# Building A Wall Of Digital Safety: A Passport For Learning Without Borders

**Virgilio G. Medina, Jr.**
*Qatar National Library*

**Ross J. Todd, Ph.D.**
*Rutgers University*

## ABSTRACT

The shift in the development of the web environment from a static information repository to an interconnected network of systems, information, and users as consumers and producers has shifted the educative focus from accessing and engaging with authoritative information to a more holistic focus on both the intellectual and social wellbeing of young people as they participate and live in this digital environment. This paper examines one aspect of this digital wellbeing – that of digital safety. Given international concerns about children online, this research study sought to gather data from students themselves in relation to their conceptions and understanding of online safety, what it means to them to be safe in an online world, and the actions/strategies they use to ensure they are safe online. Some preliminary findings are presented and discussed.

***Keywords:*** **Internet Safety, Digital Safety, Digital Literacy, Unsafe Website, Information Literacy, Library Instruction**

## INTRODUCTION

The growth of Internet since its invention in 1993 has provided unprecedented opportunities for access to an open and borderless information world for learning, personal development and enrichment, and social networking. As of October 2016, the Indexed Web was estimated to contain at least 5.08 billion pages (Worldwidewebsize.com, n.d). In March 2017 it was estimated that across the globe there were 3,739,000,000 users, 49.6% of the world's population (Internet World Stats, n.d.). Access to this information world is often considered as a passport to 21st century learning, enabling students to transcend the traditional walls of libraries and classrooms, and to interact with diverse digital media and learners from different contexts and cultures.

Use of the digital environment has become deeply imbedded into the life of school-aged students. Accompanying the growth of this global interconnected information landscape has been considerable educational attention given to access to quality information, reading and literacy development in digital environments, engaging critically with diverse perspectives, and the developing essential of information and digital literacies to be an engaged, productive and creative learner. For example, Park (2009) argued that the benefits of internet further provided a number of essential roles in an educational context such as (1) storehouse of information, (2) communication without boundaries, (3) online interactive learning, (4) electronic/online research, (5) innovation in the new world, (6) improve interest in learning, (7) global education, and (8) information catalogues (as cited in Dogruer, Eyyam, & Menevis 2011, p. 606).

However, since that time, profound changes have taken place with increasing attention being given to not just the nature of the information and its educational use in this digital environment, but also to the context of the interaction with the information, and the outcomes and impacts of this interaction for the well being of individuals.

## PROFESSIONAL ACTION

Over the last 20 years, the school Library profession has vigorously embraced learning in a web-based environment, and the focus on the development of digital and information literacy has become a mainstream endeavor. The compendium of research summed up in *School Libraries Work!* (Scholastic, 2016) highlights the central role and impact of a digital information network accessible to everyone in any place and on any device as opposed to the traditional library website (a one-way stream of information), and the central focus on the development of digital capabilities. The New Jersey School library study: *One Common Goal: Student Learning. Report Of Findings And Recommendations Of The New Jersey School Library Survey Phase 2* (Todd, Gordon, & Lu, 2011) give evidence of this. The goal of this research was to examine the dynamics of a selected sample of effective school libraries in New Jersey to establish the key inputs (both library and school-wide inputs) that enabled the school libraries to thrive and contribute richly to the learning agendas of their particular schools. In this study, participating school libraries were chosen because their teaching faculty were engaged in a substantive number of team-based instructional collaborations with the school librarian. Data were collected through school-based focus groups that consisted of the school principal, school librarian, classroom teachers, curriculum leaders and specialist teachers. The findings show that considerable instructional attention was given to the development of digital literacy, and this involved a number of key competencies:

- Recognizing quality information in multiple modes and across multiple platforms
- Accessing quality information across diverse formats and platforms
- Participating in digital communication in collaborative and ethical ways to share ideas, work together and to produce knowledge
- Using sophisticated information technology tools to search, access, create and demonstrate knowledge in new ways
- Learning appropriate ethical approaches and behaviors in relation to use of digital technologies
- Understanding the dangers inherent in the use of complex information technologies and learning strategies to protect identity, personal information, and safety.

However, these findings also show a transition from (but not excluding) the educative focus on assessing the quality and authority of web based information and its analysis and synthesis to construct knowledge of a topic, and the ethics surrounding appropriate use of information (such as academic integrity), to an increasing focus on the operational context of digital learning and being present in a collaborative web-based environment. This includes a number of key aspects: the nature and operational context of the digital environment, the reality of multiple interactions, engagement with many people, and the social as well as the intellectual wellbeing of people connected together in digital environments. This is all about safety, self-protection, and self-preservation in digital environments.

In 2012, the Pew Research Center study titled *Millennials Will Benefit And Suffer Due To Their Hyperconnected Lives* (Anderson & Rainie, 2012) raised some considerable concerns about this operational context, particularly in terms of the perspective of some commentators that focused on the shallowness of intellectual engagement with this digital environment. Based on a random sample of 1,021 technology stakeholders and critics, the study sought to identify current attitudes among technology leaders about the potential future for networked communications in the digital environment – eliciting observations about the likely impact and influence of the Internet. The study offered some contrasting predictions, with some 55% agreeing that the future for the hyperconnected generation will be positive: positive affordances included public problem-solving through cooperative work; the effortless retrieval of data and information, and the development of new information processing skills. Negative impacts included the deployment of the Internet as the “external brain”, instant gratification, an operational setting for quick choices, lack of patience, shallow consumption of information, superficial engagement with understanding the nature and quality of information, rapid responses, and lack of awareness of the vulnerabilities of the networked digital context. As one respondent said: “there will be a premium on the skill of maintaining presence, of mindfulness, of awareness in the face of persistent and pervasive tool extensions and incursions into our lives” (Anderson & Rainie, 2012, p. 5). This early study raised some interesting dimensions of the operational context. Today, it is not just a context that centers on the constructive engagement with quality information and the construction and production of knowledge, it now also centers on the well-being of the individual in that environment, and the foundation of that can only happen when a culture of cybersecurity, security and digital safety is understood, enabled and enacted by all stakeholders and users. According to the National Cyber Security Alliance: “Realizing the full potential of our ever-evolving digital lives can only happen when a culture of cybersecurity and privacy is the foundation of: Free-flowing content, multiple methods and platforms for communication, trustworthy commerce, and widely available and highly reliable connectivity" (2017).

