Online Threats vs. Mitigation Efforts: Keeping Children Safe in the Era of Online Learning

Tiffany O'Dell
Department of Mathematical, Computing, and Information Sciences
Jacksonville State University
Jacksonville, Alabama, USA
jsu3583m@jsu.edu

Arup Kumar Ghosh
Department of Mathematical, Computing, and Information Sciences
Jacksonville State University
Jacksonville, Alabama, USA
akghosh@jsu.edu

***Abstract*—As the COVID-19 pandemic resulted in school closures since early 2020, children have spent more time online through virtual classrooms using educational technology (EdTech) and videoconferencing applications. This increased presence of children online exposes them to more risk of cyber threats. Here, we present a review of the current research and policies to protect children while online. We seek to answer four key questions: what are the online threats against children when learning online, what is known about children's cybersecurity awareness, what government policies and recommendations are implemented and proposed to protect children online, and what are the proposed and existing efforts to teach cybersecurity to children? Our study emphasizes the online risks to children and the importance of protective government policies and educational initiatives that give kids the knowledge and empowerment to protect themselves online.**

***Keywords*—online safety, kid, child, teenager, adolescent, K12, remote learning, online learning, e-learning, distance learning, cybersecurity awareness, EdTech, videoconferencing**

I. Introduction

In early 2020, as COVID-19 spread and much of the world went on lockdown, remote learning became the new normal for primary and secondary school students around the globe. In the U.S. alone, approximately 50.8 million public school students were affected by this sudden shift in education delivery, and by May 2021, 80% of students were learning in a remote-only setting [1].

With this unprecedented online presence of K12 students, the risk of cybercrime, safety, and privacy threats to children also increased. The Federal Bureau of Investigation (FBI) documented a 69% increase in complaints to the Internet Crimes Complaint Center (IC3) in 2020 compared to 2019. Additionally, there were 3,202 crimes committed against children, a 59% increase from 2019 [2]. In 2021, the FBI documented a 7% rise in complaints to the IC3 as compared to 2020. Additionally, there were 2,167 crimes committed against children [3]. In April 2020, the FBI issued a public service announcement noting that cyber actors were exploiting the virtual environments being used during the pandemic, providing tips for staying safe while using education technology [4]. In December 2020, the US Cybersecurity and Infrastructure Agency (CISA) published a fact sheet noting a rise in malicious cyber incidents against school computer systems, in some cases rendering remote learning inaccessible or threatening to leak student information unless a ransom is paid [5].

While schools have essentially returned to an in-person format, some school districts have had to return to online learning due to flu outbreaks and ransomware attacks, for example [6]–[8]. Ransomware attacks against educational institutions have surged since the COVID-19 pandemic began, targeting many school districts [9]. The education sector has been subjected to cyberespionage while targets include students and platforms such as Zoom, which many students use during remote learning [10]. Even more alarmingly, 500,000 Zoom passwords have recently surfaced on the dark web [11]. Furthermore, Human Rights Watch found that 145 out of 163 educational technology (EdTech) remote learning tools collected and shared students' data with 196 third-party companies, mostly advertising technology companies, such that the students were then tracked across the internet [12]. In response, the US Federal Trade Commission (FTC) issued a policy statement to EdTech companies, in which the FTC asserted that companies cannot require students to surrender their privacy in exchange for learning online and maintained that EdTech must protect student privacy [13].

The many risks that exist to children's online privacy and safety and the increased use of EdTech learning applications necessitate investigating and summarizing the existing threats, policies, and cybersecurity awareness strategies. This literature review explores the following key questions listed by section:

- Section III.A. discusses the existing threats that kids face when using EdTech online learning tools.
- Section III.B. evaluates what is known about cybersecurity awareness among K12 students.
- Section III.C. examines government policies that have been implemented or proposed to safeguard kids' privacy and security.
- Section III.D. explores proposed and existing efforts to teach cybersecurity to K12 students.

Our research has revealed that while there are efforts being made to protect children online, much work still needs to be done by governments, organizations, and school districts

978-1-6654-7611-9/23/$31.00 ©2023 IEEE

to ensure students' privacy and safety when using EdTech and videoconferencing tools. Our goal in this article is to provide the cybersecurity community, policymakers, and K12 administrators and educators with an overview of the latest research, policies, practices, and open issues, including both existing and proposed efforts to keep K12 kids safe online in the era of online learning. Note that in our paper, the definition of a child is a person who is under 18 years old as defined by the Convention on the Rights of the Child [14].

II. Methods

Our research is based on an academic literature review, web search, and policy review. Google Scholar and Google Search were used. Most sources are from no earlier than the year 2020, although some are from before 2020 for additional background information as needed. Our research is based on answering the key questions listed in Section I and discussed in Section III. Example keywords in our search include distributed systems, children, teenager, online safety, online safety threats, cybersecurity, e-learning, online learning, remote learning, distance learning, cyberattacks on children, cybersecurity awareness, cybersecurity education, cybersecurity knowledge, cybersecurity awareness, gamification, and game-based-learning, and policies.

III. Results

A. Online Privacy and Security Risks to K12 Children

The US Government Accountability Office (GAO) reported in September 2020 that between July 2016 and May 2020, there were 99 disclosed student data breaches that affected 287 K12 school districts and thousands of students. Types of student data that were breached include academic records, personally identifiable information (PII), login credentials, medical data, location data, demographic information, etc. Data breaches such as these might result in "physical, emotional, and financial harm" [15]. The K12 Security Information Exchange (K12 SIX) revealed in its 2022 annual report that there were 1,331 publicly reported cyber incidents between 2016 and 2021, including but not limited to student data breaches, ransomware attacks, and invasions of online classes and school meetings [16].

