholders, such as *teachers and schools*, can contribute to the online safety of youths in particular**.** Since the Internet is often used for educational purposes, both at school and at home, it is appropriate that educators pay attention to children's online safety. A first approach schools have been using is technical mediation in the form of filtering software that aims to block unwanted or harmful content. It should be taken into account, however, that these tools aren't capable of removing Internet risks completely. Moreover, filtering software cannot serve as a substitute for teaching young people how to use the web responsibly. Also, single-session lectures in schools dedicated to improve children's knowledge on online safety are claimed to have rather little effect (Jones & Finkelhor, 2011). Most of these programs are implemented without any evaluation of their effectiveness. More integrated and evidence-based approaches are thus needed. An important example in this context is the Finnish KiVa Program. This program, aimed at the reduction of bullying, considers bullying a group phenomenon. It encourages bystanders to speak out and to support bully victims. In this way, bullies do not gain status within the peer group, which discourages further bullying behavior. The program provides lessons and exercises, an online learning platform, and a guide for parents. This approach has proven its effectiveness in reducing both traditional bullying and cyberbullying. It is suggested that the implementation of similar evidence-based programs to tackle other online risks, such as sexting, might be interesting. These programs can aspire to prevent specific risks, but can also teach young people how to react when they have a negative online experience. Two coping strategies might be interesting for children and adolescents in this regard: communicating (e.g., talking to someone trustworthy about the problem) and problem-solving (e.g., reporting the problem, blocking the sender). The latter coping strategy, in particular, appeals to children who feel harmed by an online experience (Vandoninck, d'Haenens, & Roe, 2013). Other authors suggest that it might be interesting to adopt a more general approach, instead of developing specific Internet safety education. They assume that stressing general life skills

like empathy, emotional intelligence, and conflict management might be beneficial. An example of such an approach is the Fourth R program, which focuses on the development of healthy friendly and romantic relationship skills. This program has proven its effectiveness in decreasing several offline risk behaviors, hence the same might hold true in an online context.

Efforts made to create a safer online environment for young people don't stop after school. Since young people most often go online at home, *parents* in particular can contribute to the online safety of their children. Two broad types of parental mediation can be distinguished: restrictive and active mediation. The former implies that parents try to control or limit the amount of time spent online, the content that is consulted (e.g., by using blocking or filtering software), and the online activities their children are involved in. This approach is perceived rather critically, since restrictions might motivate young people to use avoidance techniques. Additionally, some state that this form of mediation is indeed linked to less exposure to risks, but at the same time limits the opportunities the Internet has to offer (e.g., entertainment, communication, learning). With active mediation these problems may not arise, since in this case parents do not try to limit children's Internet use. Instead they share online activities with their children, teach them how to avoid certain online risks, and discuss their Internet use. In this way, children are able to explore the online environment by themselves, but with the guidance of an adult. It is claimed that this may improve children's learning process.

Apart from parents and teachers, peers are also an important source of influence in adolescents' lives. However, little is known about peer influence and peer support in relation to online safety. It might be interesting for future research to explore how peers can be taught skills to help each other avoid Internet risks. Moreover, future studies should address the lack of knowledge on the risks faced by relatively new Internet users, such as very young children and the elderly. Since these demographics have become more and more present online, it is imperative to develop a better understanding of their Internet use and how they cope with online risks. At the same time, academics should attentively follow the development of new modes of access to the Internet, as well as the emergence of new online risks.

SEE ALSO: EU Kids Online; Sexting

References

Bardone-Cone, A.M., & Cass, K.M. (2007). What does viewing a pro-anorexia website do? An experimental examination of website exposure and moderating effects. *International Journal of Eating Disorders, 40*(6), 537–548. doi: 10.1002/eat.20396

Costello, M., Hawdon, J., Ratliff, T., & Grantham, T. (2016). Who views online extremism? Individual attributes leading to exposure. *Computers in Human Behavior, 63*, 311–320. doi: 10.1016/j.chb.2016.05.033

Döring, N. (2014). Consensual sexting among adolescents: Risk prevention through abstinence education or safer sexting. *Cyberpsychology, 8*(1), 1–18. doi: 10.5817/CP2014-1-9

Dreβing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014). Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychology, Behavior, and Social Networking, 17*(2), 61–67. doi: 10.1089/cyber.2012.0231

Heirman, W., Walrave, M., Vandebosch, H., Wegge, D., Eggermont, S., & Pabian, S. (2016). Cyberbullying research in Belgium: An overview of generated insights and a critical assessment of the mediation of technology in a Web 2.0 world. In *Cyberbullying Across the Globe* (pp. 169–191). Berlin, Germany: Springer.

