Cybersecurity in Online Learning: Innovations for Teacher Training and Empowerment

Walter Buyu, eKRAAL Innovation Hub. E-mail: walterbuyu@e-kraal.com

Betty Ogange, Commonwealth of Learning. E-mail: bogange@col.org

Abstract

Recent technological advances in teaching and learning provide dynamic tools required to meet the educational needs of the digital era. However, teachers and other educators are increasingly experiencing cyber threats while teaching online, thereby affecting the quality of teaching as well as learning outcomes. In recent times, there have been reports of learning disruption caused by cybercriminals using attacks like ransomware, denial of service and data theft. In this context, teachers need to be able to harness the right tools, resources, and instructional practices to ensure not only continuity but also quality and effective learning. In this paper, we use the Cybersecurity Training for Teachers course series as a detailed case study to determine the cybersecurity challenges that educators faced when they moved their classes online, and how the knowledge and skills gained from the training helped to address them. The course series, offered by COL over a period of 2 years, attracted more than 7000 participants from 96 countries. Drawing from participant surveys, the paper presents an assessment of the perceived pedagogical impact of specific cyber threats. Finally, we propose innovations for teacher training and on-going empowerment in cybersecurity, to minimise the negative impact of cyber threats on online teaching and learning.

1. Introduction

The use of ICT in the education sector has increased globally over the last few decades, becoming an integral part of teaching and learning (Fouad, 2021). This upward trajectory is expected to continue with investments in education technology projected to hit $350 billion by 2025 (Li & Lalani, 2020). Developing countries have not been left behind in tapping into technological solutions for learning. The increasing affordability of ICT solutions has resulted in the adoption of digital learning in developing countries (von Solms & von Solms, 2014). However, the uptake of technology in schools has created new risks, more so around the human factor (Richardson et al., 2020). This has been further exacerbated by the rapid technological changes that teachers are not yet abreast with (Amankwa, 2021).

Increased digitisation in education introduces cybersecurity challenges (Fouad, 2021) across all levels of learning institutions including primary schools (von Solms & von Solms, 2014), secondary schools (Ivy et al., 2019), and colleges and universities (Fouad, 2021). The challenges include malware, ransomware, phishing, DoS, unauthorised disclosure, plagiarism, privacy, and protecting identity data (Impact Networking, 2021; Pusey & Sadera, 2011). Schools are targeted because of the valuable data they hold on students, parents, alumni, faculty, staff, partners, and research (Fouad, 2021; Ivy et al., 2019), which is lucrative, fetching up to $265 per record while credit card goes for $5 (Impact Networking, 2021).

The causes of attacks can be pointed to human and technical lapses. Students, faculty, and staff sometimes use personal devices to handle school data. The security of these computers might not be sufficient to protect the information accessed (Richardson et al., 2020). Learners in cyberspace might not be aware of the dangers therein pertaining to their personal safety and data (Pusey & Sadera, 2011; von Solms & von Solms, 2014) given on average the awareness among internet users is moderate to low (Amankwa, 2021). Young students not only have knowledge gaps but also miss adult support in keeping them safe online (Pencheva et al., 2020). Technically, there are inadequate security measures in place to protect the diverse set of data - academic, research, medical, banking, accommodation, etc. - that are in these institutions (Fouad, 2021; Impact Networking, 2021).

The consequences of cyberattacks include loss of data, slow or no access to computer systems, cyber-bullying, exposure to inappropriate content, disruption of classes, cancellation of exams, financial losses, and legal action (Cybersecurity and Infrastructure Security Agency, 2020; Fouad, 2021; Richardson et al., 2020). Repeat incidents have been observed pointing to a potential failure to learn from previous attacks (Impact Networking, 2021).

Despite holding invaluable information, schools have insufficient resources to handle cybersecurity (Ivy et al., 2019). They have inadequate funding, expertise, and capacities to prepare for cyber threats (Fouad, 2021). Thus, education ranks low in the security index by sector despite being among the top targeted segments (Impact Networking, 2021). It is clear that the use of technology can result in physical and emotional harm to users, their data and organisations (Pusey & Sadera, 2011). Therefore, teachers should be equipped with cybersecurity knowledge to safely apply their digital skills in teaching and learning (UNESCO, 2018).

