Empowering Youth in The Digital Age with Cyber Security Education: Results of the Interviews with Secondary School Teachers in Wales

Maha Alotaibi
Computer Science and Informatics
Cardiff University
Cardiff, UK
AlotaibiM11@cardiff.ac.uk
0009-0002-5687-4308

Yulia Cherdantseva
Computer Science and Informatics
Cardiff University
Cardiff, UK
CherdantsevaYV@cardiff.ac.uk
0000-0002-3527-1121

Omer Rana
Computer Science and Informatics
Cardiff University
Cardiff, UK
RanaOF@cardiff.ac.uk
0000-0003-3597-2646

Catherine Teehan
Computer Science and Informatics
Cardiff University
Cardiff, UK
teehanc@cardiff.ac.uk
0000-0002-2359-0694

Abstract—As cyberthreats increasingly target vulnerable youth, the need for comprehensive cybersecurity education becomes more critical. Integrating cybersecurity into secondary school curricula offers a promising solution, equipping students with the necessary skills to identify and mitigate cyber risks. Despite the increasing number of cyber risks targeting young people, cybersecurity education in secondary schools is still in its early stages of development. This study investigates the perspectives of 27 secondary school teachers in Wales, United Kingdom, on incorporating cybersecurity education into their curricula. The qualitative insights gathered through semi-structured interviews reveal key challenges and opportunities, including a lack of resources, age-appropriate materials and pedagogical support for teaching cybersecurity. Our findings highlight a need for targeted educational reforms and closer collaboration between schools and cybersecurity professionals. Based on the interview results, we provide practical recommendations for educators, school administrators, and cybersecurity practitioners to enhance secondary cybersecurity education.

Keywords—*cybersecurity education, secondary school, secondary education, cybersecurity curriculum, cybersecurity skills, curriculum development, interviews, qualitative study*

I. INTRODUCTION

In today's online world, cybersecurity education has become critical due to the growing number of threats targeting young Internet users. Increased reliance on the Internet and social media exposes young people to cyber risks, including cyberbullying, data theft, harassment and online scams. Young people aged 13 to 15 often lack cybersecurity knowledge and are particularly vulnerable to these threats. In the United States, The FBI (Federal Bureau of Investigation, United States) reported 23,200 cases of internet scams targeting individuals under the age of 21 in 2023. These scams resulted in financial losses amounting to $ 70 million USD. These scams, which occurred in the USA, underscore the growing need for cybersecurity education in the United States and beyond [1]. A study by the National Crime Agency (NCA, United Kingdom) found that 20% of children aged 10 to 16 in the UK engage in illegal online activities, such as hacking, digital piracy, or using unauthorized software [2]. For example, this includes downloading software to access others' devices, attempting to hack protected servers or making purchases with stolen card information. The NCA highlights that a lack of awareness and early intervention can lead young individuals to escalate into more serious cybercrime offenses. However, access to structured cybersecurity education remains limited, particularly for students without prior advanced technical skills. The NCA urges parents and teachers to educate young people on the risks associated with cybercrime and to encourage them to develop their digital skills through legal and ethical pathways, such as cybersecurity training and ethical hacking programs. [2]. In the absence of specific instructional programs on cyber awareness, young people remain unaware to the distinction between legal and illegal online behaviours [3].

To combat this issue, it is imperative to introduce cybersecurity education in schools, focusing on young learners. This can help fill this knowledge gap. Students will be better prepared to make educated judgments when interacting with information online and will better understand the legal regulations surrounding digital behaviours. This educational approach reduces the risk of accidental involvement in cybercrime and fosters a culture of responsible and ethical internet use [4].

The overall computer science and cybersecurity education level has drastically increased over the past years [5]. While bachelor's and master's degree programmes at the university level have increasingly incorporated cybersecurity topics such as ethical hacking, digital forensics and risk management [5], secondary school curricula have not progressed at the same rate, often overlooking the need to teach students fundamental cybersecurity skills. Although cybersecurity is a

crucial educational topic, it remains largely absent from many school curricula worldwide [5].