In 2010, distinguished scholar Renee Hobbs, Professor of Communication Studies at the Harrington School of Communication and Media at the University of Rhode Island, and Founder and Director of the Media Education Lab, released the *Digital and Media Literacy: A Plan of Action* (2010). In recognizing the heritage of instruction already in place since the development of the Internet, Hobbs referred to "digital and media Literacy" to encompass "the full range of cognitive, emotional and social competencies that includes the use of texts, tool and technologies; the sills of critical thinking and analysis; the practice of message composition and creativity; the ability to engage in reflection and ethical thinking, as well as active participation through teamwork and collaboration" (2010, p. 17). In elaborating the essential competencies, she called for deliberate actions and interventions to address risks associated with media and digital technology. She identified three types of risks associated with the use of mass media, popular culture and digital media:

- Content risks: this includes exposure to potentially harmful content, including violent, sexual, sexist, racist or hate material;
- Contact risks: this includes practices where people engage in harassment, cyber bullying and cyber stalking, talk with strangers, or violate privacy;
- Conduct risks: this includes lying or intentionally misinforming people, giving out personal information, illegal downloading, gambling, hacking and more. (Hobbs, 2010, p. 29)

In the swinging pendulum of risk and opportunity, fear, anxiety and optimism, protection, empowerment, transformation and social growth, Hobbs calls for an expansion of thinking and competency development that clearly addresses social wellbeing as a response to the technical context. Social wellbeing revolves round the sense to which people feel a sense of belonging, social inclusion, connected and supported in an environment. Social wellbeing is a growing area of multidisciplinary research. According to Dodge et al (2012): "In essence, stable wellbeing is when individuals have the psychological, social and physical resources they need to meet a particular psychological, social and/or physical challenge" (2012, p. 230). The international Organisation for Economic Co-operation and Development (OECD) had produced a data-driven Compendium of Well-Being Indicators (2011, p. 6) and identifies individual security and safety as essential components of social wellbeing. The sophisticated operational context of the Internet creates new dynamics for giving attention to social wellbeing, particularly in the wake of burgeoning growth of cybercrimes enabled by the development of the internet. In its Cybercrimes Report (2016) Cybersecurities Ventures, an international firm reporting and publishing cybercrimes, reports that the burgeoning growth of both the number and scale of cyber crimes and attacks has reached an unprecedented level. The nature of these include:

- System attacks, such as computer viruses (including worms and Trojan horses), hacking and denial of service attacks that shut down or misuse websites or computer networks, and electronic vandalism (such as defacing a website) or sabotage.
- Cyber theft, where computer access is used to steal money or other things of value from individuals and organizations. Forms of cyber theft include embezzlement, ATM and consumer fraud, theft of intellectual property, and theft of personal or financial data, file sharing and piracy, counterfeiting and forgery.
- Cyber security incidents, such as spyware, adware, hacking, phishing and other internet scam, spoofing, pinging, port scanning, using fake emails to get information form internet users, and theft of other information, regardless of whether the breach was successful.
- User target attacks, including misusing personal information (identity theft); invasion of privacy, harassment and cyberbullying (such as mean text messages or emails, rumors sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles, distributing child pornography, tracking and luring; spreading hate and inciting terrorism; grooming: making sexual advances to minors (Hackerpocalypse Cybercrime Report, 2016).

In some of the emerging discourses around social wellbeing, attention is now being given to the concept of digital wellbeing, defined as the "capacity to look after personal health, safety, relationships and work-life balance in digital settings' (JISC, n.d.). These include aspects such as:

- Using personal digital data for positive wellbeing benefits
- Using digital media to foster community actions and wellbeing
- Acting safely and responsibly in digital environments
- Managing digital stress, workload and distraction
- Acting with concern for the human and natural environment when using digital tools
- Balancing digital with real-world interactions appropriately.

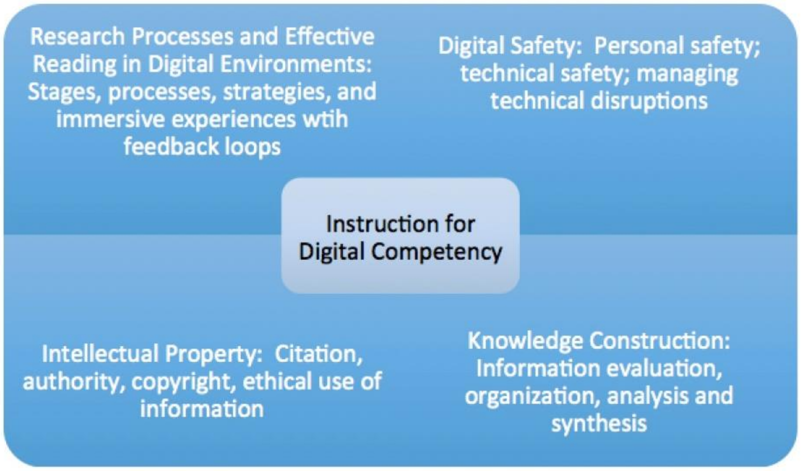
The increasing engagement of young people with the digital world brings the questions of social wellbeing and digital safety into prominence. Lenhart (2015) reports that 92% of teenagers significantly use the internet daily through a variety of devices. Reports such as those provided by the Pew Research Center and others build on earlier reports such as the Internet Society (2012) confirm teens' preference to be connected through social media platforms in which they can interact, chat, and communicate with their friends. It is a social world and a social reality for them, and it is in their pockets.

And to today, key questions center on what does it mean to be safe in an online world, what is the nature of online risks faced by children and teens, and what are the technical and educational solutions to ensure online safety as a passport to the global information world? This is increasingly important as they make intense use of mobile devices, the emergence of the 'selfie' culture, and their potential to create their own problematic contents.

Much of the scholarship on online safety comes from parents' perspectives, educators, and educational policy makers. Current research on internet safety has predominantly focused on cyberbullying, sexual solicitation and unwanted exposure to sexual content, the role of privacy, parent and community and parent involvement, and preservation of online privacy (Farrukh, Sadwick & Villasenor, 2014). For each of these, they provide an analysis of scholarly literature to identify definitions, prevalence, motives, prevention/coping strategies, and where more work I needed. In particular, they encourage more research on how the shift to the use of mobile devices impacts online safety, and the extent to which mobile technologies may be "deviance amplifying" (2014, p. 10). A substantive body of literature also exists on parental perception of children and teen's safety online, and the provision of strategies on parental and school-based guidance for online safety. Some notable examples include:

- National Parent Teacher Association (PTA) USA http://www.pta.org/parents/content.cfm?ItemNumber=3005
- Australian Government Department of Education and Training: Student Resilience and Wellbeing: Cybersafety in schools: https://www.education.gov.au/cybersafety-schools
- UK Council for Child Internet Safety (UKCCIS) https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

The qualitative research presented here seeks to understand the concept of online safety from the perspective of children and teens themselves, rather than from the authoritative stances of providers, which dominates the literature. It emerged out of an evidence-based practice project undertaken in a private school in Qatar in 2016 that sought to develop a digital literacy instructional strategy across the school, based on a survey questionnaire to 148 students in Grades 5 – 10 (Medina & Todd, 2016). Data were collected through a self-reported responses to 28 items using a modified and extended checklist, as well as open-ended questions, developed by the Open University UK titled "Being digital: Digital literacy skills checklist". The findings of this study identified five categories of help needed from the school library centering on building understanding and competencies in relation to: Intellectual property, Information organization, Information analysis and synthesis; and Digital reading, Research processes, and Internet safety. Accordingly, the evidence-based action plan presented here was developed. This has formed the basis for instructional interventions during the 2016-2017 year. The increasing attention being given to digital safety has prompted us to begin some exploratory work on this aspect.