This kind of threat to student privacy and school information technology (IT) infrastructure was only exacerbated by the sudden rush to online learning by K12 schools that were inadequately prepared or lacked the resources to handle this expanded reliance on information technology. For instance, as school districts circumvented security measures that protect students' data, the Connecticut governor signed an executive order in early 2020 that permitted Connecticut to temporarily wave its state student privacy law [1] Factors that compromise online learning safety include insecure network connections, lack of digital literacy, and the "digital hijacking" of remote learning applications [10]. Online security threats increased as an unprecedented number of K12 students attended school remotely. For instance, the FBI issued public service announcements in May and October 2020 warning of an increase in online threats to minors, including broadcasting child sexual abuse material during Zoom meetings [17] and predators luring children on social media to facilitate child abductions [18].

In a national survey, U.S. teens between 13 and 17 reported experiencing a significant increase in cyberbullying since the beginning of the pandemic, while Asian American youth have experienced racially motivated cyberbullying at an increasingly disproportionate rate [19]. However, another study found that cyberbullying had stayed relatively stable [20]. Furthermore, in December 2020, CISA issued an alert that warned of reports that cyber actors were disrupting distance learning services and stealing personal data. For example, ransomware attacks were used to disrupt distance learning and to steal and threaten to leak student data. By September 2020, over half of the reported ransomware attacks were against K12 institutions as compared to the months from January to July 2020, in which less than one-third of the attacks were against K12 institutions. Other cyber threat examples include DDoS attacks; video conferencing disruptions involving verbal harassment, showing pornography or violent depictions, and doxing; social engineering; and exploiting exposed ports or end-of-life software [21].

Additionally, as children are more reliant on EdTech software for school during remote learning, another major threat that K12 children face is the collection and selling of their personal data to third parties [12]. As a result, the Federal Trade Commission vowed to crack down on EdTech companies that engage in the surveillance of children, citing compliance with the Children's Online Privacy Protection Act (COPPA) which prohibits mandatory data collection, using children's data for economic gain and retaining data for longer than needed [22]. Examples of the kinds of data collected by common EdTech companies are listed in [23]. Finally, while the use of artificial intelligence (AI) in EdTech might help to improve a child's educational experience through personalized learning, intelligent and adaptive tutoring and testing, and task automation [24], there are concerns that the data-hungry nature of AI infringes on children's data protection and privacy rights [14]. One example is the case of two children who sued Google for allegedly using its online classroom software to collect biometric data from millions of students in violation of Illinois' Biometric Information Privacy Act and COPPA [25].

B. Cybersecurity Awareness among K12 Students

A Pew Research study in the US found that 36% of Americans never read company privacy policies before consenting, while 63% say they understand little or nothing about data privacy laws and regulations. Moreover, 59% and 78% of Americans understand little to nothing about how companies and the government, respectively, collect and use their data [26]. Additionally, another Pew Research study found that most internet users could correctly answer fewer than half of cybersecurity quiz questions [27]. Thus, it is likely that parents or caretakers, or even educators, may not know enough to help

protect children's online privacy [28]. Furthermore, as children spend a significant portion of their time online, they must have a substantial amount of knowledge and understanding of cybersecurity and data privacy principles to keep themselves safe. This section discusses several small studies that measure cybersecurity and privacy knowledge, understanding, and skills among children.

According to a U.S. survey by the EdWeek Research Center, less than half of educators say that their students receive cybersecurity education. Furthermore, over a third of teachers, principals, and district leaders said they know little or nothing at all about cybersecurity education. Only 10% said they know a lot. When asked how much educators' students know about cybersecurity education, only 3% of educators said a lot, while nearly two-thirds said their students know little or nothing at all. [29].

A New Zealand study published in 2016 surveyed cybersecurity awareness among 2,214 youth aged 8-21 years old. The respondents were divided into three age groups: 8-12 (primary school), 13-17 (secondary school), and 18-21 (university). Questions were asked about cybersecurity terms, security software, data protection concepts such as access rights and backups, and sources of security breaches such as clicking on ads or installing apps. The authors found an overall cybersecurity awareness of only 19%, 32%, and 41% among age groups 8-12, 13-17, and 18–21, respectively [30].

In a study from the Netherlands which evaluated Dutch elementary and high school students' cyber-secure behavior, the authors found that students generally exhibited both cyber-secure and reckless behavior. They surmised that students learn online behavior through personal experience or family, rather than in school, thus prompting the authors to recommend that children begin learning about cybersecurity in school at an early age [31].

In a US survey of 189 students in grades 3 through 8, only 13% created passwords that are considered "very strong", a skill that the researchers argue requires both mature cognitive and linguistic abilities. However, students generally displayed good password hygiene such as password memorization and secrecy, although 6-8th grade students reportedly shared passwords with friends at a higher rate than 3rd-5th graders. Notably, more than half of 3rd-5th graders and over three-quarters of 6-8th graders reported reusing passwords extensively [32].

It is also worth noting that socio-economic status may also influence a child's cybersecurity knowledge. For example, a study from Scotland found that children who experienced financial deprivation performed worse in both password knowledge and recall, in spite of learning from the same exact curriculum and teachers as their more affluent peers [11].

C. Policies, Practices, and Recommendations for Protecting K12 Students' Privacy and Security

According to the GAO, data privacy and data security have different meanings, although they are related ideas. Data privacy involves restricting the "collection, use, and handling" of data. On the other hand, data security means that an organization (e.g., a school system, EdTech company, etc.) preserves data "confidentiality, integrity, and availability" [15]. It is important to improve laws and practices to maintain security. This section discusses various policies, practices, and recommendations for protecting children's online data privacy and security.