According to the analysis, cybersecurity content is primarily confined to advanced computing courses, as stated by [6] and [7], leaving most students without basic cybersecurity education. The limited focus on cybersecurity education confines essential skills to a small group of advanced students, exposing the majority to cyber threats. As a result, poor cyber hygiene is prevalent, and practical guidance on integrating cybersecurity into the broader school curriculum remains insufficient [8].

Considering global challenges in cybersecurity education, governments worldwide have recognized the need to prepare young people better to combat cyber threats by equipping them with essential digital skills [3]. In line with these efforts, the UK Government introduced the National Cyber Security Strategy (NCSC) in 2016 and implemented the Cyber First initiative shortly after. The NCSC outlines a comprehensive plan to improve the UK's cybersecurity by promoting education, fostering innovation, and encouraging broader participation [3]. In Wales, implementing the Curriculum for Wales 2022 marks a significant shift in education, placing greater emphasis on digital literacy and cybersecurity skills [9]. This new curriculum allows educators to integrate cybersecurity education across different subjects, promoting a more comprehensive approach to digital safety. However, successfully implementing this framework relies heavily on teachers' proficiency in cybersecurity concepts and their ability to teach this content effectively.

Despite these initiatives, integrating cybersecurity curricula into the academic framework has faced considerable challenges. One of the primary issues with the school curriculum is the lack of resources and expertise among educators [10]. Many secondary school teachers lack the specialised knowledge and training to teach cybersecurity effectively, hampering their ability to prepare students for the emerging cyber threat landscape [11].

The primary goal of our study is to examine how cybersecurity is currently taught in Wales and explore how it could be better integrated into the curriculum. We focus on teachers' perspectives and challenges to inform educators, curriculum designers, and policymakers. We aim to answer three main research questions:

RQ1: What cybersecurity topics are currently covered in the secondary school curriculum?

RQ2: How do secondary school teachers recommend integrating cybersecurity into the curriculum, and what factors influence their chosen approach?

RQ3: What are the specific barriers teachers encounter when integrating cybersecurity education into the secondary curriculum in Wales?

To address these questions, we conducted semi-structured interviews with 27 computer science teachers from secondary schools across Wales, UK. This study makes three key contributions. First, we uncover the types of cybersecurity topics taught in Welsh secondary schools and examine how they are delivered. Second, we present new findings on the challenges teachers face. Finally, we offer practical recommendations for integrating cybersecurity more effectively into the new Curriculum for Wales [12].

II. LITERATURE REVIEW

This literature review explores the current state of cybersecurity education in secondary schools, focusing on the implications for cybersecurity curriculum design.

The existing literature reveals significant deficiencies in cybersecurity education within secondary schools, particularly regarding curriculum structure and teacher preparedness. Consequently, research has shown that while some schools are beginning to acknowledge the importance of cybersecurity, many still lack formalized programs or curricula dedicated to this critical area [13]. The International Society for Technology in Education (ISTE) survey indicates that only 42% of educators felt adequately prepared to teach cybersecurity [13]. The rapid development of technology and cyber threats complicate this lack of educator preparedness, creating a critical gap that undermines the efficacy of teaching cybersecurity in secondary schools.

Integrating cybersecurity into secondary school education faces enormous challenges. A workshop with teachers reported by [14] revealed that, while students are more knowledgeable about cybersecurity than their teachers, they lack an understanding of career pathways and online safety. Conversely, teachers lack adequate knowledge and resources to teach cybersecurity effectively [14]. Furthermore, a study by [15] found that many teachers feel insufficiently qualified to teach cybersecurity concepts due to a lack of confidence, knowledge, and limited training and resources provided by schools. These findings highlight a need for a well-designed curriculum to teach and motivate students towards cybersecurity pathways. Similarly, a study by [15] asserts that teachers must be equipped with the necessary knowledge through comprehensive lesson plans to integrate cybersecurity into schools successfully, as they often lack the requisite expertise, resources, and training.