Research Processes and Effective Reading in Digital Environments: Stages, processes, strategies, and immersive experiences wtih feedback loops
Digital Safety: Personal safety; technical safety; managing technical disruptions
Instruction for Digital Competency
Intellectual Property: Citation, authority, copyright, ethical use of information
Knowledge Construction: Information evaluation, organization, analysis and synthesis

From Digital Confidence to Digital Competence: An Evidence-Based Action Plan

*Figure 1: Evidence-Based Action Plan*

In order to understand more deeply the complex arena and dynamics of digital safety from the perspective of the students, the following study was undertaken.

## RESEARCH QUESTIONS

The research program of which this paper is an initial part seeks to understand how students define and describe online safety, what it means to them to be safe in an online world, how they recognize and determine, if at all, whether a website is safe or not, and what are the actions/strategies they use to ensure they are safe online. The goal of this research is to provide an evidence-based framework for the development of learning experiences, lesson plans and instructional interventions so students can learn to engage in safe digital practices, rather than simply being told by significant others. In particular, it wanted to build this instructional program on the various challenges encountered by students in their online activities and to provide assistance on how they can be equipped and become competent online users.

## BACKGROUND TO COUNTRY CONTEXT RESEARCH

We sought to collect the data in curricular-based school settings in two countries.
The schools have different curriculum structures and pedagogical approaches. Schools in the Philippines are administered and managed by the Department of Education, and classes are typically 40-60 in size, while the school in Qatar is an International Baccalaureate based curriculum, which is run by two partners between the Ministry of Education and Higher Education in Qatar and an educational management group in Spain. Classes in this school are typically 20-25 in size. Both of these countries have established digital safety programs, and the goals and approaches to each of these are overviewed here.

## QATAR'S CYBER SAFETY INITIATIVE

As of June 2016, Qatar is ranked second in the Middle East Countries in terms of number of internet users, with 94% population penetration (Internet Growth Statistics 1995 to 2017, 2017). It is believed that 98% of students from primary and secondary in this nation have access to the internet In addition, more than 90% of schools in Qatar confirm that students have internet connection at home as one of the education-related resources for their school homework or projects (Evaluation Institute, 2011). In Qatar, a cybersafety learning program called "Haseen" was initiated by the Ministry of Transport and Communication in collaboration with the Ministry of Education and Higher Education in 2015. This program promotes the importance of internet safety and augments security awareness among students from Grades 1 to 12 with much emphasis on becoming effective digital competent users in support of the

Qatar National Vision 2030 (Varghese, 2015). Its primary goal is to provide digital contents, educational activities, learning resources, references and other related materials that teachers are able to use and integrate in their classroom curricular-based instructions that enhance students' capacity to become effective, responsible and safe users in a global networked society.

Teachers and staff members of the school community can access the digital portal using the log-in credentials provided by the Ministry. The site is classified into different categories such as parents and teachers where users can download a wide range of approved learning resources, which have suitable corresponding grade levels and learning objectives. These resources can be integrated into classroom and library initiatives.

## PHILIPPINES DIGITAL INITIATIVE

To address the current issues on digital safety, particularly in relation to protecting children online, the Philippines Department of Education, in connection with Stairway Foundation, a non-profit organization, has published 'CyberSafe' project manuals that provide various lessons for classroom teachers tailored for Grades 5 to 6 and secondary students Grades 7 to 12 (Stairway Foundation, 2015). Advocating to ensure students' safety in an online world, this project seeks to assist students to determine different online risks and ensure online privacy involving cyber bullying, sexting, and child pornography. It is also stipulated through the Philippine Constitution Republic Act No. 9775 (known as "Anti-Child Pornography Act of 2009) which recognizes the right of every child to be protected in any forms of exploitation from physical as well as digital environments (Senate and House of Representatives of the Philippines in Congress, 2009).

A report based on a survey conducted by the Stairway foundation in the Philippines in 2013 documents considerable concerns regarding children's online behavior, aged from 7 to 16 years old. The study found that:

30% of the students were willing to communicate with strangers online;

20% spend their food allowance for internet access and add strangers in social media; 50% use public social media;

10% understand someone "who strips naked in front of a webcam in exchange for cellular load or money";

60% visit pornographic links via Social Media;

50% mention that never had any conversation about cybersafety;

40% "know someone who has been a victim of cyberbullying" (Stairway Foundation, 2013).

This survey identifies the needs to be addressed in the Philippines in helping users to become effective users in a digital networked hub. Based on these disturbing statistics the Cybersafe project in the Philippines has recommended a range of strategies for students to manage their online behaviors and be safe and protected. This set of strategies is significant in that it emerges directly from the findings of a study gathering data directly from the students.

| **Challenges** | **Useful tips** |
|---|---|
| Chatting with online strangers | • *Avoid chatting online with online strangers*<br>• *If you do, make sure you feel safe with the conversation*<br>• *Block the stranger if you feel comfortable* |
| Using food allowance for net access | • *Use your food allowance to buy healthful snacks and meals*<br>• *Ask your school to provide net access for students* |
| Having public social media accounts | • *Make your social media accounts private*<br>• *Use a blog or a second account to share general stuff safely without exposing your private information* |
| Adding strangers online in Social media | • *Avoid adding online strangers to your social media account*<br>• *Use the "Friends list" function on Facebook. Put all online strangers onto "restricted" list* |

| | |
|---|---|
| | • *Use the individual privacy setting available for each post* |
| Recognizing someone who strips naked in front of webcam in exchange for money or load | • *Block all persons who make such suggestions*<br>• *Don't be a victim of exhortation* or *further abuse*<br>• *Tell a trusted adult.* |
| Seeing pornographic links via Social Media | • *Don't click! You might get virus or malware*<br>• *Internationally clicking on illegal sites might get you in trouble with authorities* |
| No one has talked to them about cybersafety | • *Talk to children about online safety*<br>• *Educate yourself and stay aware of online risks*<br>• *Make sure children know you are a trusted adult.* |
| Knowing someone who has been a victim of cyberbullying | • *Do not respond to the cyberbully*<br>• *Take screen shot of the offending posts*<br>• *Block the sender*<br>• *Tell a trusted adult immediately* |

