https://doi.org/10.15625/2615-8957/22210304

Literature review of research in the area of digital safety competency for school age students and the prospect of digital safety education in Vietnam

Do Quyen[1], Nguyen Hong Lien[2], Hoang Phuong Hanh[3]✉

[1] Email: : quyen@doquyen.org
University of Melbourne, Australia

[2] Email: liennh@vnies.edu.vn
Vietnam National Institute of Educational Sciences, Vietnam

[3] Email: hanhhp@vnies.edu.vn
Vietnam National Institute of Educational Sciences, Vietnam
University of Auckland, New Zealand

✉ Corresponding author

ABSTRACT: *This paper describes the literature review of research about digital safety competency of school students. Review and analysis of more than 90 research papers and government documents concerning the topic were conducted using various search engines as well as through access to printed legal and guiding documents of Vietnamese Government. . In the one hand, review of the literature shows the complexity of the DL concept, on the other hand, it proves the importance of activities to reinforce the knowledge and skills and reorientation or strengthening the attitudes regarding digital safety and positive use of the new media at home and in school. The presented results also provide opportunities to enrich the insights into the educational processes which take place in the family environment in the digital age. The prospect of digital safety education in Vietnam is also discussed in relation with the global progress.*

KEYWORDS:

➔ Received 18/12/2021 ➔ Revised manuscript received 25/03/2022 ➔ Published 30/09/2022.

1. Introduction

Digital safety for young people and the role of education in improving their digital safety capacity are becoming a global concern in the rapid development of information technology and media. Many international and regional organisations have developed theoretical frameworks for digital competence; however, only some of them aim at adolescents (UNESCO et al., 2016). While youths are increasingly exposed to digital devices and online networks, they are prone to many problems such as forms of child abuse (Gasser et al., n.d.; Tejedor-Calvo & Pulido-Rodríguez, 2012; Li, 2008; Cranmer, 2013), issues of information security (Berson et al., 2002), bullying in the digital space (Lampert & Donoso, 2012) or copyright violations authority (Kim & Epstein, 2017). From that context, one of the requirements for education systems is to educate young people on digital safety and increase awareness of the whole society on this issue.

This literature review is a systematic synthesis of research on the concept of digital safety, digital safety frameworks and digital education landscape in the world and Vietnam. From there, the article aims to raise the awareness of stakeholders on the issue of strengthening digital safety capacity for adolescent students.

2. Methods

The literature search was conducted through various databases: Academic Search Complete, Education Source, E-Journals, and ERIC. In addition, reference search sites were used to search for publications related to this issue such as: Google, Google Scholar, ResearchGate. Articles published in Vietnamese only were retrieved through NASATI (National Agency for Science and Technological Information), National University Data Center Hanoi, library portals of some universities and research institutes. In addition, the research team also searched for guiding documents, official documents, circulars of the Ministry of Education and Training and some schools' curriculum and programs on related issues.

Keywords used to search included: digital safety, digital safety frameworks and digital education landscape, digital safety for adolescents. 89 documents were used to conduct this literature review to answers the research questions:

- What is digital safety?

- What are the existing digital safety competency frameworks?

- How is digital safety education for children in some countries around the world implemented?

- How is the prospect of digital education in Vietnam?

3. Review of finding results

3.1. Definitions of digital safety

3.1.1. Safety in the digital world

Digital safety for teenagers is not a well-defined and framed concept. This phrase refers to a set of issues that may directly or indirectly relate to the welfare of children using digital media, and is not limited to certain means of access such as the Internet or the telephone, smartphones, but also includes the broader features of digital media (Tomczyk, 2020). It is difficult to give a complete and comprehensive definition of "safety" but the core of this phrase emphasises protecting oneself and those around them from dangerous risks when entering the digital world through digital devices (Tomczyk, 2020).

Although there is no universally agreed-upon concept of "digital security", most definitions indicate that it is not sufficient to consider only security operations on the network (Cerf, 2011). Digital security involves avoiding risks not only from the digital space but also from computer devices and Internet connections. Children today are accessing internet-connected digital devices earlier and more easily, but research on their exposure and understanding of the Internet is still very limited (Edwards et al., 2018; Livingstone, 2001). Research by O'Neill and Dinh's (2015) shows that mobile phone ownership has increased dramatically in Ireland with 40% of teenagers having a phone connected to the Internet. Common Sense Education's survey of 1,141 13- to 17-year-olds in the US shows the same trend with 9 out of 10 kids having smartphones, up 48% from 2012. Of which, 70% use social networks more than once a day, compared with 34% six years earlier (Rideout & Robb, 2018). In addition, along with the uncertain nature of the online environment, teenagers approached by criminals more easily through forms of child abuse through pictures, sexual messages, etc. pornography, or online bullying (Gasser et al., nd; Tejedor-Calvo & Pulido-Rodríguez, 2012; Li, 2008; Cranmer, 2013). Despite being aware of the risks, teenagers are more likely to experiment with social networking sites, where personal identities are not strictly controlled. That makes it easy for others to obtain and manipulate information, cause unforeseen dangers both online and in-person (Livingstone et al., 2012; Vanderhoven et al., 2014).

Bullying is one of the most common phenomena that adolescents face in the digital space (Lampert & Donoso, 2012). In most countries, 70 to 90% of children have experienced cyberbullying, depending on the severity, but none have witnessed the issue being discussed at school or received helpful help from the school (Lobe et al., 2012; Agatston et al., 2007). The negative effects of cyberbullying on victims include depression, low self-esteem, suicidal ideation and poor mental health, with the majority of victims seeking to avoid adult attention (Fleming et al., 2006; Martin & Rice, 2012; Li, 2010; Vanderhoven et al., 2016; Ybarra et al., 2006; Hanewald, 2008).

