Jurnal Iqra' Kajian Ilmu Pendidikan

E-ISSN: 2548-7892 & P-ISSN: 2527-4449

Volume 7, Number 1, June 2022

Digital Safety During Online Learning: What We Do to Protect Our Students?

Dewanto Muhammad Zulqadri[1], Ali Mustadi[2], Heri Retnawati[3]
[1,2,3] *Universitas Negeri Yogyakarta, Indonesia*

Correspondent Author dewantomuhammad.2019@student.uny.ac.id

ARTICLE INFO
Article history:
Received
August 14, 2021
Revised
April 21, 2022
Accepted
May 19, 2022

ABSTRACT

The article aims to uncover security risks that may occur during online learning, as well as preventive measures that can be taken to avoid these threats. This study uses a combination of two methods, namely, web mining and literature review. From the results of web mining, it is found that the website articles have not provided much explanation about efforts to protect against threats on the internet, from the results of the literature review the researchers revealed that several threats that can occur on the internet, namely phishing, scamming, fraud, cyberbullying, viruses, privacy and personal data issues, and obscene or pornographic content. This study also provides three important steps in protecting children from internet threats during online learning, including assistance in accessing internet content, education about internet safety and personal data protection, as well as an introduction to Digital Citizenship and ethics in cyberspace.

Keywords: *Digital Safety, Online Learning Safety, Digital Citizenship*

How to cite Zulqadri, D., Mustadi, A., & Retnawati, H.,. (2022). Digital Safety During Online Learning: What We Do To Protect Our Students?, *Jurnal Iqra' : Kajian Ilmu Pendidikan, 7*(1). 178-191. https://doi.org/10.25217/ji.v7i1.1746

Journal Homepage http://journal.iaimnumetrolampung.ac.id/index.php/ji/

INTRODUCTION

The development of science and technology today, increasingly encourages reform efforts in the use of technological results in the learning process. Media as a part of technological renewal and very influential in the learning process. Information and Communication Technology is expected to be one of the media in carrying out the mandate of PP No. 19 of 2005 concerning National Education Standards Article 1 Paragraph 8, regarding the standards of facilities and infrastructure required, including the use of technology, information and communication. One of the widely used learning media is the internet, coupled with the COVID-19 pandemic situation.

Covid-19 has had a major impact on education, as a result of the closure of universities and schools, teachers and students, must quickly adapt to distance learning (Carrillo & Flores 2020:1) many educational institutions reacted quickly by moving traditional classes into the network (Carrillo & Flores 2020:1) Lei & So, 2020:1). Education in dealing with the outbreak, the novel coronavirus covid-19 requires critical learning and adapting to the government's response to the outbreak (Lee, Yeo & Na, 2020:1). Leaving aside the COVID-19 pandemic, looking at the data from Hootsuite We Are Social Indonesia Report 2021, internet users in Indonesia are already quite high,

namely 202.6 million people or 73.7% of the population with an average time spent on the Internet of 8 hours 52 minutes (Hootsuite We Are Social 2021). In addition, a survey conducted by the Association of Indonesian Internet Service Providers (APJII), stated that children aged 10-14 years were also starting to actively use the internet (APJII 2020). From this statistical data, it can be concluded that digital threats are important, especially for school-age children who use the internet as a learning medium. Of the many internet users in Indonesia, a new problem arises, namely the issue of digital security.

Digital security incidents started popping up since distance learning. Russian computer security company Kaspersky reports that from January 2020 to June 2020, attacks using DDoS or Distributed Denial of Services against online educational resources increased by 350% compared to 2019 (Kaspersky, 2020), DDoS attempts were made to disable system to be inaccessible. DDoS is a cyber attack, in which attackers try to make machines or network resources unavailable to legitimate clients, by temporarily or permanently interfering with host services connected to the Internet (Kaur, Bhandari & Behal, 2019). The report also mentions that 168,550 Kaspersky users are experiencing an increasing number of various threats distributed under the guise of popular online learning/video conferencing platforms such as, google classroom, moodle, coursera and so on. In addition, teachers are also faced with the increasing threat of phishing (Kaspersky, 2020).