*Table 1: Strategies for Philippines Cybersafe Project*

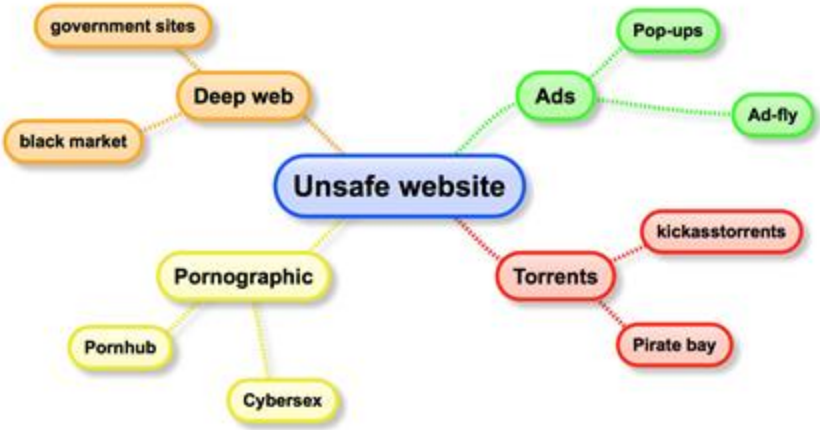
The Department of Education has continually been collaborating with their partnership non-profit organizations in developing and improving this manual to further support the development of curriculum, with a focus on digital safety in the Philippines. The strategies listed above were part of the framework for the digital literacy sessions discussed below.

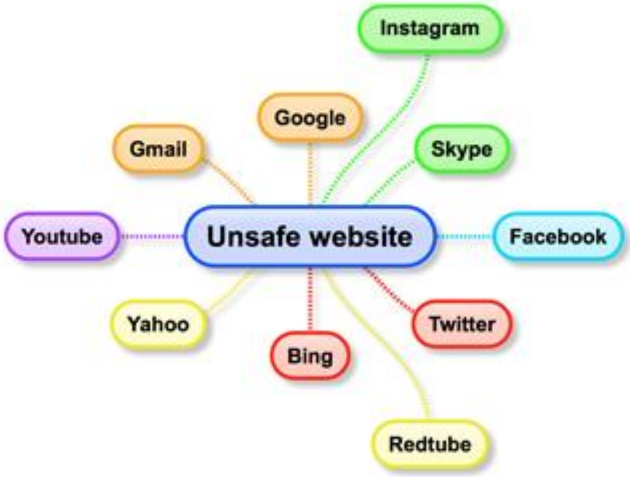
## METHODS

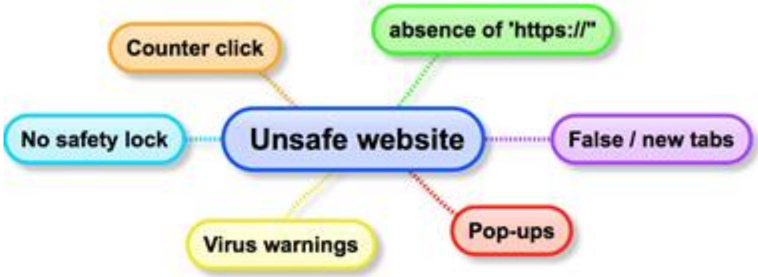
The sample of this study was students in Grades 5 to 10 from public and private schools in Qatar and Philippines, and data were collected in June-July 2016. Approximately 425 students participated in the study. The participating schools accepted a general invitation through city education division offices, allowing students to engage in a digital literacy instructional program. There were two general sessions conducted in one school in Qatar during regular library classes scheduled for students, and eight sessions in three public schools in the Philippines. The sessions were 40 minutes each (a regular class period). The sessions had a general theme of digital awareness and safety, and were very practical in nature, providing some practical strategies on how to become responsible information users as they engage in the online environment. Due to limited budget and lack of facilities especially in the Philippines, training opportunities are limited, and especially so in relation to training the students. The sessions were provided free of cost, and they were welcomed by participating teachers and school librarians. As an initial part of the sessions, students participated in groups where they had opportunity to brainstorm ideas about digital safety and unsafe websites. They were asked to record their output as a collective mind map, combining and recording similarities mentioned in their group discussions. Students participated enthusiastically in this exercise. A sample mind map was given prior the brainstorming activity in order to guide them with brainstorming their ideas. Groups were self-chosen, and varied in size – from 5 per group to 12 per group. A mind map is a diagram where participants identify concepts / key terms and organize them in some kind of structured, perhaps hierarchical way Students were provided with blank recording sheets, and were simply asked to create a map of the words that showed their ideas around unsafe websites.

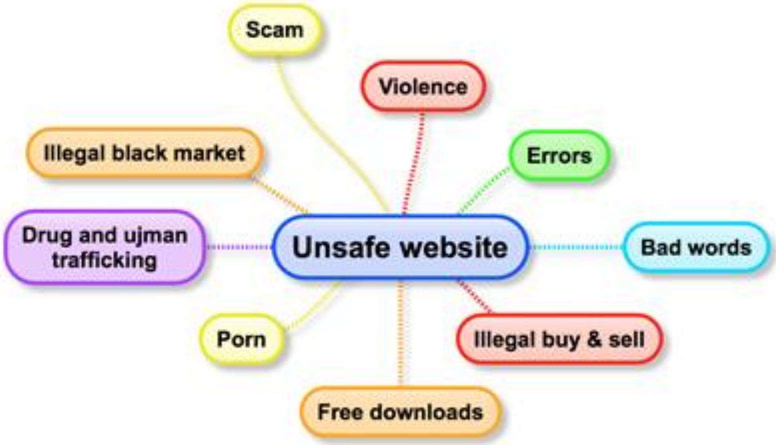
### Data Analysis and Some Preliminary Findings