Digital piracy can have a huge negative impact on the digital device market but is not being considered as serious as direct piracy, leading to rampant illegal downloading by teenagers (Kim & Epstein, 2017). There is some research on digital piracy in the behavioral sciences and criminology, but very little focus on consumer education, particularly with adolescents (Kim & Epstein, 2017; Gunter et al. al., 2010). Kim and Epstein (2017) argue that it is unnecessary and ineffective to classify this piracy as an offense to punish youth; education regulations should be prioritized instead. This is in contrast to the results of research by Higgins & Makin (2004) and Al-Jabri & Abdul-Gader (1997), this behavior is common among university students due to poor self-control and friends dragging. A study by Gunter et al. (2010) on piracy among students in grades 8 to 11 found that 72.3% of teenagers have experienced piracy at least once in their lives. 16.1% of 8th graders and 25.0% of 11th graders infringe digital content on a daily basis (Gunter et al., 2010). In the latest research, the rise in digital piracy is attributed to the prevalence of software downloads, the exchange of infringing files between peers and lack of parental control (Tomczyk, 2019). The analysis shows that digital literacy education is a primary prevention measure because piracy is not uniform for all teenagers (Tomczyk, 2019).

When adolescents are subject to unsafe behavior, they are also at risk of leaking information online through insecure privacy settings (Berson et al., 2002). The information of famous underage stars is often more publicly available and there is a higher risk of leakage (Hofstra et al., 2016). Some other studies by Shin & Kang (2016) and Zarouali et al., (2017) add that there is no link between students' perceptions of privacy issues and disclosure behavior of the children. On the other hand, Agosto & Abbas (2017) asserts that teenagers are often more concerned with privacy issues than security. The majority of participants in this study considered themselves safe users, although a small number reported negative experiences such as identity theft or hacking (Agosto & Abbas, 2017). Children may be better aware of the risks of information leakage on social sites such as Facebook than adults (Christofides et al., 2012).

3.1.2. Digital safety competence concept and digital safety education

"Digital security" includes four competencies: awareness of rights and responsibilities, information and device and identity security, physical and mental health and resilience. In this domain of competence, children must be aware of their place and responsibilities in local and global contexts and understand concepts such as data, privacy, identity and intellectual property. Next, children must also recognise signs of bullying and harassment, make offensive and humiliating statements, as well as protect themselves, improve their physical and mental health when participating in the world. Finally, digital resilience refers to the ability to manage and cope with high-risk situations through dialogue or action within the framework of proper awareness and readiness (Le et al., 2019).

As mentioned above, safety is one of the most important aspects of concern in the 21st century as digital crime is increasing at a rapid rate and children are exposed to online content from the smaller age (Gasser et al., nd; Berson et al., 2002; Sonck et al., 2012; Livingstone & Smith, 2014; Xu et al., 2013).

In the field of education, digital safety education in the context of promoting teaching and learning activities is improving students' ability to handle situations as well as prevent and protect students from unsafe risks. The risks have influenced their mental and physical health, property and personal identity when participating in the digital world (Tomczyk, 2019a).

3.2. Developed frameworks

As cyberspace has always been deemed to present extensive "community, self-identity and social change" since its coinage in 1984. It has completely transformed all aspects of our lives, especially those of the iGeneration who may encounter enormous difficulties in the absence of digital technologies (Benedikt, 1993, p.401). The need to equip digital natives with sufficient skills and knowledge in a digital environment ultimately emerged, hence the introduction of a deluge of assessment frameworks worldwide. Therefore, it is vitally important for researchers to put each in context and construct a contextually appropriate evaluation system for relevant parties. As almost every country nowadays has their ICT curricula, we take into account those developed by international and regional organisations targeting preadolescents and adolescents specifically to make a comparative assessment with the one utilised in this study. Review suggests that most previous well-established frameworks focus on the context of developed Western nations, i.e. in Europe and North America. In contrast, research into this area with a strong focus on Asian participants has only recently been introduced (UNESCO Global Citizenship Education, UNESCO Digital Landscape Studies, etc.).

UNESCO et al. (2013) introduced one of the first well-known frameworks for media literacy assessment for a wide range of stakeholders on two tiers, namely country readiness and competencies. While it does not offer a detailed approach to competencies evaluation, it has grounded the foundation for later research regarding the spectrum and level of proficiency recommended for individuals and institutions in different environments. This report, though not touching specifically on any domains of digital citizenship, put an emphasis on many aspects of safety in cyberspace. On the *"understanding, assessment and evaluation of information and media"* level, individuals have to be able to *"assess, analyse, compare, articulate and apply initial criteria for assessment of the information retrieved and its sources, as well as evaluate media and information providers in society"* and *"evaluate and authenticate information and media content gathered and its sources and media and information providers in society"* (UNESCO et al., 2013, p.59). At the advanced level, they have to *"communicate information, media content and knowledge in an ethical, legal and effective manner using appropriate channels and tools"* (UNESCO et al., 2013, p.59,60). These traits are not exhaustive of the *"safety"* aspect of cyber competence and their order of priority is remarkably different from future research, yet the attention reserved for domain has demonstrated its utmost importance for a digital citizen.

In 2016, the DQ Institute, Organisation for Economic Co-operation and Development (OECD) and IEEE Standards created the Coalition for Digital Intelligence and pointed out a Digital Intelligence framework that encompasses eight domains (i.e. digital use, digital identity, digital rights, digital literacy, digital communication, digital safety, digital security and digital emotional intelligence) (DQ Institute, 2019). The European Commission Joint Research Centre (JRC) made public their Digital Competence Framework for Citizens (DigComp) as reports of DigComp 2.0 and DigComp 2.1 were finalised in 2017 (Carretero et al., 2017; Redecker et al., 2017). DigComp is composed of five dimensions: competence areas, competence descriptors and titles, proficiency levels, applicable knowledge, skills and attitudes and examples of use (Carretero et al., 2017). Similarly, the framework covers five areas where safety consists of four subdivisions ranging from health and well-being, personal devices, data and privacy to the environment (Carretero et al., 2017).