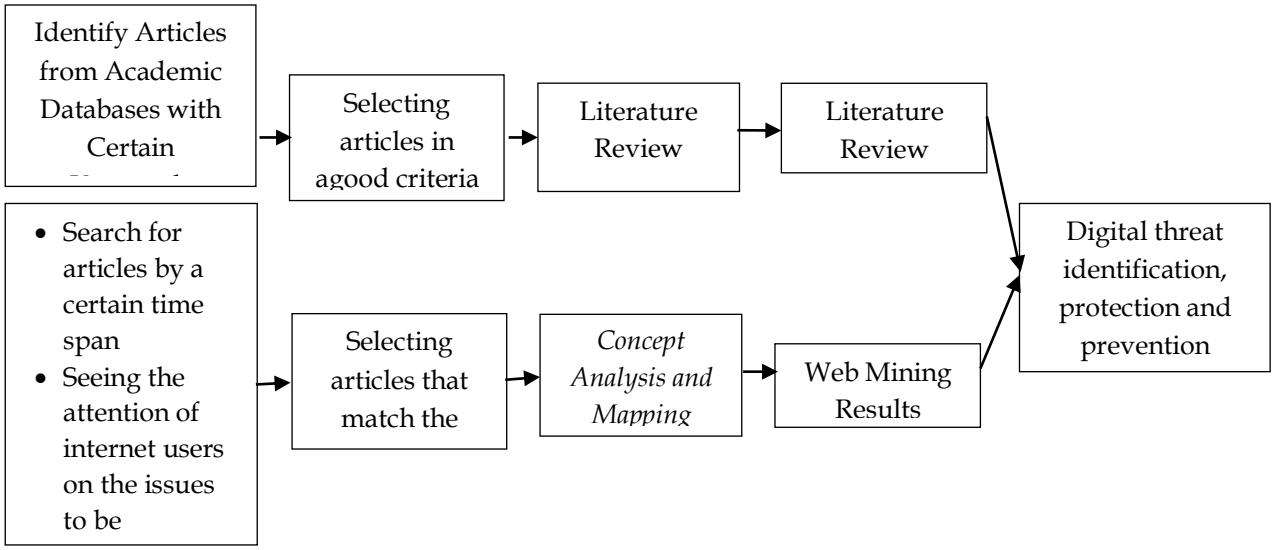
Awareness of personal data protection also needs to be built, in order to avoid the threat of phishing and theft of personal data. An attempted theft case occurred at the end of 2020, the Yogyakarta State University academic community received a phishing email pretending to be a university ICT administrator and asking for personal information such as email, email password, and date of birth, accompanied by threats of deactivating the account if they did not submit the data. within 72 hours. The ICT administrator of Yogyakarta State University responded quickly and gave an explanation of the phishing email and asked not to respond.

Internet Safety and Internet Threats are not new topics in various studies. However, further studies on this matter are still relatively few. Research conducted by Soldatova & Rasskazova states that the most common threats to children and adolescents in using the internet are fraud, identity theft, negative content, matters related to sexuality and also attempts to meet with acquaintances on the internet (Soldatova). & Rasskazova, 2016). In this study, we try to summarize some of the internet threats that often occur during distance learning, as well as provide a description of preventive and protective measures that can be taken and provide resources that can be used from an educational perspective, based on discussions and suggestions from researchers.

METHOD

This study uses two types of approaches to identify internet threats and the efforts made to avoid these threats. The first is Literature Review, this method is done by searching for articles in academic sources such as Web of Science, Google Scholar, Taylor and Francis Online, Springer Link, JSTOR, AACE Digital Library with the keyword: "Online Learning", "e-learning", " distance learning", "security", "safety", and "risk". The second is web mining, we search for articles made by writers on blogs or websites that are public and accessible to everyone, to retrieve information about online learning safety and security.

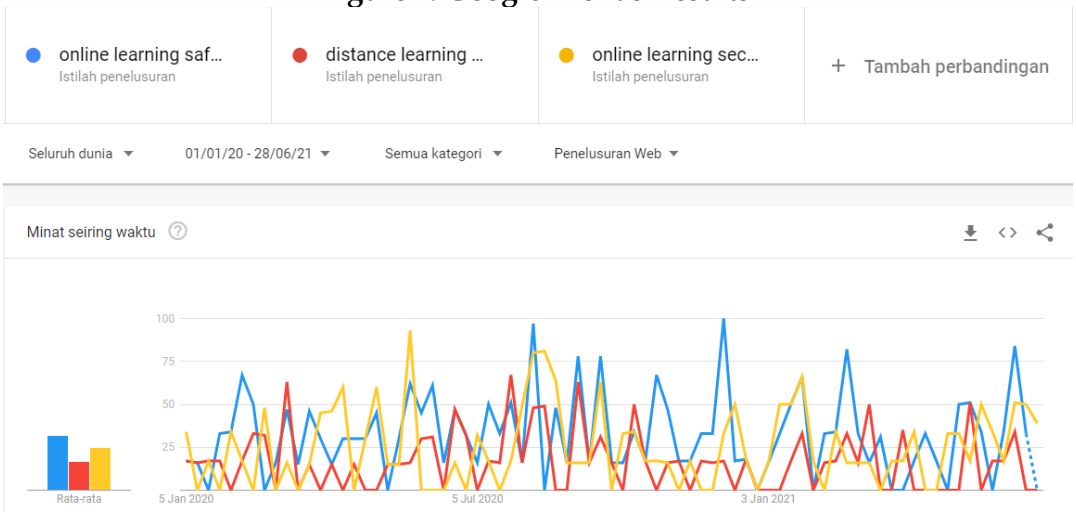
Figure 1. Research Method



Here we describe the web mining methods we use:

In the first step, we use keywords like "E-Learning", "Online Learning" "Learning From Home" "Distance Learning" "CyberSecurity" and "Internet Safety" in our advanced google search (www.google.com), Due to a large number of articles, we decided to limit search results from January 2020 to June 2021. To see how much internet users interest in security in distance learning, we use *Google Trends*, with three keywords, namely "Online Learning Security", "Online Learning Safety" and "Distance Learning Security". and obtained the following results:

Figure 2. Google Trends Results



The second step: We read and select the results obtained in web mining in the first step, and obtained 237 relevant web articles, then collected and became a sample of data to be studied further. The third step: conducting Concept Analysis and Mapping (CAAM) on the previously collected data, the data is processed with one of the CAAM software, namely Leximancer 5.0 (https://lexiportal-app.leximancer.com/),

Leximancer is used to extract and classifying keywords and themes on the data that has been collected and identifying patterns and relationships between themes and concepts (Chen & He, 2013). Leximancer is a useful tool when researchers want to explore, textual data and try to uncover important factors contained in the data (Sotiriadou, Brouwers, & Le 2014). Leximancer software uniquely extracts and describes the classification of important terms between keywords and develops a concept map (Pill, Harvey & Hyndman, 2017). Watson, Smith & Watter further stated that the technology behind Leximancer is Bayesian Theory, where fragmented pieces of evidence can be used to predict what is happening on the system (2005).