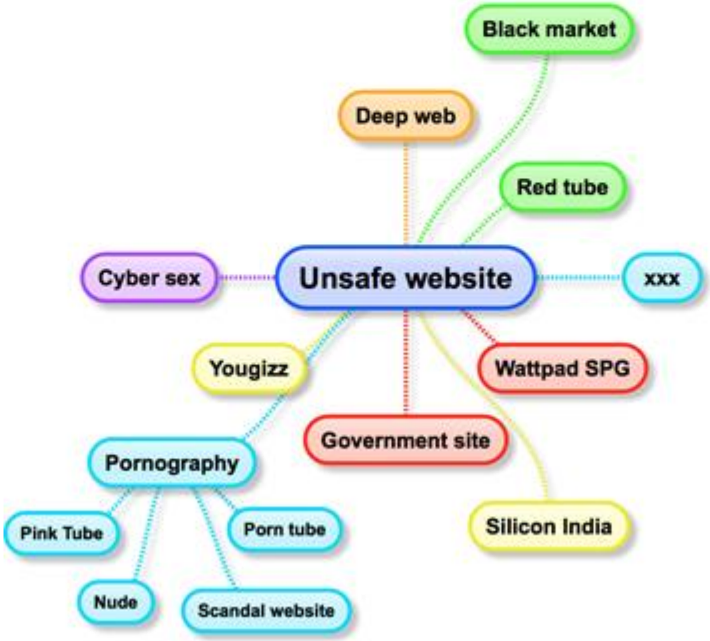
38 mind maps were collected as a result of the group activity. Some examples of mind maps created by students are shown here (transcribed from recording sheets):


government sites
Deep web
black market
Unsafe website
Pop-ups
Ads
Ad-fly
kickasstorrents
Torrents
Pirate bay
Pornographic
Pornhub
Cybersex


Instagram
Google
Gmail
Skype
Youtube
Unsafe website
Facebook
Yahoo
Twitter
Bing
Redtube


Counter click
absence of 'https://"
No safety lock
Unsafe website
False / new tabs
Virus warnings
Pop-ups


Scam
Violence
Illegal black market
Errors
Drug and ujman trafficking
Unsafe website
Bad words
Porn
Illegal buy & sell
Free downloads


Black market
Deep web
Red tube
Cyber sex
Unsafe website
xxx
Yougizz
Wattpad SPG
Government site
Pornography
Silicon India
Pink Tube
Porn tube
Nude
Scandal website

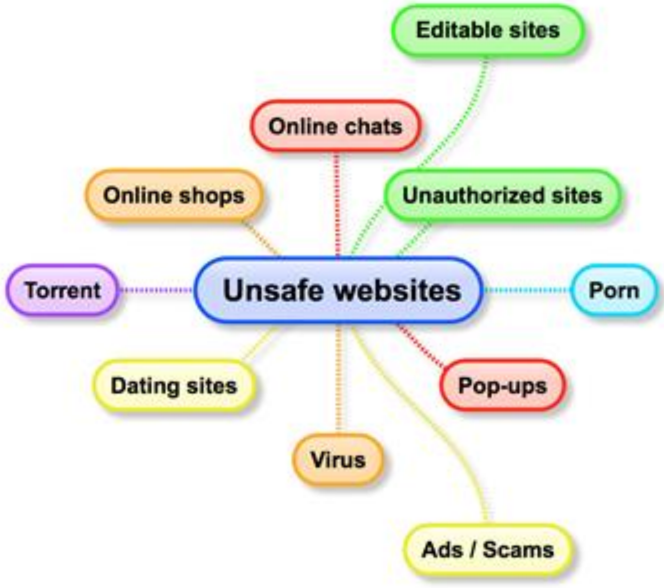


*Figure 2: Sample of Mind Maps Created by Students*

The words indicated on each mind map were listed, and grouped thematically. Overall, the participants listed 345 words / terms. A simple listing of these in alphabetical order reveals some patterns. 11 most frequently occurring words (or slight variations on a word such as "ads" and "advertisements") are shown in Table 2:

| **Term** | **Frequency** |
|---|---|
| Virus | 19 |
| Porn / pornographic / pornography | 16 |
| Pop-up /pop-ups, pop-up adds | 14 |
| Ads / Advertisements | 14 |
| Hack | 9 |
| Error | 9 |
| Fake / False | 8 |
| Malware | 7 |
| Scam / scams | 7 |
| Deep web | 7 |
| Bad (as in images, messages, videos and words) | 7 |

*Table 2: Frequency of Words / Terms*

These words comprise 30% of all the words / terms listed by the participants. The individual terms / words were then grouped into the six categories that represent the thematic summary of responses made by students:

Category 1: Sexual and Violent contents;
Category 2: Malware Pop-ups and Spam;
Category 3: Privacy and Security Issues;
Category 4: Technical errors/Virus/Auto Download;
Category 5: Social Media;

Category 6: Search Engines.

To interpret the data, the frequency of terms and its percentage value was identified in order to provide equal weight to each group responses. This is because some groups only wrote three terms while some have more than twenty terms. It could also be seen here that the groups' responses considerably range from 3 to 22 terms on the mind map. All the number of responses that each group wrote for each category were averaged, in order to find out which category generally describes what unsafe website are, based on students' knowledge and perception. By categorizing the words / terms and understanding the variation both in terms of terms and the breadth of students' knowledge, we wanted to support the larger goal of this study to make in-depth interpretations that helps educators to focus on strategic approaches and to design instructional digital literacy based on what they should know about digital safety.