Other frameworks established by international organisations including "Building Digital Capabilities: The Six Elements Defined", *"OECD Skills Study, OECD Programme for the International Assessment of Adult Competencies (PIAAC)"*, "International computer and information literacy study: assessment framework", etc., while varying in terms of the number, range or difficulty level, all take into account areas such as information management, collaboration, communication, content and knowledge creation, ethics & responsibility, evaluation & problem solving and technical operations (JISC, n.d.; Organisation for Economic Co-operation and Development, 2016; Fraillon et al., 2013; Ferrari, n.d.). Researchers, therefore, have to notice the difference between cognition-based and application-orientated approaches to accordingly benchmark against either operational skillsets or tool-orientated behaviours.

With the risks of online environments for children, UNESCO Asia and Pacific Regional Bureau for Education (UNESCO Bangkok) launched the *"Fostering Digital Citizenship through Safe, Effective and Responsible Use of ICT"* project in 2016 (UNESCO Education sector & The Global Education 2030 Agenda, n.d.; Le et al., 2019). The project proposes a detailed framework of digital citizenship domains, proficiencies, and performance indicators including digital safety and resilience, based on Bronfenbrenner's bio-logical model which proposes four layers of impact on a child's cognitive development (Le et al., 2019). Based on critiques and feedback from previous frameworks, this framework is the convergence of strengths that previous works have developed while avoiding the over-complication and overlapping of subjects and domains. With Asia-Pacific being the most diverse region regarding ICT advancement, this framework is expected to afford a holistic picture of youngsters' ICT capabilities, especially in the domain of safety (UNESCO et al., 2016).

"Safety" domain of the framework

"Digital safety and resilience" consists of four competencies including awareness of rights and obligations, information and device security and reputation, health and well-being and resilience. Under this domain, children have to be aware of their position and responsibility within both a local and global context and knowledgeable about concepts such as data, privacy, reputation and intellectual property. The third division states that children have to recognise bullying, harassment, hate speech, unplug and addiction as well as protect themselves or improve their physical and psychological conditions when being online. Last, being digitally resilient demands that children take actions in the face of risky situations by communicating or taking instrumental and cognitive actions (Le et al., 2019).

As aforementioned, safety is one of the most vital aspects to be considered in the 21st century when cyber-criminals are rising at an unprecedented rate and children are being exposed to online content at an increasingly young age (Gasser et al., n.d.; Berson et al., 2002; Sonck et al., 2012; Livingstone & Smith, 2014).

3.3. Research that concerns digital safety education in the world

Developing digital safety capacity in schools

Children are exposed to digital devices and online networks from a very young age, so it is essential to have a comprehensive ICT program in school from pre-primary level (Edwards et al., 2018; Kritzinger, 2017; Moreno et al., 2013). The risks online have led to teaching using digital tools at times referred to as a *"risk model"* (instead of a *"promising model"*) (Tomczyk, 2020, p.482). Preschool teachers face a significant barrier when teaching children about cyber safety because many programs assume that children should be aware of the basic concepts of the Internet as connected devices (Edwards et al., 2018)). With peer-to-peer cooperative learning, older students' digital skills show improvement over time. Because young children are still online and each child has a different level of disaster recovery, it is risky to let digital skills develop naturally. Therefore, digital safety education from an early age is very important (Sonck et al., 2011; Vandoninck et al., 2012). Chaudron (2015) reported in a survey in Europe that children under 9 years of age using digital media devices are not aware of the Internet and what it means to be online. However, because the link between safety skills and literacy skills has been established, this situation can be improved by improving digital literacy skills (Sonck et al., 2011; Tran et al., 2011; Tran et al., 2011). al., 2020).

Asia Pacific is home to countries with large disparities in information technology capabilities and home to some of the lowest levels of digital systems on record (UNESCO et al., 2016). However, this does not mean that there are no gaps between IT programs in developed countries. In Canada, students have showed negative attitudes towards Information Technology subject because posters, videos or class are considered boring and unacceptable (Adorjan & Ricciardelli, 2019; Agosto & Abbas, 2017). Two-thirds of parents in the Netherlands report being unaware of their child's negative online experiences; and the Netherlands is also one of the few European countries that does not make digital security a compulsory subject in the curriculum (Sonck & de Haan, 2014; Valcke et al., 2007). Hope (2002), cited in Valcke et al. (2007), also points to the case of New Zealand and especially Flanders, Belgium, where the subject of Information Technology has been proposed since 2004 but has not yet been included as a formal subject in the school curriculum.

Because many digital safety awareness programs are merely memorization, students do not have the opportunity to apply concepts to real-life situations. From then, educators can take advantage of technology with the help of interactive tools to help make lessons more relevant and effective for young children

(Cone et al., 2017; Livingstone, 2001; Valcke et al., 2011; van Niekerk et al., 2013; Thierer, 2014; Wishart et al., 2007). For Information Technology, children should be taught through trial and error. However, integrating online opportunities or using productive tools should also be a priority, although focusing on the individual needs of each student is relatively difficult (Livingstone, 2001; Vanderhoven et al. al., 2016). Several studies have shown that school programs show no effect on student behavior but instead are short-term activities and efforts from teachers (Valcke et al., 2007; Valcke et al. , 2011; Vanderhoven et al., 2016; Wishart, 2004; Mishna et al., 2011). Because adults often assume social media is negative, programs should also focus on improving students' digital safety rather than separating the Internet from the beneficial opportunities that come with it (Agosto & Abbas, 2017). Therefore, it is important that educators address the issue through evidence-based studies and evaluations of their effectiveness in maximising students' potential without creating additional opportunities for maladaptive behaviors.