RESULT AND DISCUSSION

Based on the Literature Review results from various academic sources (Google Scholar, Taylor and Francis Online, Springer Link, ACM Library, AACE Digital Library), most of the threats that can occur in distance learning is described in the table below :

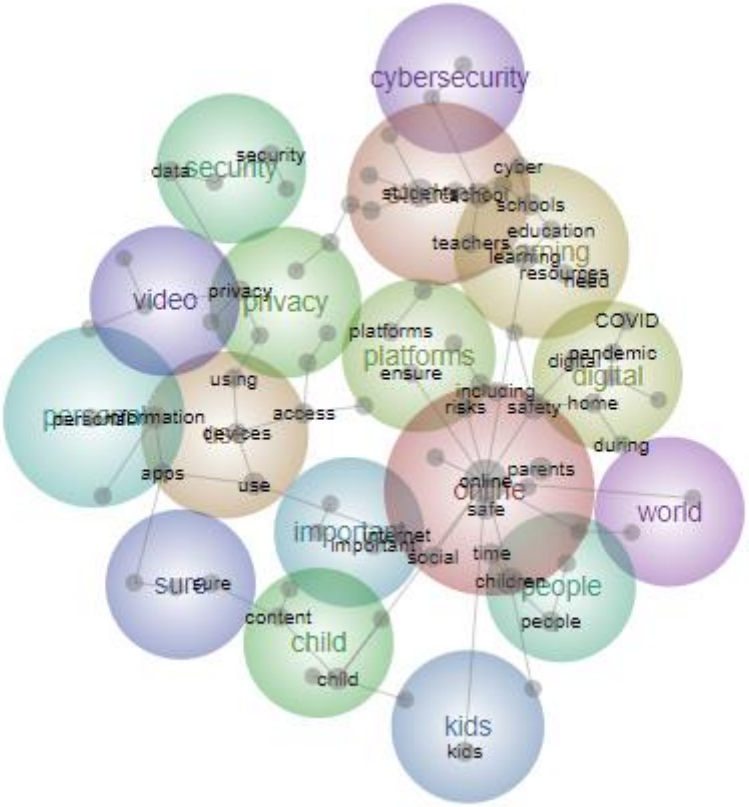
Table 1. Types of Threats & Protection Measures

Type of Threats	Protection Measures
• Phishing, Scamming, Fraud. • Cyber Bullying • Virus (Malware, Trojan, Rootkits, Ransomware) (Ktoridou, Eteokleous & Zahariadou, 2012) • Privacy and Personal data Problem (Davis&James, 2012) • Hacking (i.e.: ARP cache poisoning and Man In The Middle Attack, Brute Force Attack, Cross-Site Request Forgery, Cross-Site Scripting, Distributed Denial of Services, IP Spoofing, Session Hijacking, SQL Injection) (Chen & He, 2013) • False Information (Hoax) and Data Theft. (Piscikiene, Romeikiene & Šustickienė, 2021) • Explicit Content & Pornography (Kritzinger, 2017)	• Parental Assistance in Accessing Internet Content (Ktoridou, Eteokleous & Zahariadou 2012) • Provide learning about internet safety and personal data protection (Anastasiades & Vitalaki, 2011) • Keeping the "CIA Triad" (Availability, Integrity, Confidentiality) of information for safe in cyberspace (Miguel, et al., 2015) • The role of the teacher in providing appropriate assistance and prevention to students (Berson & Berson, 2003) • Using parental control software (i.e. Google Family Link) (Kritzinger, 2017) • Installing firewall and antivirus (Chen & He, 2013)

To avoid and minimize threats, the researchers provide some suggestions for protection and prevention, further can be seen in the table above. From the table above, the researcher provides various examples of threats that are commonly found during the online learning process, it can be seen in the table above, some examples are phishing scamming and fraud which refers to the theft of information by unauthorized

people, cyberbullying refers to behavior bullying in cyberspace. There are various prevention efforts, but most involve adult involvement in prevention.

Figure 3. Concept Map Generated in Leximancer



The figure above is the results of the analysis obtained from the Leximancer software, the following image is a concept map generated by Leximancer from web mining data. The big circle is the Cluster Concept and the dots represent the Main Concept. The table shows five groups of Cluster Concepts from the results of Leximancer's analysis. From the results of Leximancer's analysis, most of the articles on websites and blogs only focus on general things, this is shown from the resulting Cluster Concepts, the five highest Cluster Concepts are "Online", "Use", "Students", "Learning and Digital", not many articles that describe threats and protection from threats. However, most of the articles written on the website have discussed privacy issues as a threat. From the results of this web mining, it is concluded that digital threats that occur during distance learning are various and not just one type of threat, but the biggest threat being discussed is the issue of privacy.