This paper uses the Cybersecurity Training for Teachers course series as a detailed case study to determine the cybersecurity challenges that educators faced when they moved their classes online, and how the knowledge and skills gained from the training helped to address them. The course series, offered by the Commonwealth of Learning (COL) over a period of 2 years, attracted more than 7000 participants from 96 countries. Drawing from participant surveys, the paper presents an assessment of the perceived pedagogical impact of specific threats. Finally, we propose innovations and policy considerations for teacher training and on-going empowerment in cybersecurity, to minimise the impact of cyber threats on online teaching and learning. The next section provides the background to the Cybersecurity Training for Teachers course series. Section 3 describes the design and development of the courses and the methodology used to collect and analyse data. Section 4 examines the pedagogical impact of cyberattacks while Section 5 assesses the impact of the training. Section 6 details the innovations for teacher training and empowerment followed by a conclusion in Section 7.

2. Background

Digital learning has increased use of technology among teachers and students (Sailer et al., 2021). Teachers have leveraged technology to take roll calls, interact with students efficiently and effectively, and share learning resources. Additional benefits have been observed in online learning including higher retention of information and reduced time in teaching. It is anticipated that online learning will be an integral part of school education with some educators already adopting the blended approach of online and e-learning post-pandemic (Li & Lalani, 2020). Thus, it is essential that they use technology securely (Fraillon et al., 2014).

Teachers should understand the basics of cybersecurity as they use the digital space for teaching and learning (UNESCO, 2018). This is not only for their own safety but that of their students as well, many of whom might not be fully aware of the dangers in cyberspace. They tend to disregard online safety rules, thereby finding themselves in situations that teachers and parents do not fully understand (Pencheva et al., 2020). Most teachers have limited knowledge in cybersecurity, making it a challenge to enhance online safety when teaching and learning (von Solms & von Solms, 2014). While preservice teachers learn to integrate technology into instruction, they are not prepared to model or teach cybersecurity due to inadequate knowledge and teaching skills in this area. Consequently, they are unable to identify threats to themselves, their students, and institutions (Pusey & Sadera, 2011). On the other hand, schools have limited budget and resources since government support in cyber safety in schools is lacking or minimal especially in most developing countries. As a result, there is no cybersecurity curricula or extramural for cyber safety education (von Solms & von Solms, 2014).

Covid-19 disrupted learning affecting nearly 1.6 billion learners in more than 190 countries. The closure of learning spaces affected 99 per cent of low and lower-middle income countries (United Nations, 2020). The pandemic necessitated a shift to remote learning thereby accelerating the adoption of online learning even though institutions were not prepared with the right skills and infrastructure (Fouad, 2021; Li & Lalani, 2020). Schools deployed learning management systems and social media for online teaching-learning system (Garg et al., 2020), emphasising the role of technology in teaching and learning (Sailer et al., 2021). Teachers would opt for asynchronous learning so they focus on learners rather than learning new pedagogy or technology. However, they would still need to post materials online for students to access at their own time. They would also schedule online appointments to engage students (Daniel, 2020). The demand for remote learning resulted into an increase in distributed denial of service (DDoS) and virus targeting online learning platforms (Fouad, 2021). Similarly, there was a spike in disruption of classes held via video conferencing where verbal harassment, display of pornography and violent images, and doxing attendees was rife (Cybersecurity and Infrastructure Security Agency, 2020). It was, therefore, necessary to upskill teachers on cybersecurity considering social engineering was and is the leading cause of breaches (Impact Networking, 2021).

Teachers should possess skills to handle cybersecurity issues in the classroom (Richardson et al., 2020). Therefore, it is vital to create cybersecurity courses with content that educators can easily grasp and put into use (Ivy et al., 2019). Some of the available courses such as Future Learn's *Introduction to Cybersecurity for Teachers* (Future Learn, n.d.) are somewhat technical in nature and require payment. Educators with no relevant background and finances might miss out on such courses as they need to spend more time and money (Amankwa, 2021).

Supporting teachers' readiness is important in realising resilient education systems (United Nations, 2020). COL developed two cybersecurity courses – Cybersecurity Training for Teachers (CTT) and Advanced Cybersecurity Training for Teachers (ACTT) – to equip teachers, teacher educators and other education practitioners with the skills and knowledge that they need to protect themselves and their students online, as well as create awareness for parents and other stakeholders in digital learning. Both courses considered the pressing cybersecurity challenges, skills needed

by educators, and their knowledge level. The CTT and ACTT courses were each offered for free in two iterations. Each offer lasted a period of four weeks.