Livingstone & Smith (2014) suggested that the higher level of digital skills children gain, the more broadly they are likely to use the Internet, which can present more risks and opportunities alike (Vanderhoven et al., 2013). However, it should also be noted that school-based intervention programmes would not make any difference to students' behaviours, but rather, short-term tasks and engagements by teachers (Valcke et al., 2007; Valcke et al., 2011; Vanderhoven et al., 2016; Wishart, 2004; Mishna et al., 2011). Therefore, it is vitally important that educators fill in the gap with data-driven research and evaluate their effectiveness to maximise children's potentials while not creating more chances for unhealthy practices.

3.4. Prospect of digital education in Vietnam

In Vietnam, the International Computer Driving License (ICDL) of Europe and the International Computer and Internet Literacy Certification exam of Certiport (USA) was referred. Along with the actual requirements of the country, in 2014, the Ministry of Information and Communications issued the standard of skills in using IT together with the Circular No. 03/2014/TT-BTTTT dated 11/3/2014. The skill standard for using IT sets out the requirements for knowledge and skills for a general citizen, focusing on the target users for the job. The standard consists of 6 basic modules and 9 advanced modules including Basic IT Understanding, Basic Computer Use, Basic/Advanced Word Processing, Basic/Advanced Spreadsheet Usage, Use basic/advanced presentations, Basic Internet use, Database use, 2-D graphic design, Image editing, Web site editing, Information security, Use Use project planning software.

3.4.1. Curriculum

In the context of Vietnamese ICT curriculum, not much attention has been paid to the safety domain. Vietnamese students face enormous challenges in terms of infrastructure (one-to-one student per computer is no ensured), insufficient and obsolete resources, lack of professional training for teachers and lack of progress reporting from the government (Manh Tran & Stoilescu, 2016). In 2009, the Ministry of Education and Training proposed a framework to develop a digital literacy programme for Vietnamese students (Ministry of Education and Training, 2009; Ministry of Education and Training, 2017) but little improvement or change regarding digital skills training has been observed. Compared to the Australian ICT curriculum, Vietnam's current curriculum too heavily focuses on the software programming strand while lacks a balance of others such as social and ethical issues, hardware and Internet and network (Manh Tran & Stoilescu, 2016). This facilitates an urgent call for a comprehensive assessment and learning set for students of all ages where not only victims but also witnesses of online risks know how to handle dangerous situations (Nguyen et al., 2020; Cong et al., 2018).

In 2018, on the basis of inheriting the previous program and updating the program of advanced countries, the Ministry of Education and Training issued Circular No. 32/2018/TT-

BGDDT dated December 26, 2018 promulgating Chapter General education program and General education program in Informatics. Accordingly, the informatics program consists of 3 circuits (digital literacy, ICT application, computer science) divided into 7 topics with 5 requirements to achieve specific competencies.

The 7 core topics include Computers and knowledge society, Computer networks and the Internet, Organization of storage, search and exchange of information, Ethics, law and culture in the digital environment, Applications Computer applications, Computer-aided problem solving, Career with informatics.

The 5 requirements for capacity in order of increasing level are: Using and managing ICT facilities (Nla), Behaving appropriately in the digital environment (NLb), Problem solving with support of ICT (NLc), Application of ICT in learning and self-study (NLd), Cooperation in the NLe digital environment). Digital competence for high school students will be developed not only through Informatics but also through many other related subjects.

3.4.2. Digital competency framework

In principle, a digital competency framework needs to be built first, from which to develop curricula and teaching materials. However, for different objective and subjective reasons, different contexts may have to be implemented in parallel, this capacity framework must be developed. The Digital Competency Framework for students in particular must be part of the Digital Competency Framework for Citizens in general and must include specific characteristics for high school students.

This framework needs to meet a number of requirements as a basis for specific implementation, including (1) Inheriting and developing the basic advantages of the current computer science curriculum; (2) Exploiting the International Digital Competency Framework, it is necessary to select and apply appropriate contents for integration, towards the international level; (3) Ensure orientation of international integration, mutual recognition among countries in the region and the world; (4) Technology-neutral, the competency framework sets forth general requirements, regardless of any specific technology or product platform (hardware, software), regardless of closed or open-source; (5) The framework sets out requirements for both knowledge (understanding) and skills (practice); (6) Ensuring practicality, associated with the requirements of reality, between education in school and real life; (7) The content is easy to understand, easy to update and supplement, easy to locate each specific capacity; (8) Details by grade level, class block suitable for high school students (maybe the same topic but with different depth and depth).

In Vietnam's Information Technology program, the domain of digital security has not been really focused on. Vietnamese students face many barriers in terms of facilities (not guaranteeing a computer for each student), shortages and scarcity, inadequate and comprehensive professional training for teachers, and a lack of information on strategy and planning from the government (Manh Tran & Stoilescu, 2016). In 2009, the Ministry of Education and Training proposed a framework for developing digital literacy programs for Vietnamese students (Ministry of Education and Training, 2009; Ministry of Education and Training, 2017) but in reality there are no improvement in digital skills noted. Compared with Australia's Information Technology program, the current Vietnamese program focuses too deeply on software programming and lacks attention to ethical and social issues, hardware, and the Internet (Manh Tran & Stoilescu, 2016). This shows the urgent need to develop a comprehensive curriculum and assessment for students of all ages so that not only victims but also witnesses of online dangers know how to handle dangerous situations (Nguyen et al., 2020; Cong et al., 2018).

In the context of socio-economic development at home and abroad as well as innovations from the impact of information technology and digital communication, the Ministry of Education and Training has developed a draft *Digital Competency Framework for preschool children and school students (Khung năng lực số cho trẻ em mầm non – học sinh phổ thông)*, in which digital safety is identified as one of the seven domains of digital competence of Vietnamese students. Accordingly, the balance between online safety and the right to participate in the digital world as well as develop digital technology skills will be focused in the education to ensure students are ready on cognitive and social skills to protect themselves and their community when entering the digital world.