Table 2. Cluster Concept & Concept

Cluster Concept	*Concept*
Online	online, safety, children, internet, safe, parents, time, important
Use	use, privacy, access, devices, using
Students	students, school, teachers, cyber
Learning	learning, schools, education, need, resources

Digital	digital, COVID, home, pandemic, during, support

The table above is a detailed form of the previous image, it can be seen that from the results of web mining the word "Online" is related to "online, safety, children, internet, safe, parents, time, important". Likewise with the word "use" related to "privacy, access, devices, using", students related to "school, teachers, cyber", "learning" related to "schools, education, need, resources" and "digital" related to "COVID, home, pandemic, during, support". The articles we use are articles in English, this is because articles in Indonesian are very rarely discussed this problem.

Discussions about digital safety in the field of education are not new among researchers, a Tomcyzk (2019) conducted linking digital literacy and digital safety, but the discussion only covered cyberbullying and communication with other internet users, Putnam (2019) also stated the importance of digital safety and linking it with digital citizenship, another study was also conducted by Martin (2021) this study emphasizes the role of parents in supervising children in accessing the internet.

This study looks at digital safety from an Indonesian perspective so that it is provided with resources that can be used to increase knowledge about digital safety, besides that this research also discusses cyber threats that generally occur and prevention efforts taken, this study also takes the latest sources on the internet at the time of writing this article, several studies did not provide adequate resources to increase understanding of digital safety. From the results of the literature review and web mining, we will describe in detail the causes of digital threats and the protection measures that can be taken.

(1) Causes of Digital Threats

The causes of digital threats can be divided into two aspects, namely: the user side and the management side (Chen & He 2013:117). From the user's point of view Piščikienė et. al. provides the view that there are many forms of digital threats. The best way to avoid this threat is to raise awareness among internet users about cyber literacy and cyberculture (2021), in other words, to build cybersecurity awareness for interaction and collaboration between students (Raitman, et.al., 2005). Shaw defines cybersecurity awareness as the level of understanding of users about the importance of information security and their responsibilities and actions to implement an adequate level of information security controls, to protect organizational data and networks (Zwiling et. al., 2020). Self-awareness about the confidentiality of personal data needs to be built, the American Library Association provides guidelines to keep children safe on the internet (1) never give out names, addresses, telephone numbers, or school names; (2) never go to strange sites on the internet; (3) never post credit card numbers; (4) never meet someone you meet online without discussing it with your parents; (5) if you see something disturbing and scary, always ask your parents or trusted people (Burriss, 2003). From some suggestions given by experts, users in this case teachers, students and online learning management agencies need to grow awareness of digital security and be aware of the security of personal data.

Identity and privacy issues are also important issues in distance learning. The growing internet makes personal data theft and fraud also increase (Raitman, et.al., 2005). Personal data theft generally uses social engineering methods such as phishing (Piščikienė et. al., 2021), to trick victims into believing and give their data. From the management side, in this case, e-learning management institutions also need to maintain a safe e-learning environment. Alwi & Fan provide a view, the most

important thing to avoid all attacks on the e-learning environment is controlling the access through the authentication and authorization process (2010). The development of e-learning systems must be carried out using international standard security methods and standards and implement security such as access control, authentication, encryption, and user management and permissions (Costinela & Nicoleta, 2012). E-Learning must also be periodically updated to avoid bugs and security gaps that can be exploited by outsiders. To avoid and prevent DDoS attacks on e-learning platforms, Kaspersky Security Experts (Cyber Security Company) provide recommendations: (1) maintain the operation of web resources by assigning specialists who understand how to respond to DDoS attacks; (2) validation of third party agreements and contact information; (3) apply professional solutions (Kaspersky, 2020).

(2) Protection and Prevention from Digital Threats

a. Assistant in Accessing Internet Content

Research conducted on parents and children in Europe, states that children in Europe experience one of the threats on the internet, and their parents are not aware of it. About 40% of parents whose children have seen sexual images online say that their children have never seen them, 56% of parents whose children have received malicious or hurtful messages online say that their child has never experienced it (Livingstone, et. al., 2011). In the era of cyberspace as it is today, collaboration from various parties is needed, to keep students safe and secure in cyberspace. Kritzinger (2017), provides several steps that parents can take to keep their children safe in cyberspace: (1) discuss rules related to cyberspace at home; (2) explain the consequences if the rules are not followed; (3) identify possible cyber risks that may occur when using the internet; (4) download Parental Control software (eg Google Family Link) to view children's online activity; (5) provide an action plan that students can follow if a cyber incident occurs.

Mentoring children in accessing internet content is very important and necessary when learning online. Paus-Hasebrink et. al. classifying parent-child relationships into four types. The first type is children who are clearly more skilled than their parents and use the internet relatively independently. The second type is, children who have just started using the internet, have very low skills, and lack support from their parents. The third type is children who use the internet very often and exchange information with their parents. The last type is children who are strictly regulated by their parents (Paus-Hasebrink et. al., 2013). The results of a study conducted by Ihmeideh & Shawareb of four parenting styles namely Authoritarian, Authoritative, Permissive, and Neglectful indicate that parents tend to use an authoritative style, namely parenting that gives strict rules to children but they remain involved with their children (Ihmeideh & Shawareb, 2014) This is in line with the results of a study conducted by Valcke et. al. his findings found that 59.3% of the sample studied adopted an Authoritative parenting style (Valcke et. al. 2010).