Previous research highlights the importance of integrating cybersecurity into curricula for all areas of study [16]. Additionally, it emphasises the need for teachers' education programmes to meet current and future educational requirements [17]. While the need for robust cybersecurity education is universally acknowledged, the available approaches and resources vary widely, often disadvantageous to certain regions and school systems [18]. For example, a systematic literature review on cybersecurity education for children in [19] indicates the literature regarding cybersecurity education for children were what to teach, how to teach, and who should teach. Their study stated that the sample literature concerned with cyber security curriculum is highly fragmented,

lacking overall guidance for a comprehensive curriculum for schools to follow [19]. This inconsistency highlights an urgent need for coordinated efforts to standardize and enhance cybersecurity education globally.

Research has recently focused on infusing cybersecurity topics into existing courses rather than developing a comprehensive cybersecurity awareness framework [20]. Teachers' opinions regarding curriculum structure reveal a divide on whether cybersecurity should be taught as a standalone subject or integrated into existing courses [21] [22]. While some argue for its inclusion as a dedicated subject to ensure comprehensive understanding [23], others suggest an integrated approach may be more feasible within current curriculum constraints [23]. Further studies should integrate cybersecurity in non-technical classes, such as social studies and language arts, leveraging discussions, gamified activities, and content creation [4]. This debate is further complicated by the varying levels of teachers' qualifications, significantly impacting the effectiveness of cybersecurity education delivery [24].

In the UK, the teaching of cybersecurity in higher education faces challenges shaped by national policy, emphasizing the necessity for a comprehensive understanding that encompasses both the depth and breadth of cybersecurity knowledge [9]. Key issues include the quality and availability of educational resources, faculty members' competencies, and technical infrastructure adequacy [9]. The UK Government made significant progress in teaching young people cybersecurity by implementing the CyberFirst Initiative, a comprehensive plan to improve cybersecurity through education, innovation, and collaboration. Additionally, the NICE Cybersecurity Workforce Framework has been widely adopted as a guideline for defining cybersecurity roles and skills, ensuring that educational programs align with industry needs [25]. Similarly, the NIST Cybersecurity Framework provides structured guidelines for integrating cybersecurity education and risk management strategies into higher education curricula [26].

The educational system in Wales is undergoing substantial changes with the implementation of the Curriculum for Wales, which emphasizes the importance of digital literacy and cybersecurity skills [9]. This new curriculum framework allows educators to integrate cybersecurity education across various subjects, fostering a more cohesive approach to digital safety. However, the successful implementation of this framework relies heavily on teachers' understanding of cybersecurity concepts and their ability to deliver this content effectively.

Although multiple cybersecurity frameworks and innovations have been developed to establish a high standard of fundamental knowledge about cybersecurity, critical challenges remain in delivering rigorous cybersecurity content. This study aims to explore the urgent need for improved cybersecurity education in secondary schools and analyse how current curricula fall short in preparing teachers for the challenges of teaching cybersecurity in secondary schools. It will examine the differing opinions on the most effective curriculum structure, highlighting the benefits of both standalone courses and integrated approaches. Additionally, the research will investigate the specific barriers teachers face in integrating cybersecurity education into the secondary curriculum in Wales and identify areas for improvement in the current curriculum.

III. METHODS

The research investigates the challenges and strategies teachers face in integrating cybersecurity into the secondary school curriculum. Semi-structured interviews were conducted in person and online with 27 secondary school teachers in Wales. The data was analyzed using thematic analysis [27], which helped frame and interpret the findings. The data was anonymized for the analysis. Ethical implications were considered, and the required approval for conducting this data collection was obtained.

A. Participants Profiles

Participants were selected based on their experience in teaching or learning computer science or Information Communication Technology (ICT) and were recruited from a diverse range of secondary schools in Wales.