FERPA (US): Enforced by the US Department of Education, the Family Educational Rights and Privacy Act of 1974 (FERPA) requires federally funded schools to protect the privacy of personally identifiable information (PII) contained in student records. FERPA, however, does not directly address the use of EdTech [15]. iKeepSafe has provided a "FERPA 101 for EdTech Companies" [33]. For instance, it warns that schools will be held liable if the EdTech platform decides to change its terms of service in a way that violates FERPA, and thus, schools will be unable to use its platform. FERPA loopholes include the definition of educational record being too broad and an amendment that allows schools to disclose students' records to "educational partners" [34]. Additionally, FERPA lacks enforceability and requires significant updates to address the increasing use of third-party digital technologies in K12 schools such as cloud providers [35].

COPPA (US): Enforced by the FTC, the Children's Online Privacy Protection Act of 1998 (COPPA) addresses both data privacy and security of children under age 13, since children in this age group may not completely understand the online privacy risks and their potential negative impact [36]. In addition to websites and online services, COPPA also applies to EdTech vendors and requires that online vendors notify and obtain parental consent to collect a child's personal data [15]. Schools may consent to data collection so long as the data is for school purposes only [35]. The FTC's Policy Statement establishes that it will enforce EdTech to comply with the COPPA Rule, including limiting the collection, use, and storage of children's data and requiring a reasonable amount of data security [37]. An exception allowed by the FTC permits student data to be disclosed to "educational partners" by schools, which then requires FERPA oversight [34]. An example of such an exception is online test providers [35]. In 2013, a tool called POCKET(Parental Online Consent for Kid's Electronic Transactions) was designed to meet the requirements of COPPA. It is a prototype tool to give parents more control over their children's online privacy [38].

SOPIPA (California): Passing more stringent state laws that supplement existing federal laws like FERPA and COPPA may improve data privacy and security. One example is California's 2016 Student Online Personal Information Protection Act (SOPIPA), a student privacy bill that prohibits EdTech companies from using or selling student data for targeted advertising and disclosing PII with certain exceptions. SOPIPA also requires that EdTech companies have security measures in place to protect student data and permits deidentified student data to be used for the improvement of educational products and for marketing. As a result, many EdTech companies have signed the Student Privacy Pledge to apply the same privacy protections to students outside of California. However,

critics argue that lack of federal oversight does not hold the companies accountable to the pledge [35]. A searchable list of other U.S. state student privacy laws can be found at [39].

K12 Cybersecurity Act (US): In October of 2021, President Joe Biden signed the K12 Cybersecurity Act, which requires CISA to study the cybersecurity challenges faced by school IT systems and sensitive student records. It also requires CISA to provide a set of guidelines and online training for school leaders and to provide all study results, recommendations, and training on the US Department of Homeland Security (DHS) website [40, 41]. While the new recommendations should raise awareness and provide an actionable plan, one challenge that many schools might face is a lack of funding [42].

GDPR (European Union): The European General Data Protection Regulation (GDPR) is considered the "toughest privacy and security law in the world" [43] that regulates how organizations around the world gather, process, store, and distribute personal data from people in the European Union [44]. Under the GDPR, children under the age of 13 must have permission from their parents to consent to the processing of their data [43]. The Council of International Schools provides guidelines for ensuring that the use of online learning platforms is in compliance with GDPR [44].

Children's Code (United Kingdom): The UK's Children's Code, which is based on the GDPR [45], requires any UK or non-UK online service that obtains and processes the data of children accessing the service to comply with the code or risk paying fines. The UK Information Commissioner's Office recommends that companies map the collected data, verify users' ages, turn off geolocation services, refrain from pressing children to share more personal information, and deliver a high degree of privacy [46]. A UK survey of school officials revealed that 1 in 12 UK schools have no data officer, violating compliance with GDPR rules. Additionally, school officials gave themselves an average 6.9 out of 10 for GDPR compliance [47]. A 5Rights Foundation study in the UK found that only 1 in 10 students aged 7-16 approved of EdTech apps sharing their data and also identified a few key problems with data governance in schools. These problems include the impossibility of knowing what data EdTech is collecting, EdTech profiting off of children's data, lack of transparency of privacy policies and legal terms, and schools having the responsibility but no authority over EdTech data collection. The study recommends that the government require transparency of EdTech's data collection practices, prioritize children's interests over commercial interests and mandate the Children's Code for all of EdTech, require that EdTech be transparent in their privacy policies and legal terms, negotiate with EdTech to standardize contracts between EdTech companies and schools, and prohibit students' data from being transferred to a country that has lower data privacy standards than the GDPR, such as the US [48]

Around the world: A study by Comparitech revealed that 18 out of 50 countries have no data privacy legislation which clearly specifies the protection of children's data. France scored highest among countries because of the requirement in the French Data Protection Act that children under 15 also give joint consent alongside their parents or caretakers. However, the United States scored in the middle since COPPA fails to cover nonprofits, the government, and data brokers and is weaker than the GDPR in its restrictions on targeted advertising [49]. While COPPA does require security checks on third-party vendors, Comparitech found that 18% of "teacher-approved" apps in the Google app store violate COPPA [50].

In addition to the U.S. and global online child protection policies, many organizations offer recommendations and guidelines for keeping children safe online. These are described below.

GAO Recommendations (US): Due to the increasing prevalence of attacks on K12 IT infrastructure, the GAO has issued several recommendations to the Department of Education and the Department of Homeland Security. These recommendations include setting up cybersecurity coordination efforts between the agencies and school districts and measuring the efficacy of cybersecurity products and services. This is to be done in coordination with CISA [51].