3. Design and Development of Courses in Cybersecurity

Target Audience

Most teachers may be unaware of cyberthreats, as they have no knowledge and experience in cybersecurity. Therefore, they should be grounded in cybersecurity since they teach and advise students as well as observe changed behaviour (Pencheva et al., 2020; von Solms & von Solms, 2014). The CTT and ACTT courses targeted teachers in primary schools, secondary schools, and tertiary institutions. Education practitioners from ministries of education were also free to join. However, from the pre-course survey conducted, the course participants included those in early childhood education and a few individuals outside of the teaching profession. This demographic underscored the significance of the course and the importance of adapting content for a wider audience. Most of the participants were from developing countries in the Commonwealth. A considerable number of schools in these countries are underfunded and may not have the resources to train teachers on cybersecurity (von Solms & von Solms, 2014). They would benefit most from these courses to defend themselves, their learners and institutions, and inspire their students to join the cybersecurity workforce (Ivy et al., 2019; Richardson et al., 2020).

Content

A holistic approach was adopted in developing content for the courses as teachers typically engage with students, parents and other stakeholders (Amankwa, 2021).

The CTT course was designed for teachers, teacher educators and education practitioners who were likely to have college-level education but no experience in cybersecurity. The course was structured into four modules:

i. *Introduction to Cybersecurity*: covered the basic concepts to ensure participants could connect cybersecurity principles to their classroom practice (Ivy et al., 2019).
ii. *Cybersecurity Threats and Mitigation*: was designed to help participants understand cybersecurity threats, vulnerabilities, attacks, and mitigation techniques.
iii. *Best Practices*: it was vital to have general best practices and those specific to video conferencing, as the technology was prevalent during the pandemic (Cybersecurity and Infrastructure Security Agency, 2020).
iv. *Cyber Safety for Students*: focused on student online protection; online risks; the role of students, teachers, parents, and guardians; incorporating cybersecurity in the classroom; and laws on child online protection.

The ACTT course was designed for teachers and teacher educators who had either completed the introductory course, CTT, or had other relevant background. The course was structured into four modules:

i. *Advanced Cyber Attacks in Online Learning*: covered attack vectors; wireless and mobile device attacks; application and web attacks; and internal threats. The aim was to acquaint participants with the prevalent attacks in online learning (Fouad, 2021; Impact Networking, 2021)
ii. *Protecting Data*: provided appropriate measures for data security. Schools should plan for data security considering the information they hold and risks they face. This involves implementing technical, administrative, and physical controls (Richardson et al., 2020).
iii. *Securing Online Communication and Learning Devices*: focused on advanced techniques to secure data, devices, and communication between entities in educational institutions.
iv. *Cybersecurity Concerns in Emerging Educational Technologies*: emerging technologies bring new risks and teachers may face challenges keeping abreast with the threats posed by the evolving solutions (von Solms & von Solms, 2014). A cybersecurity preparedness plan was included to ensure teachers could plan, develop and implement cyber safety strategies in schools (Cybersecurity and Infrastructure Security Agency, 2020; UNESCO, 2018).

The instructional design included videos, audios, lesson transcripts, articles, case studies, discussions, polls, and webinars. Each module had a quiz and module assessment to test the participants' understanding of the subject covered. An infographic that summarised the key takeaways in every module was included for ease of reference. Equally, a resource pack containing all the module resources was available for download. Participants could repurpose the OER for teaching (Pencheva et al., 2020).

Delivery Platforms

The first and second offers of CTT as well as the first offer of ACTT were delivered on MOOCs for Development MooKIT platform. However, the second offer of ACTT was delivered on COL's Teacher Futures Moodle platform for better facilitation and learning experience. Both MooKIT and Moodle are open-source platforms, and their use aligns with COL's purpose of promoting quality learning sustainably using open technology (Commonwealth of Learning, 2021). Course webinars were held via video conference platform. The technologies deployed were suitable in enhancing learner engagement. They supported lecture videos, self-assessment, networking and communication between learners, and course facilitation (Alturkistani et al., 2018).

Evaluation of MOOC Experience

Evaluation in MOOCs can help gauge their effectiveness and improve utilisation (Alturkistani et al., 2018). Data was collected using three surveys: pre-course, end-of-course, and a reflective tool, also known as 'Tell us your story'. The questions were structured to find out the impact of the courses at four levels - reaction, learning, behaviour and results- as outlined by Kirkpatrick & Kirkpatrick (2006). Additional datasets were obtained from the forums and webinar chats.