Although Vietnam would benefit from having an ICT curriculum implemented first and foremost, it is important that other countries' performances be taken into consideration. Since many cyber-security awareness trainings are rote and students do not have the opportunity to apply concepts into real-case scenarios, educators can take advantage of ICT with the support of interactive tools to enliven lessons, which has been proved to be more effective and fun for this age range (Cone et al., 2017; Livingstone, 2001; Valcke et al., 2011; van Niekerk et al., 2013; Thierer, 2014; Wishart et al., 2007). When it comes to ICT, children should be taught through trial and error. That being the case, the incorporation of opportunities to practice surfing the Internet or using production tools should be prioritised, though it is necessary to acknowledge that it is difficult to tend to individual needs of students (Livingstone, 2001; Vanderhoven et al., 2016).

4. Conclusions

This paper provides an overview of research about digital safety competency for students in the world. While proving to be an emergingly important realm, review of current research shows that there have not been much investigations on this issue. Current findings do suggest that digital safety competency seems to relate to various external factors such as learning time, parental control. In the one hand, review of the literature shows the complexity of the DL concept, on the other hand, it proves the importance of activities to reinforce the knowledge and skills and reorientation or strengthening the attitudes regarding digital safety and positive use of the new media at home and in school. The presented results also provide opportunities to enrich the insights into the educational processes which take place in the family environment in the digital age.

In the case of Vietnam, it can be seen that the issue of digital safety appears relatively novel and under-researched. The development of a suggested digital competency framework in which digital safety constitute a component of the competency is a promising starting point to raise awareness of this area. There needs to have further examination of the validation of this national framework, as a basis for curriculum development, training roadmap for teachers and education programmes for school age children.

Acknowledgement

This article is a part of the project *"Factors affecting digital safety of lower secondary students in Vietnam"* under Decision 222/VKHGDVN funded by Vietnam National Institute of Educational Sciences.

References

Adorjan, M., & Ricciardelli, R. (2019). Student perspectives towards school responses to cyber-risk and safety: The presumption of the prudent digital citizen. *Learning, Media and Technology*, *44*(4), 430–442. https://doi.org/10.1080/17439884.2019.1583671

Agatston, P. W., Kowalski, R., & Limber, S. (2007). Students' Perspectives on Cyber Bullying. *Journal of Adolescent Health*, *41*(6), S59–S60. https://doi.org/10.1016/j.jadohealth.2007.09.003

Agosto, D. E., & Abbas, J. (2017). "Don't be dumb—that's the rule I try to live by": A closer look at older teens' online privacy and safety attitudes. *New Media & Society*, *19*(3), 347–365. https://doi.org/10.1177/1461444815606121

Al-Jabri, I., & Abdul-Gader, A. (1997). Software copyright infringements: An exploratory study of the effects of individual and peer beliefs. *Omega*, *25*(3), 335–344. https://doi.org/10.1016/S0305-0483(96)00053-9

Anthonysamy, L., Koo, A. C., & Hew, S. H. (2020). Self-regulated learning strategies in higher education: Fostering digital literacy for sustainable lifelong learning. *Education and Information Technologies*, *25*(4), 2393–2414. https://doi.org/10.1007/s10639-020-10201-8

Barry, C., Lang, M., Linger, H., Paspallis, N., Raspopoulos, M., & Schneider, C. (Eds.). (2018). *Advances in Information Systems Development: Methods, Tools and Management* (1st ed. 2018). Springer International Publishing : Imprint: Springer. https://doi.org/10.1007/978-3-319-74817-7

Benedikt, M. (1993). Book Reviews: Cyberspace: First Steps Michael Benedikt (Ed.). *Social Science Computer Review*, *11*(3), 400–405. https://doi.org/10.1177/089443939301100317

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. *Journal of School Violence*, *1*(2), 51–71. https://doi.org/10.1300/J202v01n02_04

Bronfenbrenner, U., & Ceci, S. J. (1994). Nature-nuture reconceptualised in developmental perspective: A bioecological model. *Psychological Review*, *101*(4), 568–586. https://doi.org/10.1037/0033-295X.101.4.568

Carretero, S., Vuorikari, R., Punie, Y., European Commission, & Joint Research Centre. (2017). *DigComp 2.1 the digital competence framework for citizens with eight proficiency levels and examples of use.*

Cerf, V. G. (2011). Safety in Cyberspace. *Daedalus*, *140*(4), 59–69. https://doi.org/10.1162/DAED_a_00115

Christofides, E., Muise, A., & Desmarais, S. (2012). Hey Mom, What's on Your Facebook? Comparing Facebook Disclosure and Privacy in Adolescents and Adults. *Social Psychological and Personality Science*, *3*(1), 48–54. https://doi.org/10.1177/1948550611408619

Coaliation for digital intelligence. (n.d.). In *Introducing the Coaliation for digital intelligence*. Retrieved 30 August 2020, from https://www.coalitionfordigitalintelligence.org/

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, *26*(1), 63–72. https://doi.org/10.1016/j.cose.2006.10.005

Công, T. V., Ngọc, N. P. H., Dương, N. T., & Thắm, N. T. (2015). Chiến lược ứng phó của học sinh với bắt nạt trực tuyến. *VNU Journal of Science: Education Research; Vol 31 No 3*. https://js.vnu.edu.vn/ER/article/view/188

Cong, T. V., Ngoc, N. P. H., Weiss, B., Luot, N. V., & Dat, N. B. (2018). Definition and Characteristics of "Cyberbullying" among Vietnamese Students. *VNU Journal of Science: Education Research*, *34*(4). https://doi.org/10.25073/2588-1159/vnuer.4212

Cranmer, S. (2013). Listening to excluded young people's experiences of e-safety and risk. *Learning, Media and Technology*, *38*(1), 72–85. https://doi.org/10.1080/17439884.2012.658405

Development, O. for E. C. and (Ed.). (2016). *Skills matter: Further results from the survey of adult skills*. OECD.

Education on Online Safety in Schools in Europe. (2010).