Parents face difficult challenges but must play an active role in maintaining children's digital security. By actively learning from various media and sources such as printed books, magazines, television to the internet (Dedkova, Smahel & Just, 2020). Research conducted by Wang & Xing mentions the need for parental involvement in reinforcing to reduce the risks and dangers of the internet (Wang & Xing 2018).

b. Learn About Internet Safety and Private Data Protection

In the school environment, Kritzinger (2017) also provides several prevention and protection measures, namely: (1) Implementing cybersecurity policies in schools; (2) increasing knowledge about cybersecurity by putting up posters, conducting competitions, discussions or by integrating knowledge about cybersecurity into the

curriculum; (3) implement an action plan for reporting and dealing with cybersecurity incidents; (4) Ensure teachers have the necessary cybersecurity knowledge to help students. At level of policymakers and the government also needs to play an important role in providing education and protection policies for students. Parents also need to talk about issues of digital security, privacy, the risks of posting personal information, and the importance of not talking to strangers and going somewhere with strangers. This discussion of risks and behavior on the internet needs to be as natural as any other discussion. In addition, parents need to discuss the negative consequences of bullying behavior and/or saying cruel, or threatening things through technology. (Kite, Gable & Filippeli, 2013)

The Indonesian government actively provides education about safe and comfortable in cyberspace through several institutions, for example, ICT Watch which compiled three "Indonesian Digital Literacy Frameworks" consisting of Safeguard, Rights, and Empowerment. The Ministry of Education and Culture also released the book Digital Literacy Supporting materials so that every individual needs to understand that digital literacy is an important thing needed to participate in today's modern world (Nasrullah et.al., 2017). In Indonesia, the implementation of education regarding Digital Literacy is constrained by Indonesia's economic problems, as well as the complexity and limited quantity and quality of ICT infrastructure, plus the low level of public awareness and knowledge about ICT (Rahmah, 2015). However, despite the obstacles that occur, several institutions and organizations play an active role in providing digital literacy education to the public, for example, ICT Watch, Siber Kreasi, ICT Volunteers, and internetsehat.id.

Several institutions or organizations provide education about internet safety for various ages, in Indonesia for example there is ICT Watch (http://learning.ictwatch.id/) which provides various kinds of materials, infographics, and other information about security on the internet. such as Digital Literacy Fundamentals which contain material about digital smart netizens, online parenting, digital activism, privacy & personal data protection, and so on. There is also siberkreasi (https://www.siberkreasi.id/) which actively holds seminars on digital literacy.

Common Sense (https://www.commonsensemedia.org/) also provides information on how to use social media, text messaging and privacy as well as material on internet safety, cyberbullying and good online behavior (Kite, Gable & Filippeli, 2013), Common Sense Media also provides ratings for movies, television shows, books and so on so parents can choose entertainment that suits their children (Commonsense, 2021). In addition, one part of Common Sense is common sense education which provides support for the needs of teachers to teach the next generation of digital citizens.

A digital resource for teachers, students, and education leaders, also provided by the International Society for Technology in Education (ISTE), which provides several standards of skills and knowledge for teachers, students, and education leaders about what they need to achieve, developing and contributing to an interconnected global world, ISTE focuses on Digital Citizenship, STEAM in Education, Open Educational Research, AI in education, Teacher Education, Computational Thinking in Education, Online Learning and so on (ISTE 2021).

c. Digital Citizenship Education as Character Education in the Digital World

The digital era invites us to enter a new era of character education (Ohler 2011:26). Digital Citizenship is defined as appropriate and responsible behavior in the use of digital technology, which is an important component of technology education

(Martin, Gezer & Wang 2019). Adding an explanation from Martin, Gezer & Wang, the International Society for Technology in Education (ISTE) defines digital citizenship as enabling students to recognize their rights, responsibilities, and opportunities to live, learn, and work in an interconnected digital world, and they act. and set an example in a safe, legal and ethical way (ISTE, 2021). Meanwhile, ISTE teachers explained that educators inspire students to contribute positively and participate responsibly in the digital world, one of which is guiding students in safe, legal, and ethical practices with digital tools (ISTE, 2021). In addition, the direction of digital citizenship education must be set so that students can grow into citizens who participate actively in interactions with other citizens, with various interests in online communities, to solve various community and global problems (Kim & Choi, 2018). The issue of digital citizenship is hot recently driven by the dangers that can arise from internet use, such as cyberbullying, sexting, and other psychological and physical threats (Gleason & Von, 2018).

The need to inculcate digital citizenship in students, so that they can behave ethically and have a character in cyberspace. So that they do not become perpetrators and victims of unwanted things. A hot issue at the moment is cyberbullying, Nasywa, Tentama & Mujidin provide a definition of cyberbullying, namely aggressive behavior on social media in the form of insulting, humiliating, and threatening others repeatedly (2021:1), researchers give a different view -different in the definition of cyberbullying. However, in this study, we take the definition from Patchin & Hinduja which states that "Cyberbullying is when someone repeatedly harasses, moles, or makes fun of another person online or while using a cell phone or other electronic device" (Patchin & Hinduja 2012:14). From several studies on cyberbullying in Indonesia, researchers found that both men and women had been victims of cyberbullying, but men were more often involved in cyberbullying behavior, this was due to group confirmation (Ruangnapakul, Salam & Shawkat, 2019). The teacher's role in preventing cyberbullying is considered necessary, teachers who use social media to enrich learning have the duty and responsibility to teach students how to use social media properly (Waters et.al. 2020). Teachers and parents need to have adequate knowledge about online technologies that children often use and the important features associated with these technologies. So that they have better knowledge when helping their children when they need help (Paat & Markham, 2021). In addition to digital citizenship, the term netiquette has also become a hot topic among researchers. Brown, defines netiquette as an unwritten rule when interacting in the digital world that guides how to behave and communicate (Brown, 2014). In essence, netiquette is needed to avoid discriminatory, slanderous, or insulting comments online, and to encourage respect and sensitivity to other people's cultures (Martin, et.al. 2018: 215).