Both quantitative and qualitative analysis was done using Excel and NVivo respectively. The quantitative analysis focused on descriptive statistics. The qualitative analysis employed thematic analysis using the theoretical approach at a semantic level, to determine the cyberattacks participants had experienced, the challenges they faced during training, and the impact of the courses. The data was coded to answer the questions asked (Braun & Clarke, 2006). The results of the analyses included coverage (audience reached vs targeted), participation (engagement with the MOOCs), quality (of the MOOCs), achievement (certification and assessment results), and outcomes (changes in the organisation and individual) (Chapman et al., 2016).

4. Pedagogical Impact of Cyberattacks

Cyberattacks can disrupt learning in several ways including slow or no access to learning materials, cancellation of classes, and delayed assessments (Fouad, 2021). Data collected from the second offer of the ACTT course highlighted some of the impacts of cyberattacks on teaching and learning as follows.

Disrupted teaching and learning: some participants had experienced 'Zoombombing' which can halt learning and in some cases, expose attendees to explicit and violent content (Cybersecurity and Infrastructure Security Agency, 2020).

Slow or no access to learning systems occasioned by viruses, malware, or denial of service attacks.

"Our computer network does go down from time to time due to malware or suspected hacks"

"I found ransomware attack on my office PC"

Delayed assessments can result from loss of data or denied access causing anxiety among learners (Daniel, 2020; Fouad, 2021). Providing prompt and meaningful feedback to assessment is important as it ensures immediacy and encourages learner engagement, thereby enhancing their online learning experience (Ogange et al., 2018).

"The computer holding data for the school of postgraduate studies crashed"

Loss of teacher-student trust: impersonation of teachers online could cast them in disrepute leading to loss of teacher-student trust and student-teacher interaction in the classroom (Carter, 2020). Furthermore, the reputation of the teacher's school might be affected making it less attractive to talented teachers and prospective students (Endsleigh, n.d.). Some participants shared instances where their social media accounts were hacked and used to tarnish their name, collect money, and spam their network.

Loss of teaching and learning materials could lead to more time spent developing them afresh.

"My project on my tablet was attacked by a virus, so I had to start from scratch."

Mental health of teachers who are victims of cyberbullying could negatively affect how they engage with learners and their peers. In some cases, they may opt to leave the profession (Bester et al., 2017).

"Someone hacked my Facebook and wrote certain things as if it was me and it almost destroyed me."

5. Impact of CTT and ACTT on Teaching and Learning

There is need for more evidence on the impact of MOOCs on learners' knowledge, skills, and attitudes (Alturkistani et al., 2018). This section discusses the impact of the cybersecurity course series.

Knowledge Impact: Participants indicated that their knowledge had improved across all the eight modules covered in the training. They found the course useful with those in the affirmative ranging between 89% and 100% across the four offers of the courses.

Impediments to Learning and Professional Development: The courses helped participants to think about the impediments they faced. Most indicated that the training helped them to address cybersecurity challenges. They also found it necessary to incorporate ICT in teaching online and improving the learning experience of their students.

"It helped me protect the school email account, learner digital devices, and teacher digital devices"

"The advanced Cybersecurity Training for Teachers (ACTT) course has helped me to reflect further on interactive learning for both the general education child and children with special needs (Autism spectrum, speech delays, ADHD) and ways to enhance virtual field trips, problem solving, critical thinking, literacy, and numeracy activities through gamification."

Effective use of Cybersecurity Tools: Participants were empowered to use appropriate tools and strategies to protect their devices, data, and communication.

"I was able to apply the knowledge learned about best practices in cybersecurity, using VPNs, managing cookies, and blocking websites as I utilized learning platforms personally and the LMS with my students. Additionally, the encryption of sensitive data such as students' and parents' personal data and students' grades was meaningful to me as well."

Readiness to Sensitise Learners and Institutions: A number of participants expressed readiness to sensitise their institutions, learners, and community using various means. Many indicated that they would conduct awareness campaigns through meetings, online learning platforms and classroom lessons.

"I have actually started teaching this course to my students because it coincides with one of the topics I am required to teach, that is 'threats to computers and its users'. In fact, this course provided me with the resources needed for the lessons."

Performance and Promotion: Participants indicated that the training would improve their teaching practice and performance. It would also be useful in their promotion or in getting alternative opportunities to apply their knowledge.