Edwards, S., Nolan, A., Henderson, M., Mantilla, A., Plowman, L., & Skouteris, H. (2018). Young children's everyday concepts of the Internet: A platform for cyber-safety education in the early years: Young children's everyday concepts about the Internet. *British Journal of Educational Technology*, *49*(1), 45–55. https://doi.org/10.1111/bjet.12529

Ferrari, A. (n.d.). *Digital Competence in Practice: An Analysis of Frameworks*. Joint Research Centre of the European Commission.

Fleming, M. J., Greentree, S., Cocotti-Muller, D., Elias, K. A., & Morrison, S. (2006). Safety in Cyberspace: Adolescents' Safety and Exposure Online. *Youth & Society*, *38*(2), 135–154. https://doi.org/10.1177/0044118X06287858

Fraillon, J., Schulz, W., Ainley, J., & International Association for the Evaluation of Educational Achievement (IEA). (2013). *International computer and information literacy study: Assessment framework.*

Gasser, U., Maclay, C. M., & Jr, J. G. P. (n.d.). *Working Towards a Deeper Understanding of Digital Safety for Children and Young People in Developing Nations*. 33.

Gunter, W. D., Higgins, G. E., & Gealt, R. E. (2010). Pirating Youth: Examining the Correlates of Digital Music Piracy among Adolescents. *International Journal of Cyber Criminology*, *4*, 657–671.

Hanewald, R. (2008). Confronting the Pedagogical Challenge of Cyber Safety. *Australian Journal of Teacher Education*, *33*(3). https://doi.org/10.14221/ajte.2008v33n3.1

Higgins, G. E., & Makin, D. A. (2004). Self-Control, Deviant Peers, and Software Piracy. *Psychological Reports*, *95*(3), 921–931. https://doi.org/10.2466/pr0.95.3.921-931

Hofstra, B., Corten, R., & van Tubergen, F. (2016). Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Computers in Human Behavior*, *60*, 611–621. https://doi.org/10.1016/j.chb.2016.02.091

Huang, H., & Leung, L. (2009). Instant Messaging Addiction among Teenagers in China: Shyness, Alienation, and Academic Performance Decrement. *CyberPsychology & Behavior*, *12*(6), 675–679. https://doi.org/10.1089/cpb.2009.0060

Institute, D. Q. (2019). *DQ Global Standards Report 2019 Common Framework for Digital Literacy, Skills and Readiness*. https://www.dqinstitute.org/wp-content/uploads/2019/11/DQGlobalStandardsReport2019.pdf

Jackson, L. A., von Eye, A., Witt, E. A., Zhao, Y., & Fitzgerald, H. E. (2011). A longitudinal study of the effects of Internet use and videogame playing on academic performance and the roles of gender, race and income in these relationships. *Computers in Human Behavior*, *27*(1), 228–239. https://doi.org/10.1016/j.chb.2010.08.001

JISC. (n.d.). *Building digital capabilities: The six elements defined*. http://repository.jisc.ac.uk/6611/1/JFL0066F_DIGIGAP_MOD_IND_FRAME.PDF

Karamti, C. (2016). Measuring the Impact of ICTs on Academic Performance: Evidence From Higher

Education in Tunisia. *Journal of Research on Technology in Education*, *48*(4), 322–337. https://doi.org/10.1080/15391523.2016.1215176

Kim, J. E. (2015). Gender Differences in Problematic Online Behavior of Adolescent Users over Time. *Family and Environment Research*, *53*(6), 641–654. https://doi.org/10.6115/fer.2015.051

Kim, J. E., & Kim, J. (2015). Software Piracy among Korean Adolescents: Lessons from Panel Data. *Deviant Behavior*, *36*(9), 705–724. https://doi.org/10.1080/01639625.2014.977111

Kim, J.-E., & Epstein, N. B. (2017). Differential Longitudinal Associations of Juvenile Status and Delinquent Offenses with Incidence of Software Piracy Among Adolescent Consumers. 소비문화연구, *20*(3), 113–141. https://doi.org/10.17053/JCC.2017.20.3.007

Kritzinger, E. (2017). A Curriculum Approach to Improving Cyber Safety in South African Schools. In T.-C. Huang, R. Lau, Y.-M. Huang, M. Spaniol, & C.-H. Yuen (Eds.), *Emerging Technologies for Education* (Vol. 10676, pp. 95–105). Springer International Publishing. https://doi.org/10.1007/978-3-319-71084-6_11

Lampert, C., & Donoso, V. (2012). Bullying. In S. Livingstone, L. Haddon, & A. Görzig (Eds.), *Children, risk and safety on the Internet* (1st ed., pp. 141–150). Bristol University Press. https://doi.org/10.2307/j.ctt9qgt5z.16

Le, A.-V., Do, D.-L., Pham, D.-Q., Hoang, P.-H., Duong, T.-H., Nguyen, H.-N., Vuong, T.-T., Nguyen, H.-K. T., Ho, M.-T., La, V.-P., & Vuong, Q.-H. (2019). Exploration of Youth's Digital Competencies: A Dataset in the Educational Context of Vietnam. *Data*, *4*(2), 69. https://doi.org/10.3390/data4020069

Leung, L., & Lee, P. S. N. (2012). Impact of Internet Literacy, Internet Addiction Symptoms, and Internet Activities on Academic Performance. *Social Science Computer Review*, *30*(4), 403–418. https://doi.org/10.1177/0894439311435217

Li, Q. (2008). A cross-cultural comparison of adolescents' experience related to cyberbullying. *Educational Research*, *50*(3), 223–234. https://doi.org/10.1080/00131880802309333

Li, Q. (2010). Cyberbullying in High Schools: A Study of Students' Behaviors and Beliefs about This New Phenomenon. *Journal of Aggression, Maltreatment & Trauma*, *19*(4), 372–392. https://doi.org/10.1080/10926771003788979

Livingstone, S. (2001). *Online freedom and safety for children* (No. 3). LSE Research Online. http://eprints.lse.ac.uk/416/1/IPPR.pdf