In the end, being safe and comfortable in the digital world depends on the child himself. Even though the internet offers anonymity, digital footprints or information spread across the internet can backfire. The concept of "Netiquette" or ethics in cyberspace and maintaining one's reputation in cyberspace must be introduced early (Pridgen 2010: 135). In addition, in the future, cybersecurity education is expected to prevent inappropriate postings, hacking incidents, or privacy violations (Atif & Chou, 2018:153). The importance of parents accompanying children and the role of various related parties are needed so that children can be safe and comfortable in cyberspace.

(3) Education and Digital Safety

Understanding digital safety in the online learning era such as the current covid-19 pandemic provides a sense of security in learning and working in the digital world,

digital safety is one of the indicators in many studies on digital literacy, Tomcyzk (2020) stated that teachers should have an understanding up-to-date on digital safety and cyber threats so that they can provide examples and a comprehensive understanding of prevention and things to do, in addition, Moreno (2013) stated that teachers in this era should teach about internet safety, even from elementary school students. In addition, understanding digital safety has also become a concern for the Indonesian government in the digital literacy program, coupled with the ongoing covid-19 pandemic, resulting in the learning process relying heavily on digital media, an understanding of digital safety, and digital literacy is considered necessary to be well understood.

From the findings that have been described previously, it is necessary to have a deep understanding of digital threats and their prevention efforts, besides that adequate digital literacy is needed to support understanding of digital threats during online learning, based on a survey conducted by the Ministry of Communications and Information Technology of the Republic of Indonesia which states that the index digital literacy is at 3.49 on a scale of 1-5, this means that Indonesia is on a medium level, so it is necessary to increase the level of digital literacy (APTIKA, 2022).

In addition, with awareness of digital threats when online learning is considered necessary so that teachers and students are aware and more careful in using internet media, it is hoped that understanding threats and prevention can be useful knowledge in the event of a digital security incident in the classroom in the future. Tomcyzk (2019) stated that an understanding of digital safety is something that teachers need to have today, especially the learning resources used mostly come from the internet.

CONCLUSION

Based on the results of research conducted, several threats that can occur are phishing, scamming, fraud, cyberbullying, viruses, privacy issues and personal data as well as obscene or pornographic content, from the results of web mining discussions conducted by articles on the website have not provided details. However, the issue of privacy is the most discussed discussion, prevention efforts need to be carried out, cooperation between parties in providing protection and prevention is considered important, researchers provide several recommendations that can be done to avoid threats. The synergy between schools, parents, teachers and the government also needs to be improved.

Some suggestions for prevention that can be done are assistance in accessing internet content, providing learning about internet safety and personal data protection, as well as an introduction to Digital Citizenship and ethics in cyberspace. In the future, it is hoped that there will be learning about ethics in cyberspace in the curriculum, so that students can have character not only in the real world but also in cyberspace. Based on the researcher's direct experience in the research process, there are several factors that become research limitations that can be considered for future researchers in order to improve their research, including: web mining data are data taken from January 2020 to June 2021, so that maybe in the future there will be additional data, threats and solutions from other researchers.

ACKNOWLEDGEMENT

The researchers highly appreciate all supports from the Universitas Negeri Yogyakarta. The researchers would like to thank and appreciate all supervisors, editors, and academics.

AUTHOR CONTRIBUTION STATEMENT

DMZ is main researcher, and the paper is evaluated by AM and HR.

REFERENCES

Alwi, N. H. M., & Fan, I. S. (2010). E-learning and information security management. *International Journal of Digital Society (IJDS)*, 1(2), 148-156. Google Scholar

Anastasiades, P. S., & Vitalaki, E. (2011). Promoting Internet Safety in Greek Primary Schools: the Teacher's Role. *Educational Technology & Society*, 14 (2), 71–80. Google Scholar

Asosiasi Penyedia Jasa Internet Indonesia (APJII) (2019) *Laporan Survey Internet APJII 2019-2020 (Q2)*. Retrieved July,2,2021, Google Scholar

Aptika Kominfo (2022). Indeks Literasi Digital Indonesia 3.49, Ini yang Bisa Dilakukan Pemerintah. Retrivied May 18 2022 from Google Scholar

Atif, Y., & Chou, C. (2018). Digital Citizenship: Innovations in Education, Practice, and Pedagogy. *Journal of Educational Technology & Society*, 21(1), 152-154. Retrieved July 1, 2021, Google Scholar

Berson J. M., & Berson I. R. (2003) Lessons Learned About Schools and Their Responsibility to Foster Safety Online, *Journal of School Violence*, 2:1, 105-117, https://doi.org/10.1300/J202v02n01_06

Brown, S. A. (2014). Conceptualizing digital literacies and digital ethics for sustainability education. *International Journal of Sustainability in Higher Education*, 15(3), 280–290. https://doi.org/10.1108/ijshe-08-2012-0078

Burriss, L., L. (2003) Safety in the Cybervillage Some Guidelines for Teachers and Parents, *Childhood Education*, 79:5, 318-319, DOI: https://doi.org/10.1080/00094056.2003.10521219