CISA Recommendations (US): In the early days of the pandemic, CISA offered guidance to K12 schools using videoconferencing tools and online learning applications. The agency offers security and best practice recommendations to K12 organizations and end users. Example recommendations include reducing schools' attack surface by minimizing the number of collaboration tools and establishing distance learning policies that address physical and information security needs. [52].

K12 SIX Recommendations: Established in 2020, the nonprofit organization K12 Security Information Exchange (K12 SIX) aims to collaborate with and assist K12 institutions to defend themselves from growing cyber threats. The organization provides a list of actionable cybersecurity protections for schools to implement, which includes sanitizing network traffic, protecting devices, safeguarding identities, and performing routine security maintenance. Additionally, K12 SIX also advocates for more K12 cyber incident disclosures, improved cybersecurity practices among cloud software vendors like EdTech, K12 sector-specific threat intelligence and best practices, and collaboration across K12 districts [16].

D. Educating Kids about Online Safety

For students to protect themselves online and become responsible digital citizens, they need to have knowledge of cybersecurity and privacy principles. Several examples of existing or proposed measures to educate students about online safety and cybersecurity are described below. Many of these measures leverage children's interest in playing computer games. Gamification and game-based learning techniques may also be used to engage and motivate students and to improve problem-solving abilities [53].

Sponsored by the National Science Foundation and National Security Agency, the GenCyber summer camp program offers cybersecurity education to middle and high school students across the United States. Since it began in 2014, the program's

goal is to educate and inspire youth to learn cybersecurity principles through hands-on learning [54]. The total number of camps grew from 42 in 2015 to 123 in 2019, while the number of students grew from 1,240 to 15,545 in the same period. [55]. Furthermore, high interest in cybersecurity jumped from 33% to 69% in 2018 and from 27% to 73% in 2019. Additionally, attitudes towards safe online behavior grew from 85% in 2017 to 97% in 2019 [55]. Furthermore, GenCyber Girls was also shown to increase girls' interest in cybersecurity [56].

Google's Be Internet Awesome targets children in the 3rd to 5th grades [57] and aims to teach "kids the fundamentals of digital citizenship and safety so they can explore the online world with confidence". It includes a web-based game called "Interland" to teach kids digital safety and a downloadable curriculum for educators [58]. While it has the advantage of being an accessible and fun educational tool for kids, it falls short in the three following areas: (1) it doesn't educate kids about how organizations might use their data, (2) it focuses on what the user can control (e.g., passwords), but not on what the user cannot control (e.g., personal data being sold to advertisers), and (3) it depicts Google as an authority on the subject [57].

Other available educational resources include MIT Media Lab's student workshops [59], Fordham CLIP's Privacy Educators Program [60], Teaching Privacy [61], UK Safer Internet Center for ages 3-11 [62] and 11-19 [63], netsmartzkids [64], and *Stop. Think. Connect.* [65].

Antonenko, et. al. [66] proposed a curriculum that uses web- and Android-based games, puzzles, simulations, unplugged group activities, stories, and role model videos to teach kids in grades 3 through 5 cryptology and cybersecurity concepts. In the study, the authors found that by using this curriculum students as young as 8 successfully learned cryptology and cybersecurity skills.

Additional examples of gamification or game-based learning techniques proposed in the literature for cybersecurity education include "A Day in the Life of the JOs" [67], a Gamification Awareness prototype on Facebook Messenger [68], an iMonsters board game [69], the RAD-SIM framework [70], and CryptoScratch [71]. Furthermore, one study has also proposed a machine learning-based automatic feedback system for students studying cybersecurity [72].

Existing cybersecurity education techniques are not without criticism, however. Smith et. al. [54] noted a weakness in cybersecurity education programs, arguing that while these programs impart cybersecurity knowledge to the students, they may not necessarily translate into modified behavior. Thus, the authors propose that to stimulate behavioral change, the protection motivation theory must also be integrated into cybersecurity lessons. However, an empowerment strategy that promotes critical thinking is also proposed as an effective technique through building both awareness and strategic thinking [57]. Furthermore, digital literacy has been found to improve the online risk and self-control of elementary-aged students who participate in online learning [73].

A major challenge in teaching K12 students cybersecurity is the lack of teachers who have the competency and knowledge to teach the subject. A proposed solution to this is the PICSAR project used to both educate students and provide cybersecurity education training to teachers. It also helps K-8 teachers to develop STEAM lesson plans to teach grade-specific topics such as cryptography and digital ethics [74]. Additionally, Dawson et. al. [75] have proposed a 2025 vision to integrate cybersecurity education into preservice teacher education programs so that preservice teachers can incorporate cybersecurity education into their classrooms. For instance, the authors propose integrating cryptography into social studies, language arts, science, and mathematics lessons, citing CryptoClubs as an example [75].

IV. DISCUSSION

Before the pandemic, there were already concerns about children's privacy in relation to online learning [1]. When lockdowns began, schools increasingly relied on information technology infrastructure to support children's learning including EdTech and videoconferencing tools, which made K12 school systems more vulnerable to attacks [51]. In our review, we have found that as children increasingly use EdTech online learning tools, they are also at an increased risk of security and privacy breaches, especially since children tend to lack the appropriate knowledge of cybersecurity and online safety. Furthermore, the sporadic nature of K12 cybersecurity education [75] necessitates a national and international cybersecurity education standard for both K12 students and teachers.

Although there are existing and proposed policies such as those listed in Section III.C., as more children use EdTech and the internet for school, policies and best practices need to be created and improved to protect students' data and privacy and to educate them about online safety. According to the GAO, it is not entirely known the extent to which cybersecurity incidents have impacted schools because school systems may not publicly disclose a cybersecurity breach [15]. K12 SIX has estimated that up to twenty times more K12 cyber incidents might occur than what is publicly disclosed [16]. Kamaludeen *et. al.* [76] have proposed a framework of standard guidelines for K12 school districts to close gaps in existing cybersecurity frameworks, which could be implemented to help schools improve incident response and disclosures.