Jones, L.M., & Finkelhor, D. (2011). Increasing youth safety and responsible behavior online: Putting in place programs that work. Washington, DC: Family Online Safety Institute. Retrieved from http://scholars.unh.edu/ccrc/56/

Jones, L.M., Mitchell, K.J., & Finkelhor, D. (2012). Trends in youth Internet victimization: Findings from three youth Internet safety surveys 2000–2010. *Journal of Adolescent Health, 50*(2), 179–186. doi: 10.1016/j.jadohealth.2011.09.015

Lewis, S.P., & Knoll, A.K. (2015). Do it yourself: Examination of self-injury first aid tips on YouTube. *Cyberpsychology, Behavior, and Social Networking, 18*(5), 301–304. doi: 10.1089/cyber.2014.0407

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the Internet: The perspective of European children. Full Findings*. London, England: EU Kids Online. Retrieved from http://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/D4FullFindings.pdf

Livingstone, S., & Smith, P.K. (2014). Annual research review. Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of Child Psychology and Psychiatry, 55*(6), 635–654. doi: 10.1111/jcpp.12197

Mok, K., Ross, A.M., Jorm, A.F., & Pirkis, J. (2016). An analysis of the content and availability of information on suicide methods online. *Journal of Consumer Health on the Internet, 20*(1–2), 41–51. doi: 10.1080/15398285.2016.1167579

Näsi, M., Räsänen, P., Hawdon, J., Holkeri, E., & Oksanen, A. (2015). Exposure to online hate material and social trust among Finnish youth. *Information Technology & People, 28*(3), 607–622. doi: 10.1108/ITP-09-2014-0198

Olson, K.E., O'Brien, M.A., Rogers, W.A., & Charness, N. (2011). Diffusion of technology: Frequency of use for younger and older adults. *Ageing International, 36*(1), 123–145. doi: 10.1007%2Fs12126-010-9077-9

Tokunaga, R.S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior, 26*(3), 277–287. doi: 10.1016/j.chb.2009.11.014

Vandoninck, S., d'Haenens, L., & Roe, K. (2013). Online risks: Coping strategies of less resilient children and teenagers across Europe. *Journal of Children and Media, 7*(1), 60–78. doi: 10.1080/17482798.2012.739780

Wardle, H., Moody, A., Griffiths, M., Orford, J., & Volberg, R. (2011). Defining the online gambler and patterns of behaviour integration: Evidence from the British Gambling Prevalence Survey 2010. *International Gambling Studies, 11*(3), 339–356. doi: 10.1080/14459795.2011.628684

Willoughby, T., Adachi, P.J., & Good, M. (2012). A longitudinal study of the association between violent video game play and aggression among adolescents. *Developmental Psychology, 48*(4), 1044–1057. doi: 10.1037/a0026046

Youth Protection Roundtable. (2009). Youth protection roundtable toolkit. EC Safer Internet Programme. Retrieved from http://www.yprt.eu/yprt/content/sections/index.cfm/secid.11

Further reading

Livingstone, S.M., Haddon, L., & Gorzig, A. (2012). *Children, risk and safety on the Internet: Research and policy challenges in comparative perspective*. Bristol, England: Policy Press.

Valcke, M., De Wever, B., Van Keer, H., & Schellens, T. (2011). Long-term study of safe Internet use of young children. *Computers & Education, 57*(1), 1292–1305. doi: 10.1016/j.compedu.2011.01.010

Walrave, M., Ponnet, K., Vanderhoven, E., Haers, J., & Segaert, B. (Eds.). (2016). *Youth 2.0: Social media and adolescence. Connecting, sharing and empowering.* Berlin, Germany: Springer.

Lies De Kimpe is a PhD student at the Department of Communication Studies of the University of Antwerp (MIOS) and at Ghent University (imec-mict). Her main research interests are online risk behavior and cybercrime victimization.

Michel Walrave is a professor at the Department of Communication Studies of the University of Antwerp and Chairman of the research group MIOS (Media and ICT in Organisations and Society). His research is centered around online self-disclosure and privacy. He investigates adolescents' and adults' online disclosure of personal information to other individuals or companies, and related opportunities and risks.

Koen Ponnet a professor at Ghent University (imec-mict). His main research interests are the determinants of risk and problem behavior of adolescents and adults, both offline and online.

Joris Van Ouytsel is a researcher at the Department of Communication Studies of the University of Antwerp. His research focuses on cyberdating abuse and sexting. His work is supported by the Research Foundation—Flanders.

View publication stats