Carrillo, C., & Flores, M. A. (2020). COVID-19 and teacher education: a literature review of online teaching and learning practices. *European Journal of Teacher Education*, 1–22. https://doi.org/10.1080/02619768.2020.1821184

Chen, Y. & He, W. (2013). Security Risks and Protection in Online Learning: A Survey. *International Review of Research in Open and Distributed Learning*, 14(5), 108–127. https://doi.org/10.19173/irrodl.v14i5.1632

Costinela-Luminița, C. (Defta), & Nicoleta-Magdalena, C. (Iacob). (2012). E-learning Security Vulnerabilities. *Procedia - Social and Behavioral Sciences*, 46, 2297–2301. https://doi.org/10.1016/j.sbspro.2012.05.474

Commonsense (2021). *You know your kids. We know media and tech. Together we can build a digital world where our kids can thrive*. Google Scholar

Dedkova, L., Smahel, D., & Just, M. (2020) Digital security in families: the sources of information relate to the active mediation of internet safety and parental internet skills. *Behaviour & Information Technology*, DOI: https://doi.org/10.1080/0144929X.2020.1851769

Gleason, B., & Von Gillern, S. (2018). Digital Citizenship with Social Media: Participatory Practices of Teaching and Learning in Secondary Education. *Journal of Educational Technology & Society*, 21(1), 200-212. Retrieved July 1, 2021, from http://www.jstor.org/stable/26273880

Hootsuite We Are Social. (January 2021)*Indonesia Digital Report 2021*.Retrieved July, 2, 2021, from Google Scholar

Ihmeideh, F., M., & Shawareb, A., A. (2014) The Association Between Internet Parenting Styles and Children's Use of the Internet at Home, *Journal of Research in*

Childhood Education, 28:4, 411-425, DOI: https://doi.org/10.1080/02568543.2014.944723

International Society for Technology in Education (ISTE). (2021) *ISTE Standard for Students*. Google Scholar

International Society for Technology in Education (ISTE). (2021) *ISTE Standard for Teachers*. Diakses di https://www.iste.org/standards/iste-standards-for-teachers

Katie Davis & Carrie James (2013) Tweens' conceptions of privacy online: implications for educators. *Learning, Media and Technology*, 38:1, 4-25, https://doi.org/10.1080/17439884.2012.658404

Kaur Chahal, J., Bhandari, A., & Behal, S. (2019). Distributed Denial of Service Attacks: A Threat or Challenge. *New Review of Information Networking*, 24(1), 31–103. https://doi.org/10.1080/13614576.2019.1611468

Kaspersky. (September 2020). *DDoS attacks against educational resources increased by more than 350% this spring*. Retrieved July, 5, 2021, from https://www.kaspersky.com/about/press-releases/2020_ddos-attacks-against-educational-resources-increased-by-more-than-350-this-spring

Kim, M., & Choi, D. (2018). Development of Youth Digital Citizenship Scale and Implication for Educational Setting. *Journal of Educational Technology & Society*, 21(1), 155-171. Retrieved July 1, 2021, from Google Scholar

Kite, S. L., Gable, R. K., & Filippelli, L. P. (2013). Cyber threats: a study of what middle and high school student know about threatening behaviours and internet safety. *International Journal of Social Media and Interactive Learning Environments*, 1(3), https://doi.org/10.1504/ijsmile.2013.055733

Kritzinger, E. (2017) Cultivating a cyber-safety culture among school learners in South Africa, *Africa Education Review*, 14:1, 22-41, DOI: https://doi.org/10.1080/18146627.2016.1224561

Ktoridou, D., Eteokleous, N., & Zahariadou, A. (2012). Exploring parents' and children's awareness on internet threats in relation to internet safety. *Campus-Wide Information Systems*, 29(3), 133–143. https://doi.org/10.1108/10650741211243157

Lei, Sut Ieng & So, Amy Siu Ian (2021) Online Teaching and Learning Experiences During the COVID-19 Pandemic – A Comparison of Teacher and Student Perceptions, *Journal of Hospitality & Tourism Education*, 33:3, 148-162, https://doi.org/10.1080/10963758.2021.1907196

Lee, S., Yeo, J., & Na, C. (2020). Learning From the Past: Distributed Cognition and Crisis Management Capabilities for Tackling COVID-19. *The American Review of Public Administration,* 50(6–7), 729–735. https://doi.org/10.1177/0275074020942412

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children. Full Findings*. London: EU Kids Online. Retrieved July, 6, 2021 from Google Scholar

Miguel, J., Caballé, S., Xhafa, F., & Prieto. J. (2015) Security in online web learning assessment. *World Wide Web 18*, 1655–1676. https://doi.org/10.1007/s11280-014-0320-2

Martin, F., Gezer, T., & Wang, C. (2019). Educators' Perceptions of Student Digital Citizenship Practices. *Computers in the Schools*, 1–17. doi: https://doi.org/10.1080/07380569.2019.1674621

Martin, F., Gezer, T., Anderson, J., Polly, D., & Wang, W. (2021). Examining Parents Perception on Elementary School Children Digital Safety. Educational Media International, 58(1), 60–77. https://doi.org/10.1080/09523987.2021.1908500

Martin, F., Wang, C., Petty, T., Wang, W., & Wilkins, P. (2018). Middle School Students' Social Media Use. *Journal of Educational Technology & Society*, 21(1), 213-224. Retrieved July 1, 2021, from Google Scholar

Moreno, M.A., Egan, K.G., Bare, K. et al. Internet safety education for youth: stakeholder perspectives. *BMC Public Health* 13, 543 (2013). https://doi.org/10.1186/1471-2458-13-543

Naila,N., Tentama, F., & Mujidin. (2021). What Makes The Cyberbullying Model Among Vocational High School Students. *Cakrawala Pendidikan*, Vol. 40, No. 2, June 2021. https://doi.org/10.21831/cp.v40i2.34549

Nasrullah, Rullie. Et. al. (2017). *Materi Pendukung Literasi Digital* [Digital Literacy Support Materials] . Jakarta:Kementerian Pendidikan dan Kebudayaan.