"For sure the course will improve my teaching practice and performance. I have learned skills in document sharing with students and securing their scores and data. I can also help the institution understand the risk involved in the online classes and how to be protected."

"It will improve my opportunity for promotion as now my school will rely on me on cybersecurity related matters in all departments."

6. Innovations for Teacher Training and Ongoing Empowerment

Facilitated MOOCs

The MOOCs provide a low-cost solution as an innovative approach to teaching cybersecurity (Fraillon et al., 2014). Though internet connectivity and appropriate learning devices was a challenge to some (Li & Lalani, 2020), the content was delivered on lightweight platforms (Moodle and MooKIT) and in different formats (audio, text, video) accessible to a diverse group of learners.

The CTT and ACTT MOOCs were designed to be easily understood by educators to ensure they would be able to apply the skills and knowledge gained in the classroom (Ivy et al., 2019). In fact, a new term was coined for this approach: 'teacherising cybersecurity'.

Free and Open Source Tools and OER

Several free and open source tools were used which teachers would exploit during and beyond the training. All the resources were available to the participants as OER, which they could repurpose for teaching (Pencheva et al., 2020). In addition, the courses also leveraged native capabilities in the learners' smartphones and computers to secure their data and devices.

Cybersecurity Preparedness Plan

Schools should plan, prepare, and implement security policies (Cybersecurity and Infrastructure Security Agency, 2020) and put an appropriate response plan in place in case of an incident (Richardson et al., 2020). Participants developed and shared a cybersecurity preparedness plan for their institutions as part of the activities in the ACTT course.

Communities of Practice

Educators trained in cybersecurity are expected to train others to build more capacity in the area (Amankwa, 2021). Some participants expressed the desire to train their colleagues, family, and community, thereby evolving local and regional communities of practice (Wenger, 1998). Consequently, facilitator guides for both courses were developed which would assist not only in teaching the course but also mentoring other trainers in their CoPs.

AI-based Teacher Support

Online learning should not replicate the traditional classroom. Different pedagogical approaches are required that incorporate collaboration tools and engagement methods which promote inclusion, personalisation, and intelligence (Li & Lalani, 2020). We view innovation in teacher education as the interfacing of knowledge sharing, learning analytics, and application of AI towards improved learning outcomes. The data from the surveys was analysed to identify challenges that may possibly be resolved using AI. The main outcome of this undertaking was a taxonomy of needs that would lead to sustainable capacity building when on-demand personalised learning is realised, as shown in Figure 1. By integrating AI at all the levels identified in the taxonomy, educators can learn on-demand and access the resources and support they need when learning and teaching cybersecurity (Amankwa, 2021; Pencheva et al., 2020).