Teachers were selected based on their direct involvement in teaching subjects related to cybersecurity or ICT. This included those who teach core computer science courses and those integrating digital literacy into their curriculum. Heads of schools and ICT or digital technology department leaders provided insights into institutional policies, resource allocation, and support structures for teaching cybersecurity. Curriculum coordinators offered perspectives on curriculum development and implementation strategies. Additionally, a leader of an outreach programme provided insights into the importance of practical experience in bridging the gap between theoretical knowledge and real-world applications. Table I provides a detailed overview of each participant's profile, including *Alias, the identifier used to protect individual identity in the qualitative study, their role, years of experience, educational background at university, and cybersecurity background.

TABLE I. Profile of Study Participants

Alias	***Role***	***Experience***	***Background***	***Cybersecurity background***
T1	Schoolteacher	[5-10] years	ICT	Yes
T2	Schoolteacher	[10-20] years	Electronics.	No
T3	Headmaster of computer science department	[5-10] years	ICT	No

*Alias	Role	Experience	Background	Cybersecurity background
T4	Leader of outreach program	[0-5] years	Chemistry	No
T5	Tutor	[0-5] years	ICT	No
T6	Schoolteacher	[0-5] years	Game art design	No
T7	Schoolteacher	[10-20] years	Information systems.	No
T8	Schoolteacher	[0-5] years	Multimedia	Yes
T9	Schoolteacher	[10-20] years	Business information systems.	No
T10	Headmaster for ICT department	[0-5] years	ICT	No
T11	Schoolteacher	[10-20] years	Chemical engineering.	No
T13	Schoolteacher	[0-5] years	French language	No
T14	Schoolteacher	[0-5] years	Media production	No
T15	Schoolteacher	[0-5] years	Systems analysis	No
T16	Schoolteacher	[10-20] years	Marketing and media	No
T17	Schoolteacher	[10-20] years	Sports	No
T18	Schoolteacher	[5-10] years	Forensic science	No
T19	Schoolteacher	[10-20] years	Computing informatics	Yes
T20	Schoolteacher	[5-10] years	Computer Science	Yes
T21	Schoolteacher	[20-30] years	Manufacturing technology	No
T22	Headmaster	[20-30] years	Sport	No
T23	Schoolteacher	[0-5] years	Physics	No
T24	Schoolteacher	[10-20] years	Business	No
T25	Schoolteacher	[5-10] years	Chemistry	No
T26	Headmaster of ICT	[10-20] years	IT	Yes
T27	Schoolteacher	[10-20] years	Psychology in French	No

IV. RESULTS

In this section, we present our findings from the interviews on cybersecurity topics taught, the strategies and resources used, and recommendations for integrating cybersecurity into the curriculum.

A. Integrate cybersecurity into the curriculum (RQ1)

While there is general agreement on the importance of incorporating cybersecurity into secondary school curriculum, teachers primarily cover fundamental principles of cybersecurity, online safety, digital citizenship, and the topics discussed below. Password security: Teachers consistently reported the importance of effectively creating and managing strong passwords. T15 stated: *"We make sure the students understand how to create strong passwords and use password managers, but we don't go into the technical aspects of why it's important."* This response suggests a focus on practical and technical instruction over theoretical aspects. Privacy and data protection: Students are introduced to basic privacy and data protection concepts, particularly on social media and websites; however, these topics are only briefly covered. Although these lessons aim to raise awareness about the importance of data protection, most teachers acknowledge that they do not delve into the more technical aspects of cybersecurity, such as encryption or data security protocols. For example, T13 explained: *"We teach them about privacy settings and how to protect their personal information online, but we don't go into encryption or the technical side of data protection."* Similarly to T15, this quote highlights the tendency to prioritise practical, user-level privacy settings over deeper, technical concepts such as encryption. Advanced Topics and Their Limited Coverage: Although basic online safety is commonly taught, the interviewees stressed the lack of coverage of more technical cybersecurity topics, such as encryption, ethical hacking, and network security. This lack of depth in technical topics points to a broader issue where students may learn about cybersecurity in theory but lack the practical skills needed to engage with the digital world safely and ethically. T14 explained: *"We mention encryption when discussing privacy, but we don't go deep into how encryption works or the different types of encryption methods."* Overall,

teachers suggest bringing topics such as malware, networking, password security, cybersecurity threats, phishing, and social engineering into the curriculum. Table II summarises the topics the interviewees proposed to be covered at the secondary school level.