The major stakeholders in protecting children's privacy and security–i.e. caregivers, teachers, school leaders, policymakers, EdTech, and cybersecurity professionals–must foster an environment that promotes good cyber hygiene and keeps kids safe online. The growing interest in cybersecurity (Fig. 1) along with expanding cybersecurity education initiatives [77]–[80] and a widening cybersecurity workforce gap [81] suggests a climate that might foster advancements in K12 cybersecurity education at all grade levels.

V. CONCLUSION

Overall, we have come to the following conclusions in our research: there are numerous threats to children as they learn online with EdTech and videoconferencing software, children

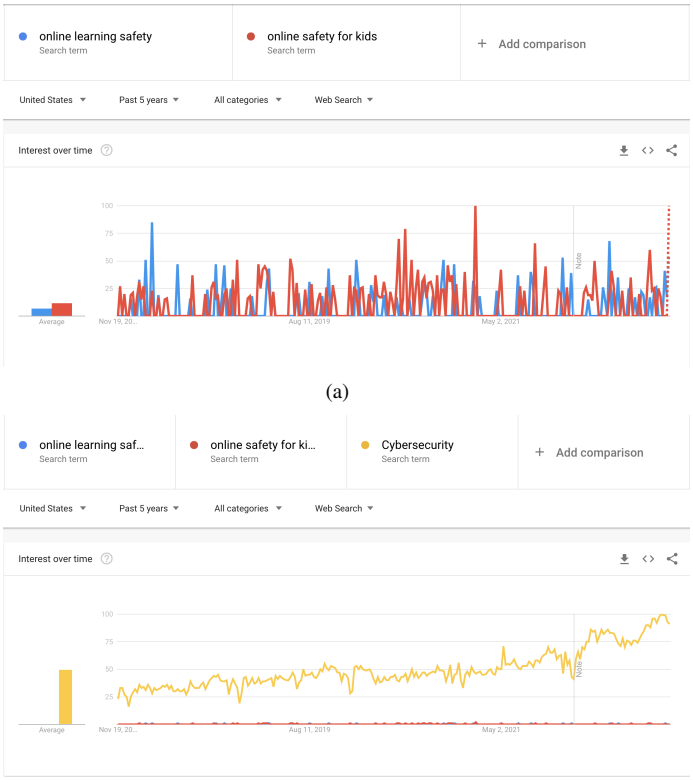

Fig. 1. Google Trends search keywords from November 2017 to November 2022. A value of 100 indicates peak popularity for the search term. (a) Search terms included in this data are "online learning safety" [82] and "online safety for kids". There was not enough data for the search term "online learning safety for kids". (b) Compared to the previous two search terms, an interest in cybersecurity appears to have been steadily growing over the past five years among Google Search users. [83]

need nationally standardized online safety and cybersecurity education in schools, governments and organizations must strengthen policies to protect children while using EdTech and videoconferencing tools to learn online, and game-based learning and training may be effective tools to teach children online safety.

In future studies, it would be useful to conduct a comprehensive and comparative review of EdTech's privacy and cybersecurity policies with respect to K12 students' data and privacy. Moreover, evaluating the cybersecurity tools employed by K-12 school systems to safeguard student privacy and security during online learning via EdTech and videoconferencing platforms would be prudent. Comparable research has been conducted in the context of families [84]–[87]. It would likewise be valuable to quantify to what extent cybersecurity is taught in the approximately 98,000 US K12 public schools [15] and how effective such programs are in boosting cybersecurity knowledge and improving students' online safety behavior. Finally, it would be worthwhile to conduct a large-scale and comprehensive survey of K12 students' cybersecurity knowledge and to what degree they have faced security and privacy threats while learning online using EdTech and videoconferencing platforms, while also taking into account various demographics. Answers to these open questions and issues may help to guide policymakers and school districts to improve both cybersecurity policies and practices and curriculum design.

References

[1] R. R. Zota and B. Granovskiy, "Remote learning for k-12 schools during the covid-19 pandemic. crs report r46883, version 3." *Congressional Research Service*, 2021.

[2] FBI. (2021) Internet crime report 2020. Accessed: 2022-11-09. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[3] ——. (2022) Internet crime report 2021. Accessed: 2022-11-09. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[4] ——. (2020) Cyber actors take advantage of covid-19 pandemic to exploit increased use of virtual environments. Accessed: 2022-11-09. [Online]. Available: https://www.ic3.gov/Media/Y2020/PSA200401

[5] CISA. (2020) Cyber threats to k-12 remote learning education. Accessed: 2022-11-09. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Cyber_Threats_to_K-12_Remote_Learning_Fact_Sheet_15_Dec_508_0.pdf

[6] M. B. Pasciak. (2021) Buffalo public schools recovering from ransomware attack. Accessed: 2022-11-09. [Online]. Available: https://www.govtech.com/education/k-12/buffalo-public-schools-recovering-from-ransomware-attack.html

[7] S. Travis. (2021) Broward schools warn 50k employees, students of data breach. Accessed: 2022-11-09. [Online]. Available: https://www.govtech.com/education/k-12/broward-schools-warn-50k-employees-students-of-d

[8] S. Tryens-Fernandes. (2022) Does your child have the flu? cases are increasing in alabama, prompting remote learning. Accessed: 2022-11-09. [Online]. Available: https://www.al.com/educationlab/2022/10/does-your-child-have-the-flu-cases-are-increasing-in-alabama.html

[9] J. G. Koomson. (2021) Rise of ransomware attacks on the education sector during the covid-19 pandemic. Accessed: 2022-11-09. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/rise-of-ransomware-attacks-on-the-education-sector-during-the-covid-19-pandemic

[10] H. Saleous, M. Ismail, S. H. AlDaajeh, N. Madathil, S. Alrabaee, K.-K. R. Choo, and N. Al-Qirim, "Covid-19 pandemic and the cyberthreat landscape: Research challenges and opportunities," *Digital Communications and Networks*, 2022.