| Group | Sexual and Violent contents | Percentage | Malware Pop-ups and Spam | Percentage | Privacy and Security Issues | Percentage | Technical errors/Viru s/Auto Download | Percentage | Social Media | Percentage | Search Engine (Reliable/ Unreliabl | Percentage | | Percentage |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | % | | % | 3 | % | 4 | % | 5 | % | 6 | % | Total | % |
| 1 | 0 | 0% | 3 | 50% | 2 | 33% | 1 | 17% | 0 | 0% | 0 | 0% | 6 | 100% |
| 2 | 1 | 17% | 1 | 17% | 3 | 50% | 1 | 17% | 0 | 0% | 0 | 0% | 6 | 100% |
| 3 | 5 | 63% | 0 | 0% | 2 | 25% | 1 | 13% | 0 | 0% | 0 | 0% | 8 | 100% |
| 4 | 1 | 10% | 2 | 20% | 1 | 10% | 6 | 60% | 0 | 0% | 0 | 0% | 10 | 100% |
| 5 | 1 | 17% | 3 | 50% | 1 | 17% | 1 | 17% | 0 | 0% | 0 | 0% | 6 | 100% |
| 6 | 0 | 0% | 1 | 9% | 1 | 9% | 1 | 9% | 4 | 36% | 4 | 36% | 11 | 100% |
| 7 | 1 | 17% | 1 | 17% | 1 | 17% | 3 | 50% | 0 | 0% | 0 | 0% | 6 | 100% |
| 8 | 13 | 93% | 0 | 0% | 0 | 0% | 0 | 0% | 1 | 7% | 0 | 0% | 14 | 100% |
| 9 | 6 | 67% | 1 | 11% | 0 | 0% | 2 | 22% | 0 | 0% | 0 | 0% | 9 | 100% |
| 10 | 1 | 13% | 4 | 50% | 2 | 25% | 1 | 13% | 0 | 0% | 0 | 0% | 8 | 100% |
| 11 | 0 | 0% | 4 | 50% | 2 | 25% | 2 | 25% | 0 | 0% | 0 | 0% | 8 | 100% |
| 12 | 2 | 25% | 1 | 13% | 0 | 0% | 3 | 38% | 0 | 0% | 2 | 25% | 8 | 100% |
| 13 | 1 | 10% | 0 | 0% | 0 | 0% | 0 | 0% | 7 | 70% | 2 | 20% | 10 | 100% |
| 14 | 0 | 0% | 0 | 0% | 0 | 0% | 0 | 0% | 6 | 75% | 2 | 25% | 8 | 100% |
| 15 | 1 | 13% | 2 | 25% | 0 | 0% | 4 | 50% | 1 | 13% | 0 | 0% | 8 | 100% |
| 16 | 0 | 0% | 1 | 20% | 1 | 20% | 3 | 60% | 0 | 0% | 0 | 0% | 5 | 100% |
| 17 | 3 | 33% | 2 | 22% | 1 | 11% | 3 | 33% | 0 | 0% | 0 | 0% | 9 | 100% |
| 18 | 6 | 50% | 3 | 25% | 0 | 0% | 3 | 25% | 0 | 0% | 0 | 0% | 12 | 100% |
| 19 | 2 | 15% | 2 | 15% | 4 | 31% | 3 | 23% | 0 | 0% | 2 | 15% | 13 | 100% |
| 20 | 1 | 11% | 1 | 11% | 1 | 11% | 6 | 67% | 0 | 0% | 0 | 0% | 9 | 100% |
| 21 | 5 | 71% | 0 | 0% | 0 | 0% | 1 | 14% | 0 | 0% | 1 | 14% | 7 | 100% |
| 22 | 2 | 20% | 1 | 10% | 0 | 0% | 0 | 0% | 6 | 60% | 1 | 10% | 10 | 100% |
| 23 | 0 | 0% | 0 | 0% | 1 | 33% | 2 | 67% | 0 | 0% | 0 | 0% | 3 | 100% |
| 24 | 0 | 0% | 2 | 25% | 1 | 13% | 5 | 63% | 0 | 0% | 0 | 0% | 8 | 100% |
| 25 | 2 | 50% | 0 | 0% | 2 | 50% | 0 | 0% | 0 | 0% | 0 | 0% | 4 | 100% |
| 26 | 0 | 0% | 0 | 0% | 1 | 14% | 1 | 14% | 3 | 43% | 2 | 29% | 7 | 100% |
| 27 | 0 | 0% | 1 | 17% | 0 | 0% | 1 | 17% | 1 | 17% | 3 | 50% | 6 | 100% |
| 28 | 3 | 25% | 4 | 33% | 0 | 0% | 2 | 17% | 3 | 25% | 0 | 0% | 12 | 100% |
| 29 | 0 | 0% | 0 | 0% | 0 | 0% | 6 | 100% | 0 | 0% | 0 | 0% | 6 | 100% |
| 30 | 1 | 9% | 2 | 18% | 2 | 18% | 3 | 27% | 3 | 27% | 0 | 0% | 11 | 100% |
| 31 | 2 | 18% | 3 | 27% | 1 | 9% | 3 | 27% | 2 | 18% | 0 | 0% | 11 | 100% |
| 32 | 3 | 38% | 2 | 25% | 1 | 13% | 1 | 13% | 0 | 0% | 1 | 13% | 8 | 100% |
| 33 | 1 | 8% | 1 | 8% | 1 | 8% | 3 | 23% | 4 | 31% | 3 | 23% | 13 | 100% |
| 34 | 1 | 8% | 0 | 0% | 2 | 17% | 3 | 25% | 1 | 8% | 5 | 42% | 12 | 100% |
| 35 | 3 | 21% | 5 | 36% | 2 | 14% | 3 | 21% | 1 | 7% | 0 | 0% | 14 | 100% |
| 36 | 1 | 10% | 3 | 30% | 1 | 10% | 2 | 20% | 2 | 20% | 1 | 10% | 10 | 100% |
| 37 | 2 | 29% | 1 | 14% | 1 | 14% | 2 | 29% | 1 | 14% | 0 | 0% | 7 | 100% |
| 38 | 5 | 23% | 11 | 50% | 1 | 5% | 3 | 14% | 2 | 9% | 0 | 0% | 22 | 100% |
| | 76 | 22% | 68 | 20% | 39 | 11% | 85 | 25% | 48 | 14% | 29 | 8% | 345 | 100% |

**Table 1: Summary of Categorization in the mind map activity**

### Category 1: Sexual and Violent Contents

76 words related to Sexual and Violent Contents were written by the students as they participated in the activity and described what unsafe websites were. For instance, some students listed down specific pornographic websites that online users are able to explore and navigate in an internet world. It can also be seen in the data that students were also aware of the restricted age limit that normally pops up in the screen when somebody attempts to access it. Lastly, the word "porn" seemed to be the most used description that students associated with unsafe website and links.

### Category 2: Malware Pop-ups and Spam

According to TechTerms, Malware, short term for "malicious software", is defined as "software programs designed to damage or do other unwanted actions on a computer system" (n.d.). In essence, this refers to the viruses, worms, Trojan horses, and spyware that could destroy or damage individual computer files if inflicted. In the data, there were 68 words relating to Malware Pop-ups and Spam. Students express that "pop advertisements" are usually seen in a variety number of websites that have been affected by computer viruses. Noteworthy is that some inputs included money matters such as "scamming promos'', "money offers", "fake promotions", "fake donations", "free giveaways" and "online buy and sell". These terms seemed to be prevalent terms /d phrases that students use to determine the quality of content and information on the website.

### Category 3: Privacy and Security Issues

"Private and Security Issues" is ranked as the second to the least in the categories with 39 frequent words. One group wrote "absence of https//" in their mind map as one way to recognize the safety of the website, which actually is an important tip that Mike Schema pointed out in his article entitled "Web Security: Why You Should Always Use HTTPS". He emphasized that "the encryption within HTTPS is intended to provide benefits like confidentiality, integrity and identity" (2011). Moreover, the word "Hack" was the most repetitive word amongst the students when talking about online privacy and security issues. Some words namely: "Unknown sites", ".com", "unauthorized site", "no safety lock" were also words that students presented in their mind maps.