TABLE II. Overview of Cybersecurity Topics

Topic	***No Teachers***	***Percentage***	***Quote***
Malware	19	70%	*"We need to teach what threats are out there and the prevention methods already available." (T1)*
Networking	15	55%	*"We talk about networks and general security, including how to protect your network physically." (T10)*
Password Security	16	60%	*"Every pupil needs to understand the basics of having a secure password or using a password manager." (T10)*
Cybersecurity Threats	15	56%	*"There are not just malicious threats aimed at financial gain; we also need to consider sabotage." (T5)*
Phishing and Social Engineering	14	52%	*"Many students don't have email accounts yet, so they might not understand what a phishing email looks like." (T13)*

B. Integrate cybersecurity into the curriculum (RQ2)

The integration of cybersecurity education into the secondary school curriculum presents a range of challenges and opportunities. Based on the interviews, teacher preferences are divided among standalone subjects, ICT units and cross-curricular integration. However, each approach brings distinct advantages and challenges that must be critically evaluated regarding feasibility, effectiveness, and long-term impact on student outcomes. Based on the interviews, four critical approaches for integrating cybersecurity into schools were identified and discussed below.

Cross-curricular integration: Five out of 27 teachers supported integrating cybersecurity concepts like digital citizenship and data privacy into humanities subjects and social sciences, using subjects such as social studies and business. For example, a social studies teacher (T26) mentioned using cybersecurity-related current events, such as data breaches or election interference, to teach about civic responsibility and digital citizenship. It was suggested that cybersecurity should not be seen only as technical knowledge but as an integral component of larger ethical conversations to make it more relevant for all students. T3 summarized the benefit of this approach, stating that *"if we teach cybersecurity as standalone, it's limited to students who choose ICT. But if we embed it into multiple subjects, everyone gets exposure to it."*

Integration into STEM subjects for deeper technical understanding: Similarly, five out of 27 teachers preferred cybersecurity integration within STEM subjects. This approach, which seeks to link topics such as encryption with mathematical concepts such as modular arithmetic and prime factorization, aligns well with the technical topics within cybersecurity. By embedding cybersecurity within mathematics and science, students will likely better understand the technical concepts directly applicable to real-world scenarios. T23 discussed integrating cybersecurity into lessons on the Internet of Things (IoT) and explaining how interconnected devices create new vulnerabilities.

Standalone subject: Six out of 27 teachers supported creating a standalone cybersecurity subject, emphasizing the topic's complexity as justification. Teachers in this group argued that cybersecurity is far too complex to be adequately addressed in just one or two lessons embedded within other subjects. T8 stated, *"Cybersecurity should be treated equally as subjects like math or science. It's a fundamental part of the digital world our students will inherit."*

A unit within ICT: For teachers who did not view cybersecurity as a standalone subject, the most common suggestion was to deliver it as a focused unit within the ICT or computer science curriculum. Seven out of 27 teachers preferred incorporating cybersecurity into ICT units, embedding it into an already established course structure. They felt this would allow for deeper exploration of cybersecurity topics without overburdening schools that may lack the resources for an entire course. T7 used this model by bringing in guest speakers from the industry to provide students with insights into real-world cybersecurity challenges.

C. Barriers teachers encounter when integrating cybersecurity education into the secondary curriculum (RQ3)

Teacher confidence and knowledge gap: Table I shows that 5 out of 27 teachers have a background in cybersecurity or relevant experience. This result highlights teachers' lack of confidence when delivering more technical cybersecurity topics. This lack extends beyond mere "technical skills" and addresses a broader array of deficiencies, such as a lack of familiarity with complex concepts and training. T21 commented that while teachers feel comfortable discussing online safety, they lack confidence in addressing the more technical aspects of cybersecurity.