[11] S. Prior and K. Renaud, "The impact of financial deprivation on children's cybersecurity knowledge & abilities," *Education and Information Technologies*, pp. 1–21, 2022.

[12] HRW. (2022) "how dare they peep into my private life?" children's rights violations by governments that endorsed online learning during the covid-19 pandemic. Accessed: 2022-11-09. [Online]. Available: https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments

[13] D. Harwell. (2022) Ftc to ed tech: Protecting kids' privacy is your responsibility. Accessed: 2022-11-09. [Online]. Available: https://www.ftc.gov/business-guidance/blog/2022/05/ftc-ed-tech-protecting-kids-privacy-your-responsibility

[14] UNICEF. (2020) Policy guidance on ai for children. Accessed: 2022-11-19. [Online]. Available: https://www.unicef.org/globalinsight/media/1171/file

[15] J. M. Nowicki, "Data security: Recent k-12 data breaches show that students are vulnerable to harm. report to the republican leader, committee on education and labor, house of representatives. gao-20-644." *US Government Accountability Office*, 2020.

[16] D. A. Levin, "The state of k-12 cybersecurity: Year in review – 2022 annual report," *K12 Security Information Exchange (K12 SIX)*, 2022.

[17] FBI. (2020) Fbi warns of child sexual abuse material being displayed during zoom meetings. Accessed: 2022-11-17. [Online]. Available: https://www.fbi.gov/news/press-releases/press-releases/fbi-warns-of-child-sexual-abuse-material-being-displayed-during-zoom-meetings

[18] ——. (2020) Child abductors potentially using social media or social networks to lure victims in lieu of an in-person ruse. Accessed: 2022-11-17. [Online]. Available: https://www.ic3.gov/Media/Y2020/PSA201015

[19] J. W. Patchin and S. Hinduja, "Cyberbullying among asian american youth before and during the covid-19 pandemic," *Journal of school health*, 2022.

[20] J. W. Patchin. (2021) Bullying during the covid-19 pandemic. Accessed: 2022-11-19. [Online]. Available: https://cyberbullying.org/bullying-during-the-covid-19-pandemic

[21] CISA. (2020) Cyber actors target k-12 distance learning education to cause disruptions and steal data. Accessed: 2022-11-17. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa20-345a

[22] FTC. (2022) Ftc to crack down on companies that illegally surveil children learning online. Accessed: 2022-11-19. [Online]. Available: https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-crack-down-companies-illegally-surveil-children-learning-online

[23] A. Wang, "Scrutinizing coppa: The privacy of our past, present, and future," *Joseph Wharton Scholars*, 2022.

[24] S. von Struensee, "Eye on developments in artificial intelligence and children's rights: Artificial intelligence in education (aied), edtech, surveillance, and harmful content," *EdTech, Surveillance, and Harmful Content (June 4, 2021)*, 2021.

[25] R. Nieva. (2020) Two children sue google for allegedly collecting students' biometric data. Accessed: 2022-11-19. [Online]. Available: https://www.cnet.com/tech/tech-industry/two-children-sue-google-for-allegedly-collecting-students-biometric-data/

[26] B. Auxier, L. Rainie, M. Anderson, A. Perrin, M. Kumar, and E. Turner. (2019) Americans and privacy: Concerned, confused and feeling lack of control over their personal information. Accessed: 2022-11-23. [Online]. Available: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

[27] K. Olmstead and A. Smith. (2017) What the public knows about cybersecurity. Accessed: 2022-11-23. [Online]. Available: https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/

[28] A. Srivastava. (2020) The case for privacy education in k–12. Accessed: 2022-11-23. [Online]. Available: https://iapp.org/news/a/a-case-for-privacy-education-in-k-12/

[29] E. R. Center. (2020) The state of cybersecurity education in k-12 schools. Accessed: 2022-11-09. [Online]. Available: https://cyber.org/sites/default/files/2020-06/The\%20State\%20of\%20Cybersecurity\%20Education\%20in\%20K-12\%20Schools.pdf

[30] S. S. Tirumala, A. Sarrafzadeh, and P. Pang, "A survey on internet usage and cybersecurity awareness in students," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016, pp. 223–228.

[31] J. W. A. Witsenboer, K. Sijtsma, and F. Scheele, "Measuring cyber secure behavior of elementary and high school students in the netherlands," *Computers & Education*, vol. 186, p. 104536, 2022.

[32] Y.-Y. Choong, M. F. Theofanos, K. Renaud, and S. Prior, ""passwords protect my stuff"—a study of children's password practices," *Journal of cybersecurity*, vol. 5, no. 1, p. tyz015, 2019.

[33] iKeepSafe. Ferpa 101 for edtech companies. Accessed: 2022-11-23. [Online]. Available: https://ikeepsafe.org/content/uploads/2017/01/FERPA-101-for-EdTech-iKeepSafe.pdf

[34] S. G. Urchambault, "Student privacy in the digital age," *BYU Education & Law Journal*, vol. 2021, no. 1, p. 6, 2021.

[35] D. Peterson, "Edtech and student privacy: California law as a model," *Berkeley Tech. LJ*, vol. 31, p. 961, 2016.