### Category 4 Technical errors/Virus/Auto Download

Category 4 relating to Technical errors/Virus/Auto Download was ranked first on the list with the highest frequency of 85 words / terms or .25 mean among all the categories. It seems that most of the respondents associate unsafe websites based on technical glitches, errors viruses, and auto download files that they have encountered while being online and searching on the web. This is followed by Category 1 involving Sexual and Violent Contents with the frequency of 72 words or 0.22 mean. According to statistics provided by Guardchild's website, the largest group of internet porn users is children (Internet Statistics, n.d.). One notable point here is that Group 8's responses mainly center on two categories: Sexual and Violent contents, with 0.93 mean while 0.07 for the social media. Likewise, responses from Group 23 center only for two categories as shown above. Students from Group 29 provided a set of terms that merely tackle category 4.

### Category 5 Social Media

The mind maps showed that most of the popular social media sites such as Facebook, Twitter, Instagram, Skype, Youtube, and blogs were thought to be unsafe websites, with 48 responses from participants. The maps also indicate "dating sites" as a prevalent common term. In fact, Enough is Enough, a non-profit organization, published an article about the dangers of social media and its negative effects in the lives of teenagers (Van Ouytsel, J., Ponnet, K., & Walrave, M. (2014). This article also emphasizes the risks and privacy of choosing a public profile where everyone can view all the posts related to this account. In addition, "teens with public profiles are more likely to receive messages from strangers and be harassed by peers" according to the Teen Internet safety survey conducted by Cox Communications in 2007.

### Category 6: Search Engines

"Search engines" under category 6 takes the last place with having 29 responses. In these responses, students identified "Answer.com" "Google, "Yahoo" and "Wikipedia" as unsafe websites. During the discussion of the activity, one student explained that all the unsafe websites are searchable through these engines that anyone, regardless of age, can access it, which could be a good point of new insights for future studies. In an early study initiated by Edelman (2006), he identifies the safety of leading search engines using the “Siteadvisor’s automated web site rating: “MSN search results had the lowest percentage (3.9%) of dangerous sites while Ask search results had the highest percentage (6.1%). Google was in between (5.3%)”. Risks and dangers were also found on the common keywords that young people and novices use as they get online.

## Some Further Commentary

One of the key findings to date is that students do have a very specific knowledge about unsafe websites, at least shown in the general topical categorizations that have emerged. This is shown in the specificity of technical terms used, the reference to specific websites, and, in addition to these, the ways that access can be enabled, for example “auto-downloads”, “attachments”, and “fake surveys”.

What is strongly evident in the analysis of the words/ terms used is the specificity of technical terms that are already part of the vocabulary of the students, for example: Deep Web found in 7 of the group mind maps, which is reference to the invisible web content that is not indexed by standard search engines; and Torrent, a file that contains metadata about files that are to be distributed / shared, and which contains information that can initiate download of content such as pirated materials. In relation to the references to “torrents”, there was also one group’s reference to “Kick Ass Torrents”, the directory, abbreviated as KAT, which is a directory for torrent files. Other technical terms included “clickbait”, the term describing the web use of curiosity-driven thumbnails and headers that initiate further seeking; cracked games / cracking websites which appear to focus on password cracking tools; “Omegle”, a free chat site enabling people to talk via webcam to complete strangers without any signup required. The single reference to “Black” is possibly a reference to the Darknet, Deepnet, or the Hidden web.

Overall, there seems to be an awareness of some of the complex layers of the web, not just in terms of the layers surrounding the “dark web”, but even a mystery / urban legend, expressed by reference to “Marinas Web”.

There were also single references to many different individual terms. One group mentioned “Gumblar”**,** a malicious JavaScript trojan horse file that redirects a user's Google searches, and then installs rogue security software. There was also a single reference by one group to the website xnxx.com, and explicit pornography site with videos, live chat and connections, as well as two references to “youjizz”, another website that provides pornography videos, live sex and meeting opportunities. One entry “BEEG” is reference to another pornography site (beeg.com) providing similar content, as well as “niche” content (eg underage). There were three references to “Wattpad”, a diverse online story telling community with user-generated content submitted by participants. Of note here was the one reference to “Wattpad SPG”, the section of wattpad.com that is labeled as “My 'hot shots collection' stories”, short stories that contain graphical sex scenes. There was also mention of “Chi anime” a source of free anime movies, including an “erotica” category.

The data also present many curiosities. Two groups mention “government site(s)”, with one group connecting these to the “deep web”. What are the connections here, and the deeper understanding being presented here? At this point we do not know. Students also specify what we might consider standard, everyday sites and access modes, such as “Bing”, “Facebook”, “Google”, “Twitter” and “Gmail”. Why? We do not know. This is the starting point of the research agenda - and next is to unpack the conceptions captured in the mind maps to get to the heart of their understanding about unsafe websites, and indeed the practices they engage in to be safe.

We deliberately did not provide the students with any definition of what an “unsafe website” was. We wanted the conceptions to emerge from the data. However, the words / terms represented in the mind maps and in the categorizations do tell only part of the story. Predominantly, the terms / words used make reference to aspects of access, technical structures, and potential for technical harm (i.e. to the computer) and far fewer references to sites where self is potentially harmed (although there were some). Students seem to know the technical, but not the personal dimensions around unsafe websites. From the perspective of the data collected here, the students do not see themselves as part of the “unsafe”. It did not seem to register to them that they are part of the digital equation of safety. There was no reference to their interactions with strangers, their role in creating their own privacy boundaries, cyberbullying indicators, and managing offensive posts, interactions and images. In essence, “unsafe” was predominantly seen as a system problem, of which there seems to be some level of awareness, rather than a personal – social – interaction problem. One of the most predominant themes that comes up in the authority-driven conceptions (such as by parent groups, educational associations and teacher groups) is the notion of safety built around understanding the active role of self in the digital environment) and identifying the indicators of interactions that signal unsafe. There was only one reference to “fake Identity” and no reference to “strangers”.

The absence of the “stranger danger” set of indicators is clearly worthy of further deep investigation. In the context of the proliferation of mobile devices, understanding the extent to which students may be using a range of apps to connect with people, and their capacity to establish whether this is friend or foe is an important direction. While it is easy to stress to young people not to interact with strangers, there is need to understand how students make this judgment and determination, if at all, and whether they see that there is some kind of risk – digital danger. Given the centrality of social media, there was no sense of the staying power of social media – the ‘forever potential’ of social media and the capacity of social media content to be archived, accessed and used in positive and negative ways by colleges, potential employers and even insurance and medical agencies.