Livingstone, S., Haddon, L., & Görzig, A. (Eds.). (2012). *Children, risk and safety on the Internet: Research and policy challenges in comparative perspective* (1st ed.). Bristol University Press. https://doi.org/10.2307/j.ctt9qgt5z

Livingstone, S., Haddon, L., Görzig, A., & Olafsson, K. (2012). *Risks and safety on the Internet: The perspective of European children: Full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries*. European Community Safer Internet Plus Programme. http://eprints.lse.ac.uk/33731/

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. https://doi.org/10.1111/jcpp.12197

Lobe, B., Livingstone, S., Olafsson, K., & Vodeb, H. (2012). *Cross-national comparison of risks and safety on the Internet: Initial analysis from the EU Kids Online survey of European children*. http://eprints.lse.ac.uk/39608/

Manh Tran, T., & Stoilescu, D. (2016). An Analysis of the Content, Policies and Assessment of ICT Curricula in the Final Years of Secondary Schooling in Australia and Vietnam: A Comparative Educational Study. *Journal of Information Technology Education: Research*, *15*, 049–073. https://doi.org/10.28945/2335

Martin, N., & Rice, J. (2012). Children's cyber-safety and protection in Australia: An analysis of community stakeholder views. *Crime Prevention and Community Safety*, *14*(3), 165–181. https://doi.org/10.1057/cpcs.2012.4

Maureen, I. Y., van der Meij, H., & de Jong, T. (2018). Supporting Literacy and Digital Literacy Development in Early Childhood Education Using Storytelling Activities. *International Journal of Early Childhood*, *50*(3), 371–389. https://doi.org/10.1007/s13158-018-0230-z

Mishna, F., Cook, C., Saini, M., Wu, M.-J., & MacFadden, R. (2011). Interventions to Prevent and Reduce Cyber Abuse of Youth: A Systematic Review. *Research on Social Work Practice*, *21*(1), 5–14. https://doi.org/10.1177/1049731509351988

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2008). Are blogs putting youth at risk for online sexual solicitation or harassment? *Child Abuse & Neglect*, *32*(2), 277–294. https://doi.org/10.1016/j.chiabu.2007.04.015

Moreno, M. A., Egan, K. G., Bare, K., Young, H. N., & Cox, E. D. (2013). Internet safety education for youth: Stakeholder perspectives. *BMC Public Health*, *13*(1), 543. https://doi.org/10.1186/1471-2458-13-543

Nguyen, H. T. L., Nakamura, K., Seino, K., & Vo, V. T. (2020). Relationships among cyberbullying, parental attitudes, self-harm and suicidal behavior among adolescents: Results from a school-based survey in Vietnam. *BMC Public Health*, *20*(1), 476. https://doi.org/10.1186/s12889-020-08500-3

Notten, N., & Nikken, P. (2016). Boys and girls taking risks online: A gendered perspective on social context and adolescents' risky online behavior.

New Media & Society, *18*(6), 966–988. https://doi.org/10.1177/1461444814552379

Nwosu, J. C., John, H. C., Izang, A. A., & Akorede, O. J. (2018). Assessment of information and communication technology (ICT) competence and literacy skills among undergraduates as a determinant factor of academic achievement. *Educational Research and Reviews*, *13*(15), 582–589. https://doi.org/10.5897/ERR2018.3539

Prior, D. D., Mazanov, J., Meacheam, D., Heaslip, G., & Hanson, J. (2016). Attitude, digital literacy and self efficacy: Flow-on effects for online learning behavior. *The Internet and Higher Education*, *29*, 91–97. https://doi.org/10.1016/j.iheduc.2016.01.001

Redecker, C., Punie, Y., European Commission, & Joint Research Centre. (2017). *European framework for the digital competence of educators DigCompEdu.*

Reid Chassiakos, Y. (Linda), Radesky, J., Christakis, D., Moreno, M. A., Cross, C., & COUNCIL ON COMMUNICATIONS AND MEDIA. (2016). Children and Adolescents and Digital Media. *Pediatrics*, *138*(5), e20162593. https://doi.org/10.1542/peds.2016-2593

Sadik, A. (2008). Digital storytelling: A meaningful technology-integrated approach for engaged student learning. *Educational Technology Research and Development*, *56*(4), 487–506. https://doi.org/10.1007/s11423-008-9091-8

sector, U. E., & Agenda, T. G. E. 2030. (n.d.). *Conference on Digital Citizenship Education in Asia-Pacific*. UNESCO Asia and Pacific Regional Bureau for Education. https://en.unesco.org/sites/default/files/dkap-conference-outcome-mar2017.pdf

Shin, W., & Kang, H. (2016). Adolescents' privacy concerns and information disclosure online: The role of parents and the Internet. *Computers in Human Behavior*, *54*, 114–123. https://doi.org/10.1016/j.chb.2015.07.062

Sonck, N., & de Haan, J. (2014). Safety by Literacy? Rethinking the Role of Digital Skills in Improving Online Safety. In S. van der Hof, B. van den Berg, & B. Schermer (Eds.), *Minding Minors Wandering the Web: Regulating Online Child Safety* (Vol. 24, pp. 89–104). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-005-3_5

Sonck, N., Kuiper, E., & de Haan, J. (2012). Digital skills in the context of media literacy. In S. Livingstone, L. Haddon, & A. Görzig (Eds.), *Children, risk and safety on the Internet* (1st ed., pp. 87–98). Bristol University Press. https://doi.org/10.2307/j.ctt9qgt5z.12

Sonck, N., Livingstone, S., Kuiper, E., & de Haan, J. (2011). *Digital literacy and safety skills*. EU Kids online, London School of Economics & Political Science.