Similarly, T9 mentioned that while he is confident teaching basic topics such as social engineering and malware, his confidence declines with technical concepts such as SQL

injection and penetration testing. He remarked, *"I'd love to do more practical things like penetration testing, but that's where my confidence starts to slip away."* T6 expressed similar sentiments. This knowledge gap prevents the introduction of more advanced cybersecurity topics, leaving students with only a basic grasp of cybersecurity.

Lack of training and resources: Teachers commonly struggle with limited access to appropriate teaching resources and lack sufficient training. The interviewees noted that they lack training in advanced cybersecurity topics, making them uncomfortable teaching beyond the basics of online safety and phishing. Access to technical resources is also a problem. Several teachers mentioned that their schools lack the necessary computing infrastructure for practical cybersecurity lessons. T6 pointed out that the lack of physical computers and software makes it difficult to demonstrate attacks or run simulations: *"We don't have the equipment to do things like demonstrate virtual attacks, which limits what we can teach."*

Additionally, internet filtering policies in some schools restrict students from accessing critical content needed for cybersecurity lessons. T10 shared that students are often blocked from searching for terms such as SQL injections, which are part of the curriculum because they are flagged as unsafe.

Curriculum design and lack of guidance: Many teachers identified time constraints and a lack of flexibility as key curriculum limitations. For instance, T9, who has experience teaching at both primary and secondary levels, noted that the Welsh curriculum focuses more on programming, leaving little room for dedicated cybersecurity lessons: *"The curriculum is heavily focused on programming, which means we don't have enough time to cover cybersecurity properly."*

Additionally, clear guidance on topics such as ethical hacking or data encryption and how to integrate them into existing subjects is often lacking. T21 suggested that cybersecurity is addressed in the curriculum superficially, lacking in-depth content, a structured framework, detailed lesson plans, or progression guidelines. It does not provide an effective guide for teachers. T21 explained: *"We get a bit of cybersecurity here and there, but there's no clear framework for teaching it."*

V. DISCUSSION

The analysis of 27 interviews with secondary school teachers with technical and non-technical backgrounds revealed their diverse perspectives on integrating cybersecurity into secondary school curricula. These findings align with previous research highlighting the importance of addressing the current inadequacies in cybersecurity education [28] [29]. While the study indicates enthusiasm among teachers for incorporating cybersecurity into their lessons in various subjects, it also reveals practical challenges such as current curriculum constraints and insufficient training opportunities. Many teachers struggle to find time to introduce cybersecurity concepts within an already packed curriculum regarding the lack of support for educators., echoing findings from Pencheva et al. [14]

A key finding from the interviews is the divergence of opinion on whether cybersecurity should be taught as a standalone subject or incorporated into existing courses. The teachers with a technical background in ICT or computer science generally preferred a standalone approach, viewing cybersecurity as a critical area that requires in-depth exploration due to its complexities. This perspective supports the importance of teaching practical skills, such as penetration testing and ethical hacking, that are essential in the cybersecurity field [19]. However, the standalone subject approach presents significant challenges related to curriculum overload, as secondary school schedules are highly structured, leaving limited room for additional subjects. Conversely, teachers from non-technical backgrounds preferred integrating cybersecurity across various subjects, embedding it into courses such as social studies and business. This view aligns with findings from Yusuf [28], who noted that a multidisciplinary approach enhances both graduates' soft skills, such as teamwork and problem-solving, and their practical knowledge in cybersecurity. However, teachers expressed concerns that existing curricula often lack the practical focus necessary to adequately prepare students for real-world challenges. As the literature suggests, many educational institutions struggle to design effective cybersecurity curricula, which often remain generic and theoretical [16]. Despite these differing opinions, considerable barriers remain in delivering effective cybersecurity education. The lack of confidence in delivering cybersecurity content, exacerbated by insufficient professional development and a curriculum lacking clear guidance. This conclusion mirrors the findings of Chen et al. [29], which highlight similar concerns among educators in the field. We recommend implementing structured professional development programs that focus on enhancing teachers' practical skills and content knowledge. Such programs should align with the conclusions drawn by Holley et al. [22], who emphasize the importance of targeted training in building educators' confidence and competence in delivering cybersecurity education effectively. To address the challenges identified in cybersecurity education, there is a pressing need for a structured curriculum that provides clear guidance on teaching cybersecurity, that offers comprehensive guidance on effective teaching practices. This curriculum should be accompanied by robust professional development programs that provide hands-on training and ongoing support, therefore providing teachers with the essential skills and information required for efficient teaching. Additionally, in light of these challenges, we recommend the establishment of a centralized repository for high-quality cybersecurity teaching materials and resources. This initiative should leverage successful models that demonstrate effective frameworks for resource sharing among educators, facilitating improved access to essential teaching tools.