[36] D. S. Skowronski, "Coppa and educational technologies: The need for additional online privacy protections for students," *Georgia State University Law Review*, vol. 38, no. 4, p. 12, 2022.

[37] FTC. (2022) Policy statement of the federal trade commission on education technology and the children's online privacy protection act. Accessed: 2022-11-23. [Online]. Available: https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-education-technology-childrens-online-privacy-protection

[38] F. Bélanger, R. E. Crossler, J. S. Hiller, J.-M. Park, and M. S. Hsiao, "Pocket: A tool for protecting children's privacy online," *Decision Support Systems*, vol. 54, no. 2, pp. 1161–1173, 2013.

[39] State student privacy laws. Accessed: 2022-11-25. [Online]. Available: https://studentprivacycompass.org/state-laws/

[40] 117th Congress (2021-2022). (2021) K-12 cybersecurity act of 2021. Accessed: 2022-11-09. [Online]. Available: https://www.congress.gov/bill/117th-congress/senate-bill/1917/all-info

[41] J. Biden. (2021) Statement of president joe biden on signing the k-12 cybersecurity act into law. Accessed: 2022-11-09. [Online]. Available: https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/08/statement-of-president-joe-biden-on-signing-the-k-12-cybersecurity-act-into-law/

[42] R. Torchia. (2022) What will happen after cisa's k–12 cybersecurity act review? Accessed: 2022-11-13. [Online]. Available: https://edtechmagazine.com/k12/article/2022/02/what-will-happen-after-cisas-k-12-cybersecurity-act-review

[43] B. Wolford. What is gdpr, the eu's new data protection law? Accessed: 2022-11-23. [Online]. Available: https://gdpr.eu/what-is-gdpr/

[44] M. Orchison and K. Rigg. Data protection and privacy implications of online and remote learning. Accessed: 2022-11-23. [Online]. Available: https://www.cois.org/about-cis/perspectives-blog/blog-post/~board/perspectives-blog/post/data-protection-and-privacy-implications-of-online-and-remote-learning

[45] E. editorial staff. (2022) Edtech firms failing to protect children's data, say campaigners. Accessed: 2022-11-13. [Online]. Available: https://eandt.theiet.org/content/articles/2022/08/edtech-firms-fail-to-protect-childrens-data-campaigners-say/

[46] ICO. (2022) Introduction to the age appropriate design code. Accessed: 2022-11-13. [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code/

[47] S. Cavanagh. (2019) How gdpr is pressuring schools and ed-tech companies to improve data privacy. Accessed: 2022-11-13. [Online]. Available: https://marketbrief.edweek.org/marketplace-k-12/gdpr-pressuring-schools-ed-tech-companies-improve-data-privacy/

[48] K. P. Louise Hooper, Sonia Livingstone. (2022) Problems with data governance in uk schools: the cases of google classroom and classdojo. Accessed: 2022-11-13. [Online]. Available: https://digitalfuturescommission.org.uk/wp-content/uploads/2022/08/Problems-with-data-governance-in-UK-schools.pdf

[49] P. Bischoff. (2022) Where in the world is your child's data safe? 50 countries ranked on their child data protection legislation. Accessed: 2022-11-23. [Online]. Available: https://www.comparitech.com/blog/information-security/child-data-privacy-by-country/

[50] ——. (2021) 1 in 5 children's google play apps breach children's online privacy protection act rules. Accessed: 2022-11-23. [Online]. Available: https://www.comparitech.com/blog/vpn-privacy/app-coppa-study/

[51] GAO. (2022) Critical infrastructure protection: Additional federal coordination is needed to enhance k-12 cybersecurity. Accessed: 2022-11-19. [Online]. Available: https://www.gao.gov/products/gao-23-105480

[52] CISA. (2020) Cybersecurity recommendations for k-12 schools using video conferencing tools and online platforms. Accessed: 2022-11-19. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/CISA_Cybersecurity_Recommendations_for_K-12_Schools_Using_Video_Conferencing_S508C_2.pdf

[53] R. Al-Azawi, F. Al-Faliti, and M. Al-Blushi, "Educational gamification vs. game based learning: Comparative study," *International journal of innovation, management and technology*, vol. 7, no. 4, pp. 132–136, 2016.

[54] D. T. Smith and A. I. Ali, "You've been hacked: A technique for raising cyber security awareness." *Issues in Information Systems*, vol. 20, no. 1, 2019.

[55] M. Dark, J. Daugherty, R. Dark, H. Albright, D. Brown, M. Emry, and A. McCallen. (2021) Gencyber 5-year evaluation 2015-2019. Accessed: 2022-11-25. [Online]. Available: https://www.ftc.gov/legal-library/browse/policy-statement-federal-trade-commission-education-technology-childrens-online-privacy-protection

[56] T. West, "The synergy of intertwining grant activities: Cyber up! and gencyber girls," in *2022 ASEE Annual Conference & Exposition*, 2022.

[57] J. Seale and N. Schoenberger, "Be internet awesome: A critical analysis of google's child-focused internet safety program," *Emerging Library & Information Perspectives*, vol. 1, pp. 34–58, 2018.