## CONCLUSION

### The Continuing Story

With the preliminary findings and commentary presented in this paper, the longer term goal is to consider how these findings impact professional practice and instructional interventions, not only for school libraries but for all libraries that are committed to addressing the needs of 21st century skills as well as helping students in becoming responsible citizen of information users in an online world. Safe access to quality information, and access and use of information that protects both self and systems is seen as a passport to a global learning environment – learning without walls, learning without the sense of personal or system safety being compromised. While the findings here from 425 students who have recorded their ideas in relation to unsafe website present some knowledge of the safe / unsafe landscape of the web, the perception of unsafe websites as being part of the technical environment, rather than actions on their part, raises some key questions around the nature of instruction and educational intervention. How do we educate young people to ensure their internet safety as they engage in borderless digital learning? What does it take? How do we build their understanding about the dangers and risks that could significantly bring negative consequences to their learning growth in ways that empower them to take action – to protect both self and system. This is the question we hope to follow through at the IASL conference. In the digital “selfie” culture, the protection of self by self emerges as a significant challenge.

## REFERENCES

Anderson, J. & Rainie, L. (2012). Millennials will benefit and suffer due to their hyperconnected lives. Retrieved June 11, 2017 from http://www.pewinternet.org/2012/02/29/millennials-will-benefit-and-suffer-due-to-their-hyperconnected-lives/

Cox Communications. (2007). Cox Communications Teen Internet Safety Survey, Wave II – in partnership with the National Center for Missing & Exploited Children® (NCMEC) and John Walsh (Fielded Among Young People Aged 13-17) (1st ed.). Retrieved from http://www.cox.com/wcm/en/aboutus/datasheet/takecharge/archives/2007-teen-survey.pdf?campcode=takecharge-archive-link_2007-survey_0511

Hackerpocalypse Cybercrime report. (2016, August 12). Retrieved June 14, 2017 from http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Dodge, R., Daly, A. P., Huyton, J., & Sanders, L. D. (2012). The challenge of defining wellbeing. *International Journal of Wellbeing, 2*(3), 222-235.

Dogruer, N., Eyyam, R., & Menevis, I. (2011). The use of the internet for educational purposes. Procedia. *Social and Behavioral Sciences, 28*, 606–611.

Edelman, B. (2006). The safety of internet search engines. Retrieved June 11, 2017 from http://www.siteadvisor.com/studies/search_safety_may2006.html

Evaluation Institute. (2011). Schools and Schooling in Qatar: A Statistical Overview of Aspects of Schools and School in Qatar (1st ed.). Retrieved from http://www.edu.gov.qa/Statistical%20Report/2010-2011.pdf

Farrukh, A., Sadwick, R., & Villasenor, J. (2014). Youth internet safety: Risks, responses, and research recommendations. Center for Technology Innovation at Brookings. Retrieved June 14, 2017 from http://www. brookings. edu/~/media/research/files/papers/2014/10/21-youth-internetsafety-farrukh-sadwick-villasenor/youth-internet-safety_v07. pdf.

Hobbs, R. (2010). *Digital and media literacy: A plan of action*. Washington, DC: The Aspen Institute.

Internet growth statistics 1995 to 2017 - the global village online. (n.d.). Retrieved June 11, 2017, from http://www.internetworldstats.com/emarketing.htm

Internet Statistics. (n.d.). GuardChild: Protecting children in the digital age. Retrieved June 11, 2017 from https://www.guardchild.com/statistics/

Internet Society. (2017). Children and the internet. Retrieved from https://www.internetsociety.org/sites/default/files/bp-childrenandtheinternet-20129017-en.pdf

JISC. (n.d.). Building Digital Capability. Retrieved June 11, 2017 from https://www.jisc.ac.uk/rd/projects/building-digital-capability

Lenhart, A. (2015). Teens, social media & technology overview 2015. Retrieved June 11, 2017 from http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/

Malware definition. (n.d.). Retrieved June 11, 2017 from https://techterms.com/definition/malware

Medina, V G. & Todd, R. J. (2016). Empowering students for a digital world: Global concerns, local school evidence and strategic actions. research forum. *Proceedings of the 45nd International Conference incorporating the 20th International Forum on Research in School Librarianship.* Meiji University, Tokyo, Japan, August 22-26.

National Cyber Security Alliance. (2017). About the National Cyber Security Alliance StaySafeOnline.org. Retrieved 11 June 2017 from https://staysafeonline.org/about-us/

OECD. (2011) OECD better life initiative. Compendium of OECD well-being indicators. Paris, France: Organization of Economic Co-Operation and Development.

Pierce, D. (2015, September 24). The 9 essential elements of digital citizenship. Retrieved June 11, 2017 from https://www.eschoolnews.com/2015/09/24/digital-citizenship-244/

Royal Society for Public Health. (2017). Instagram ranked worst for young people's mental health. Retrieved June 11, 2017 from http://www.rsph.org.uk/about-us/news/instagram-ranked-worst-for-young-people-s-mental-health.html

Schema, M. (n.d.). Web security: Why you should always use HTTPS. Retrieved June 11, 2017 from http://mashable.com/2011/05/31/https-web-security/#GAFhsHvC15qK

Scholastic Library Publishing. (2015). School libraries work! A compendium of research supporting the effectiveness of school libraries, 2016 edition. Retrieved June 11, 2017 from http://www.scholastic.com.au/assets/pdfs/schoollibraries-work.pdf

Senate and House of Representatives of the Philippines. (n.d.). Republic Act 9775 | Philippine Commission on Women. Retrieved June 11, 2017,from http://pcw.gov.ph/law/republic-act-9775

Stairway Foundation. (n.d.). About - Cybersafe. Retrieved June 11, 2017 from https://www.cybersafe.asia/about/

Survey – Cybersafe. (2013). Retrieved June 11, 201, from https://www.cybersafe.asia/survey/

Todd, R.J., Gordon, C.A., & Lu, Y.L. (2011). Report of findings and recommendations of the New Jersey School Library Survey Phase 2. Princeton, NJ: School of Communication and Information Rutgers, The State University of New Jersey. Retrieved from http://cissl.rutgers.edu/images/stories/docs/njasl_phase%20_2_final.pdf

Van Ouytsel, J., Ponnet, K., & Walrave, M. (2014). The associations between adolescents' consumption of pornography and music videos and their sexting behavior. *Cyberpsychology, Behavior, and Social Networking, 17*(12), 772–778.

Varghese, J. (2015, Feb. 11). Over 40% schoolchildren post personal details on net. Retrieved June 11, 2017 from http://www.gulf-times.com/story/426731/Over-40-schoolchildren-post-personal-details-on-Net

WorldWideWebSize.com. (n.d.). The size of the world wide web (the internet). Retrieved June 11, 2017 from http://www.worldwidewebsize.com/

Acknowledgement: The authors acknowledge the support given by Kenneth Gabriel Juquiana and Nikki Mabilin, for providing insights and for undertaking statistical analyses of the data.