VI. CONCLUSION

As this study indicates, integrating cybersecurity into secondary school curricula is both complex and essential.

The varied opinions regarding how best to teach cybersecurity emphasizes the need for flexibility in curriculum design. Some teachers advocate for a dedicated subject, believing this approach will offer the depth and focus to prepare students for future cybersecurity challenges. Others prefer cross-curricular integration, embedding cybersecurity into subjects like social studies and business, making it more accessible to non-technical students.

Teachers also face considerable barriers, including insufficient knowledge, outdated or inadequate IT infrastructure, and a lack of specialized training. Addressing these challenges will require a concerted effort to provide professional development opportunities for teachers and more structured support within the curriculum.

To adequately prepare students for a digital future, cybersecurity education must be adapted to address the challenges discussed in this paper. A combination of more focused and better-defined approaches to teaching cybersecurity topics in STEM subjects with cross-curricular integration, supported by accessible teaching and learning resources developed with the support from cybersecurity professionals and academics, and provision of ongoing cybersecurity education training for teachers, will offer a balanced way forward. Only through these efforts could we ensure that all students, regardless of their chosen field, have the foundational knowledge and skills to navigate and contribute to an increasingly digital and interconnected world.

REFERENCES

[1] A. I. Ajibade, "Common online scams targeting teenagers." [Online]. Available: https://www.internetmatters.org/hub/expert-opinion/common-online-scams-targeting-teenagers/. Accessed: Sep. 02, 2024.

[2] N. C. Agency, "Protecting the public from serious and organised crime." [Online]. Available: https://www.nationalcrimeagency.gov.uk/news/one-in-five-children-found-to-engage-in-illegal-activity-online. Accessed: Jun. 07, 2024.

[3] N. C. Agency, "Cyber choices: Helping young people make informed choices about cybercrime." [Online]. Available: https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices. Accessed: Aug. 04, 2024.

[4] Z. Kilhoffer, Z. Zhou, F. Wang, F. Tamton, Y. Huang, P. Kim, T. Yeh, and Y. Wang, "How technical do you get? i'm an english teacher": Teaching and learning cybersecurity and ai ethics in high school," in *2023 IEEE symposium on security and privacy (SP)*, pp. 2032–2032, IEEE, 2023.

[5] M. Jalil, N. H. Ali, F. Yunus, F. A. M. Zaki, L. H. Hsiung, and M. A. Almaiah, "Cybersecurity awareness among secondary school students post covid-19 pandemic," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 37, no. 1, pp. 115–127, 2024.

[6] M. Alotaibi, Y. Cherdantseva, O. Rana, and C. Teehan, "Enhancing cybersecurity education in secondary schools: a cybok-based analysis and strategic approach," in *INTED2024 Proceedings*, vol. 1, pp. 5096–5104, 2024.

[7] O. Stepney and J. Allison, "Cyber security in english secondary education curricula: A preliminary study," in *SIGCSE 2023 - Proceedings of the 54th ACM Technical Symposium on Computer Science Education*, vol. 1, pp. 193–199, 2023.

[8] D. Ondrušková and R. Posṕıšil, "The good practices for implementation of cyber security education for school children," *Contemporary Educational Technology*, vol. 15, no. 3, 2023.