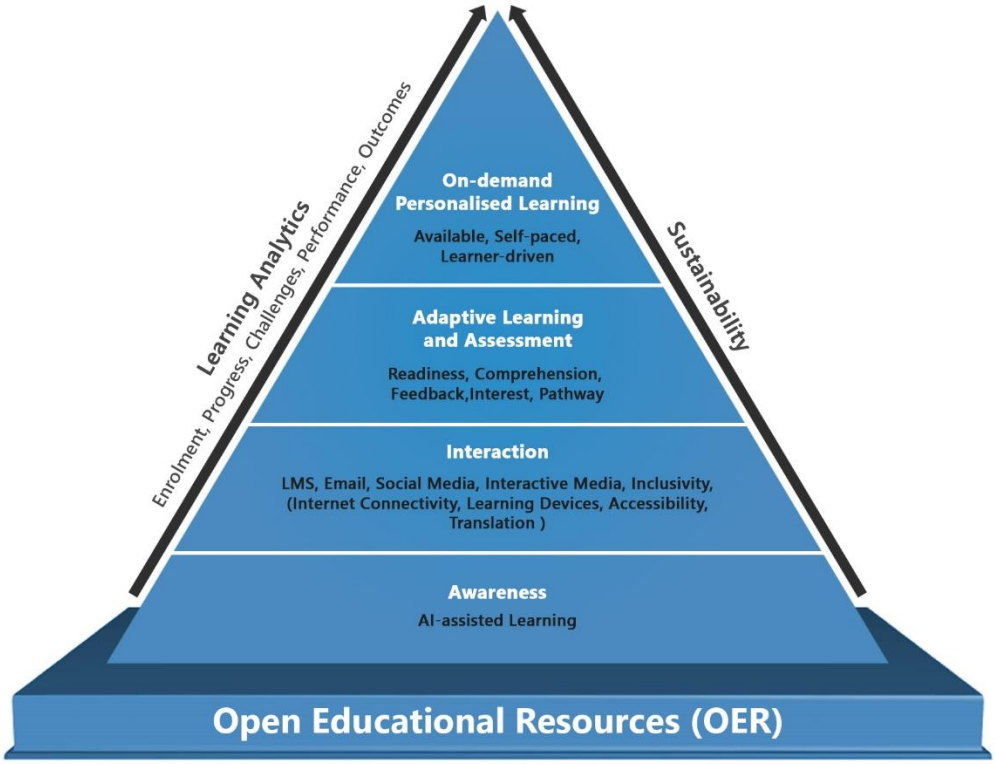

Figure 1. Taxonomy of needs in AI-based teacher support

Policy towards Secure Learning Spaces

Even though the education sector does not meet the existential threshold to warrant serious government policy interventions, practitioners and institutions in the sector do meet cybersecurity challenges that warrant attention including financial losses, disruption of learning, and theft of intellectual property, that combined greatly hamper personal and national security (Fouad, 2021).

Cybersecurity should be included in pre-service and in-service teacher training programmes (UNESCO, 2018). This would ensure educators adopt teaching models that incorporate cybersecurity, and proactively protect themselves, their learners, and institutions. To realise this, government support is essential in subsidising expenses related to implementation of cybersecurity programmes in educational institutions and facilitating access to affordable and reliable internet connectivity (Amankwa, 2021; Pusey & Sadera, 2011).

Teachers should upskill in AI in "a pedagogical and meaningful way" that is relevant to teaching, learning and research (Popenici & Kerr, 2017; UNESCO, 2019). The use of AI in teaching and learning will redefine the role of teachers, as teaching tools, learning methods, access to knowledge and teacher training revolutionise. In the same way ICT skills are important to today's teacher, AI skills will be crucial for tomorrow's educator (Higuera, 2019).

7. Conclusion

This paper highlighted the cybersecurity challenges affecting teachers in online learning, and explored innovative approaches to the problem including MOOCs, AI, communities of practice and policy considerations towards safer learning spaces. Educators and learners can be exposed to cyberattacks that could disrupt teaching and learning in various ways. It is, therefore, imperative to prepare teachers to be aware of and handle cyberattacks. MOOCs offer a low-cost innovative solution to teacher training and empowerment. Cybersecurity MOOCs for teachers should be tailored in the context of teaching and learning with a focus on practicality in the classroom. Such training offers knowledge, tools, and skills that educators can use to sensitise their learners and institutions. It also improves their performance and chances of promotion. As part of teacher professional development, AI has the potential of scaling cybersecurity training for teachers through on-demand personalised learning as well as providing access to targeted OER. Promoting cybersecurity training and the integration of AI requires policy intervention. From a policy perspective, cybersecurity training for teachers should be included in pre-service training and after they join learning institutions. Government support is vital for schools and teacher training institutions to successfully implement cybersecurity awareness and training programmes, and integrate AI in teacher development, teaching, and learning.

Disclaimer

The views represented in this paper are those of the authors and not those of the Commonwealth of Learning and eKRAAL Innovation Hub.

References

Alturkistani, A., Car, J., Majeed, A., Brindley, D. A., Wells, G., & Meinert, E. (2018). Determining the effectiveness of a Massive Open Online Course in Data Science for Health. *International Conference E-Learning, WP-*.

Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security*, *12*(4), 233–249.

Bester, S., du Plessis, A., & Treurnich, J. (2017). A secondary school teacher's experiences as a victim of learner cyberbullying. *Africa Education Review*, *14*(3–4), 142–157. https://doi.org/10.1080/18146627.2016.1269608

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Carter, H. L. (2020, January). A Call To Action For School Leaders. *Principal Leadership*. https://www.nassp.org/publication/principal-leadership/volume-20/principal-leadership-january-2020/cyberbullying-january-2020/

Chapman, S. A., Goodman, S., Jawitz, J., & Deacon, A. (2016). A strategy for monitoring and evaluating massive open online courses. *Evaluation and Program Planning*, *57*, 55–63. https://doi.org/https://doi.org/10.1016/j.evalprogplan.2016.04.006

Commonwealth of Learning. (2021). *Strategic Plan 2021-2027*. http://oasis.col.org/bitstream/handle/11599/3871/2021-2027_COL_Strategic Plan.pdf?sequence=1&isAllowed=y

Cybersecurity and Infrastructure Security Agency. (2020). *Cyber Threats To K-12 Remote Learning Education*.