[58] Google. (2022) Be internet awesome. Accessed: 2022-11-19. [Online]. Available: https://beinternetawesome.withgoogle.com

[59] S. Nguyen, D. DiPaola, and C. Breazeal. (2020) Family-friendly data privacy + ai activities: Interactive lessons to help kids learn and design with data privacy in mind. Accessed: 2022-11-23. [Online]. Available: https://www.media.mit.edu/posts/family-friendly-data-privacy-ai-activities-interactive-lessons-to-help-kids-learn-and-design-with-data-privacy-in-mind/

[60] Fordham. Privacy education. Accessed: 2022-11-23. [Online]. Available: https://www.media.mit.edu/posts/family-friendly-data-privacy-ai-activities-interactive-lessons-to-help-kids-learn-and-design-with-data-privacy-in-mind/

[61] Welcome to teaching privacy. Accessed: 2022-11-23. [Online]. Available: https://teachingprivacy.org/

[62] Resources for 3-11 year olds. Accessed: 2022-11-23. [Online]. Available: https://saferinternet.org.uk/guide-and-resource/young-people/resources-for-3-11s

[63] Resources for 11-19 year olds. Accessed: 2022-11-23. [Online]. Available: https://saferinternet.org.uk/guide-and-resource/young-people/resources-for-11-19s

[64] Be safer online! Accessed: 2022-11-23. [Online]. Available: https://www.netsmartzkids.org/

[65] About stop. think. connect. Accessed: 2022-11-23. [Online]. Available: https://www.stopthinkconnect.org/about

[66] P. Antonenko, Z. Xu, C. Wusylko, K. Dawson, S. Bhunia, A. Benedict *et al.*, "Engaging children in cryptology and cybersecurity learning and career awareness," in *2022 ASEE Annual Conference & Exposition*, 2022.

[67] S. Maqsood and S. Chiasson, "Design, development, and evaluation of a cybersecurity, privacy, and digital literacy game for tweens," *ACM Transactions on Privacy and Security (TOPS)*, vol. 24, no. 4, pp. 1–37, 2021.

[68] B. F. Faith, Z. A. Long, S. Hamid, O. F. Johnson, C. I. Eke, and A. Norman, "An intelligent gamification tool to boost young kids cybersecurity knowledge on fb messenger," in *2022 16th International Conference on Ubiquitous Information Management and Communication (IMCOM)*. IEEE, 2022, pp. 1–8.

[69] S.-S. Tseng, T.-Y. Yang, W.-C. Shih, and B.-Y. Shan, "Building a self-evolving imonsters board game for cyber-security education," *Interactive Learning Environments*, pp. 1–19, 2022.

[70] L. Thompson, N. Melendez, J. Hempson-Jones, and F. Salvi, "Gamification in cybersecurity education: The rad-sim framework for effective learn," in *European Conference on Games Based Learning*, vol. 16, no. 1, 2022, pp. 562–569.

[71] N. Percival, P. Rayavaram, S. Narain, and C. S. Lee, "Cryptoscratch: Developing and evaluating a block-based programming tool for teaching k-12 cryptography education using scratch," in *2022 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 2022, pp. 1004–1013.

[72] E. M. Dillon, C. Carpenter, J. Cook, T. D. Wills, and H. S. Narman, "A machine learning-based automatic feedback system to teach cybersecurity principles to k-12 and college students," in *2022 IEEE Global Humanitarian Technology Conference (GHTC)*. IEEE, 2022, pp. 219–225.

[73] S. Purnama, M. Ulfah, I. Machali, A. Wibowo, and B. S. Narmaditya, "Does digital literacy influence students' online risk? evidence from covid-19," *Heliyon*, vol. 7, no. 6, p. e07406, 2021.

[74] J. Chase, P. Uppuluri, E. Denny, B. Patterson, J. Eller, D. Lane, B. Edwards, and R. Onuskanich, "Steam powered k-12 cybersecurity education," in *Journal of The Colloquium for Information Systems Security Education*, vol. 7, no. 1, 2020, pp. 8–8.

[75] K. Dawson, P. Antonenko, Z. Xu, C. Wusylko *et al.*, "Promoting interdisciplinary integration of cybersecurity knowledge, skills and career awareness in preservice teacher education," *Journal of Technology and Teacher Education*, vol. 30, no. 2, pp. 275–287, 2022.

[76] M. Kamaludeen, S. Ismaeel, S. Asiri, T. Allen, and C. Scarfo, "A framework for cyber protection (fcp) in k-12 education sector," in *3rd Smart Cities Symposium (SCS 2020)*, vol. 2020. IET, 2020, pp. 239–244.

[77] NIST. (2022) National initiative for cybersecurity education (nice). Accessed: 2022-11-19. [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/nice

[78] USDE. (2022) Cybersecurity education. Accessed: 2022-11-19. [Online]. Available: https://cte.ed.gov/initiatives/cybersecurity

[79] C. I. Center. (2022) Initiatives — cyber.org. Accessed: 2022-11-19. [Online]. Available: https://cyber.org/initiatives

[80] ENISA. (2022) Awareness raising. Accessed: 2022-11-19. [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-education

[81] (ISC)2. (2022) (isc)2 cybersecurity workforce study 2022. Accessed: 2022-11-25. [Online]. Available: https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

[82] Y. Chen and W. He, "Security risks and protection in online learning: A survey," *The International Review of Research in Open and Distributed Learning*, vol. 14, no. 5, 2013.

[83] Google. (2022) Google trends. Accessed: 2022-11-13.

[84] A. K. Ghosh, C. E. Hughes, and P. J. Wisniewski, "Circle of trust: a new approach to mobile online safety for families," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–14.

[85] P. Wisniewski, A. K. Ghosh, H. Xu, M. B. Rosson, and J. M. Carroll, "Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety?" in *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 2017, pp. 51–69.

[86] A. K. Ghosh, "Taking a more balanced approach to adolescent mobile safety," in *Proceedings of the 19th International Conference on Supporting Group Work*, 2016, pp. 495–498.

[87] A. T. Pinter, A. K. Ghosh, and P. J. Wisniewski, "Going beyond cyberbullying: Adolescent online safety and digital risks," *Cyberbullying and Digital Safety: Applying Global Research to Youth in India*, 2022, book chapter, Library Press @ UF, USA.