Ohler, Jason (2011) Digital Citizenship Means Character Education for the Digital Age, *Kappa Delta Pi Record*, 47:sup1, 25-27, DOI: https://doi.org/10.1080/00228958.2011.10516720

Pill S., Harvey S., & Hyndman B. (2017) Novel research approaches to gauge global teacher familiarity with game-based teaching in physical education: an exploratory #Twitter analysis, *Asia-Pacific Journal of Health, Sport and Physical Education*, 8:2, 161-178, https://doi.org/10.1080/18377122.2017.1315953

Piscikiene, I., Romeikiene, J., & Šustickienė, B. (2021) Cyber Vulnerability In Light Of Online Learning Reality. SIE (Society Integration Education) *Proceedings of the International Scientific Conference*. Volume V, May 28th-29th, 2021. 426-435. https://doi.org/10.17770/sie2021vol5.6367

Patchin, J., W. & Hinduja S. (2012) *Cyberbullying Prevention and Response, Expert Perspective*. New York: Routledge

Paat, Y., & Markham, C. (2021) Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century, *Social Work in Mental Health*, 19:1, 18-40, DOI: https://doi.org/10.1080/15332985.2020.1845281

Pridgen, B. (2010) Navigating the Internet Safely: Recommendations for Residential Programs Targeting At-Risk Adolescents, *Harvard Review of Psychiatry*, 18:2, 131-138, https://doi.org/10.3109/10673221003684000

Paus-Hasebrink, I., Bauwens, J., Dürager, A. E., & Ponte, C. (2013). Exploring Types of Parent–Child Relationship and Internet use across Europe. *Journal of Children and Media*, 7(1), 114–132. https://doi.org/10.1080/17482798.2012.739807

Putnam, Christina, "Teaching in a Digital Age: Internet Safety Education" (2019). Capstone Projects and Master's Theses. 429. Google Scholar

Raitman, R., L. Ngo, N. Augar & Wanlei Zhou, "Security in the online e-learning environment," *Fifth IEEE International Conference on Advanced Learning Technologies (ICALT'05)*, 2005, pp. 702-706, doi: https://doi.org/10.1109/ICALT.2005.236.

Rahmah, A. (2015). Digital Literacy Learning System for Indonesian Citizen. *Procedia Computer Science*, 72, 94–101. https://doi.org/10.1016/j.procs.2015.12.109

Ruangnapakul, N., Salam Y.D., & Shawkat A.R., (2019) A Systematic Analysis of Cyber bullying in Southeast Asia Countries. *International Journal of Innovative Technology and Exploring Engineering (IJITEE).* Volume-8, Issue-8S, June 2019. Retrieved : 17 July 2021, From Google Scholar

Soldatova, G. U., & Rasskazova, E. I. (2016). Adolescent Safety on the Internet. *Russian Education & Society*, 58(2), 133–162. https://doi.org/10.1080/10609393.2016.1214492
Soldatova, G. U., & Rasskazova, E. I. (2016). Adolescent Safety on the Internet. *Russian Education & Society*, 58(2), 133–162. https://doi.org/10.1080/10609393.2016.1214492
Sotiriadou,P., Brouwers J., & Tuan-Anh Le (2014) Choosing a qualitative data analysis tool: a comparison of NVivo and Leximancer, *Annals of Leisure Research*, 17:2, 218-234, https://doi.org/10.1080/11745398.2014.902292

Tomczyk, Ł., (2019) What Do Teachers Know About Digital Safety?, Computers in the Schools, 36:3, 167-187, https://doi.org/10.1080/07380569.2019.1642728

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. Google Scholar

Valcke, M., Bonte, S., De Wever, B., Rots, I., Internet parenting styles and the impact on Internet use of primary school children, *Computers & Education*, Volume 55, Issue 2, 2010, Pages 454-464, https://doi.org/10.1016/j.compedu.2010.02.009

Wang, X., & Xing, W. (2018). Exploring the Influence of Parental Involvement and Socioeconomic Status on Teen Digital Citizenship: A Path Modeling Approach. *Journal of Educational Technology & Society*, 21(1), 186-199. Retrieved July 6, 2021, from http://www.jstor.org/stable/26273879

Watson M., Smith A., & Watter S. (2005) Leximancer Concept Mapping of Patient Case Studies. In: Khosla R., Howlett R.J., Jain L.C. (eds) Knowledge-Based Intelligent Information and Engineering Systems. KES 2005. *Lecture Notes in Computer Science*, vol 3683. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11553939_171

Waters, S., Russell, W. B., & Hensley, M. (2020). Cyber Bullying, Social Media, and Character Education: Why It Matters for Middle School Social Studies. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, 1–10. https://doi.org/10.1080/00098655.2020.1760770

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin F. & Basim H., N. (2020) Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, *Journal of Computer Information Systems*, DOI: https://doi.org/10.1080/08874417.2020.1712269