Tejedor-Calvo, S., & Pulido-Rodríguez, C. M. (2012). Challenges and Risks of Internet Use by Children. How to Empower Minors? *Comunicar*, *20*(39), 65–72. https://doi.org/10.3916/C39-2012-02-06

Thierer, A. (2014). A Framework for Responding to Online Safety Risks. In S. van der Hof, B. van den Berg, & B. Schermer (Eds.), *Minding Minors Wandering the Web: Regulating Online Child Safety* (Vol. 24, pp. 39–66). T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-005-3_3

Tomczyk, Ł. (2019a). The Practice of Downloading copyrighted files among adolescents in Poland: Correlations between piracy and other risky and protective behaviours online and offline. *Technology in Society*, *58*, 101137. https://doi.org/10.1016/j.techsoc.2019.05.001

Tomczyk, Ł. (2019b). What Do Teachers Know About Digital Safety?. Computers in the Schools, 36(3), 167-187.

Tomczyk, Ł. (2020). Skills in the area of digital safety as a key component of digital literacy among teachers. *Education and Information Technologies*, *25*(1), 471–486. https://doi.org/10.1007/s10639-019-09980-6

Training, M. of E. and. (2009). QUYẾT ĐỊNH Phê duyệt Kế hoạch tổng thể phát triển nguồn nhân lực công nghệ thông tin đến năm 2015 và định hướng đến năm 2020. In *Ministry of Education and Training*. https://moet.gov.vn/giaoducquocdan/tang-cuong-ung-dung-cntt/Pages/chi-tiet-van-ban-chi-dao-dieu-hanh.aspx?ItemID=2054

Training, M. of E. and. (2017). *Document 4446 BGDĐT-CNTT*. https://moet.gov.vn/content/vanban/Lists/VBDH/Attachments/2263/4116-BGDDT-CNTT.pdf

Tran, T., Ho, M.-T., Pham, T.-H., Nguyen, M.-H., Nguyen, K.-L. P., Vuong, T.-T., Nguyen, T.-H. T., Nguyen, T.-D., Nguyen, T.-L., Khuc, Q., La, V.-P., & Vuong, Q.-H. (2020). How Digital Natives Learn and Thrive in the Digital Age: Evidence from an Emerging Economy. *Sustainability*, *12*(9), 3819. https://doi.org/10.3390/su12093819

Unesco, Communication and Information Sector, & UNESCO Institute for Statistics. (2013). *Global media and information literacy (MIL): Assessment framework : country readiness and competencies*.

Unesco, Unesco, & Asia and Pacific Regional Bureau for Education. (2016). *A policy review: Building digital citizenship in Asia-Pacific through safe, effective and responsible use of ICT.*

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. https://doi.org/10.1016/j.compedu.2011.01.010

Valcke, M., Schellens, T., Van Keer, H., & Gerarts, M. (2007). Primary school children's safe and unsafe use of the Internet at home and at school: An exploratory study. *Computers in Human Behavior*, *23*(6), 2838–2850. https://doi.org/10.1016/j.chb.2006.05.008

van Niekerk, J., Thomson, K.-L., & Reid, R. (2013). Cyber Safety for School Children. In R. C. Dodge & L. Futcher (Eds.), *Information Assurance and Security Education and Training* (pp. 103–112). Springer

Berlin Heidelberg.

Vanderhoven, E., Schellens, T., & Valcke, M. (2013). Exploring the Usefulness of School Education About Risks on Social Network Sites: A Survey Study. *Journal of Media Literacy Education*, *5*(1).

Vanderhoven, E., Schellens, T., & Valcke, M. (2014). Educating teens about the risks on social network sites. An intervention study in Secondary Education. *Comunicar*, *22*(43), 123–132. https://doi.org/10.3916/C43-2014-12

Vanderhoven, E., Schellens, T., & Valcke, M. (2016). Decreasing Risky Behavior on Social Network Sites: The Impact of Parental Involvement in Secondary Education Interventions. *The Journal of Primary Prevention*, *37*(3), 247–261. https://doi.org/10.1007/s10935-016-0420-0

Vanderhoven, E., Schellens, T., Vanderlinde, R., & Valcke, M. (2016). Developing educational materials about risks on social network sites: A design based research approach. *Educational Technology Research and Development*, *64*(3), 459–480. https://doi.org/10.1007/s11423-015-9415-4

Vandoninck, S., d'Haenens, L., & Segers, K. (2012). Coping and resilience: In S. Livingstone, L. Haddon, & A. Görzig (Eds.), *Children, risk and safety on the Internet* (1st ed., pp. 205–218). Bristol University Press. https://doi.org/10.2307/j.ctt9qgt5z.21

Wishart, J. (2004). Internet safety in emerging educational contexts. *Computers & Education*, *43*(1–2), 193–204. https://doi.org/10.1016/j.compedu.2003.12.013

Wishart, J. M., Oades, C. E., & Morris, M. (2007). Using online role play to teach internet safety awareness. *Computers & Education*, *48*(3), 460–473. https://doi.org/10.1016/j.compedu.2005.03.003

Xu, Z., Hu, Q., & Zhang, C. (2013). Why computer talents become computer hackers. *Communications of the ACM*, *56*(4), 64–74. https://doi.org/10.1145/2436256.2436272

Ybarra, M. L., Mitchell, K. J., Wolak, J., & Finkelhor, D. (2006). Examining Characteristics and Associated Distress Related to Internet Harassment: Findings From the Second Youth Internet Safety Survey. *PEDIATRICS*, *118*(4), e1169–e1177. https://doi.org/10.1542/peds.2006-0815

Yuksel-Arslan, P., Yildirim, S., & Robin, B. R. (2016). A phenomenological study: Teachers' experiences of using digital storytelling in early childhood education. *Educational Studies*, *42*(5), 427–445. https://doi.org/10.1080/03055698.2016.1195717

Zarouali, B., Ponnet, K., Walrave, M., & Poels, K. (2017). "Do you like cookies?" Adolescents' skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing. *Computers in Human Behavior*, *69*, 157–165. https://doi.org/10.1016/j.chb.2016.11.050