[9] W. Government, "Introduction to curriculum for Wales guidance." [Online]. Available: https://hwb.gov.wales/curriculum-for-wales/introduction-to-curriculum-for-wales-guidance/. Accessed: Aug. 02, 2024.

[10] T. Crick, C. Knight, R. Watermeyer, and J. Goodall, "The impact of covid-19 and 'emergency remote teaching' on the uk computer science education community," ACM *International Conference Proceeding Series*, pp. 31–37, 2020.

[11] J. Idziorek, J. Rursch, and D. Jacobson, "Security across the curriculum and beyond," in *Proceedings - Frontiers in Education Conference, FIE*, no. 3, pp. 1–6, 2012.

[12] N. C. S. Centre, "Resources for schools." [Online]. Available: https://www.ncsc.gov.uk/information/resources-for-schools. Accessed: Oct. 14, 2024.

[13] ISTE, "Educator preparation in cybersecurity: A survey report." [Online]. Available: https://iste.org/standards/educators. Accessed: Jul. 04, 2024.

[14] D. Pencheva, J. Hallett, and A. Rashid, "Bringing cyber to school: Integrating cybersecurity into secondary school education," Technical Report 1, University of Bristol, 2020.

[15] S. V. Solms and R. V. Solms, "Towards cyber safety education in primary schools in Africa," in *Proceedings of the 8th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2014*, vol. 3, pp. 185–197, 2014.

[16] S. Syarova and S. T.-S., "Cybersecurity issues in the secondary and higher education systems' curricula," vol. 5114, 2023.

[17] A. Martin and J. Collier, "Beyond awareness: Reflections on meeting the interdisciplinary cyber skills demand," in *Cyber Security Education*, pp. 55–73, Routledge, 2020.

[18] R. B. Sağlam, V. Miller, and V. N. Franqueira, "A systematic literature review on cyber security education for children," *IEEE Transactions on Education*, vol. 66, no. 3, pp. 274–286, 2023.

[19] M. Khader, M. Karam, and H. Fares, "Cybersecurity awareness framework for academia," *Information*, vol. 12, no. 10, p. 417, 2021.

[20] M. A. Ayanwale, I. T. Sanusi, R. R. Molefi, and A. O. Otunla, "A structural equation approach and modelling of pre-service teachers' perspectives of cybersecurity education," *Education and Information Technologies*, vol. 29, no. 3, pp. 3699–3727, 2024.

[21] A. Lodgher, J. Yang, and U. Bulut, "An innovative modular approach of teaching cyber security across computing curricula," in *2018 IEEE Frontiers in Education Conference (FIE)*, pp. 1–5, IEEE, 2018.

[22] J. Bernd, D. Garcia, B. Holley, and M. Johnson, "Teaching cybersecurity: Introducing the security mindset," in *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 2*, pp. 1195– 1195, 2022.

[23] N. Ahmad, P. A. Laplante, J. F. DeFranco, and M. Kassab, "A cybersecurity educated community," *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 3, pp. 1456–1463, 2021.

[24] S. Yusif and A. Hafeez-Baig, "Cybersecurity policy compliance in higher education: a theoretical framework," *Journal of Applied Security Research*, vol. 18, no. 2, pp. 267–288, 2023.

[25] National Institute of Standards and Technology (NIST), "Nist cybersecurity framework." https://www.nist.gov/cyberframework, 2018. [Accessed: Feb. 10, 2024].

[26] National Initiative for Cybersecurity Education (NICE), "Nice cybersecurity workforce framework." https://niccs.cisa.gov/workforce-development/nice-framework, 2020. [Accessed: Feb. 10, 2024].

[27] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[28] M. Erickson and P. Kim, "Designing cybersecurity curriculum: Exploring the need for industry certifications and experiential learning.," *Issues in Information Systems*, vol. 22, no. 4, 2021.

[29] W. Chen, Y. He, X. Tian, and W. He, "Exploring cybersecurity education at the k-12 level," in *SITE Interactive Conference*, pp. 108–114, Association for the Advancement of Computing in Education (AACE), 2021.