Daniel, S. J. (2020). Education and the COVID-19 pandemic. *PROSPECTS*, *49*(1), 91–96. https://doi.org/10.1007/s11125-020-09464-3

Endsleigh. (n.d.). *Why schools should care about their online reputation*. Retrieved March 30, 2022, from https://www.endsleigheducation.co.uk/downloads/why-schools-should-care-about-their-online-reputation/

Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*, *6*(2), 137–154. https://doi.org/10.1080/23738871.2021.1973526

Fraillon, J., Ainley, J., Schulz, W., Friedman, T., & Gebhardt, E. (2014). *Preparing for life in a digital age: The IEA International Computer and Information Literacy Study international report*. Springer Nature.

Future Learn. (n.d.). *Introduction to Cybersecurity for Teachers*. Retrieved March 17, 2022, from https://www.futurelearn.com/courses/teaching-cybersecurity

Garg, S., Aggarwal, D., Upadhyay, S. K., Kumar, G., & Singh, G. (2020). Effect of COVID-19 on school education system: Challenges and opportunities to adopt online teaching and learning. *Humanities & Social Sciences Reviews*, *8*(6), 10–17.

Higuera, C. de la. (2019). *A report about Education, Training Teachers and Learning Artificial Intelligence: Overview of key issues.* Knowledge 4 All Foundation. https://www.k4all.org/wp-content/uploads/2019/11/Teaching_AI-report_09072019.pdf

Impact Networking. (2021). *15 Cybersecurity In Education Stats You Should Know*. https://www.impactmybiz.com/blog/cybersecurity-in-education-stats/

Ivy, J., Lee, S. B., Franz, D., & Crumpton, J. (2019). Seeding Cybersecurity Workforce Pathways With Secondary Education. *Computer*, *52*(3), 67–75. https://doi.org/10.1109/MC.2018.2884671

Kirkpatrick, D. L., & Kirkpatrick, J. D. (2006). *Evaluating Training Programs: The Four Levels*. Berrett-Koehler Publishers, Inc.

Li, C., & Lalani, F. (2020). *The COVID-19 pandemic has changed education forever. This is how*. Word Economic Forum. https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-

learning/

Ogange, B., Agak, J., Okelo, K., & Kiprotich, P. (2018). Student Perceptions of the Effectiveness of Formative Assessment in an Online Learning Environment. *Open Praxis*, *10*(1), 29–39. https://www.learntechlib.org/p/183571

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education. *IEEE Security & Privacy*, *18*(2), 68–74. https://doi.org/10.1109/MSEC.2020.2969409

Popenici, S. A. D., & Kerr, S. (2017). Exploring the Impact of Artificial Intelligence on Teaching and Learning in Higher Education. *Research and Practice in Technology Enhanced Learning*, *12*(1), 22. https://doi.org/10.1186/s41039-017-0062-8

Pusey, P., & Sadera, W. A. (2011). Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. *Journal of Digital Learning in Teacher Education*, *28*(2), 82–85. https://doi.org/10.1080/21532974.2011.10784684

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for Cyber Security in Schools: The Human Factor. *Educational Planning*, *27*(2), 23–39.

Sailer, M., Murböck, J., & Fischer, F. (2021). Digital learning in schools: What does it take beyond digital technology? *Teaching and Teacher Education*, *103*, 103346. https://doi.org/https://doi.org/10.1016/j.tate.2021.103346

UNESCO. (2018). *UNESCO ICT Competency Framework for Teachers Version 3*. https://unesdoc.unesco.org/ark:/48223/pf0000265721

UNESCO. (2019). *Artificial Intelligence in Education: Challenges and Opportunities for Sustainable Development*. https://www.gcedclearinghouse.org/sites/default/files/resources/190175eng.pdf

United Nations. (2020). *Policy Brief: Education during COVID-19 and beyond*.

von Solms, S., & von Solms, R. (2014). Towards Cyber Safety Education in Primary Schools in Africa. *HAISA*, 185–197.

Wenger, E. (1998). Communities of Practice: Learning, Meaning, and Identity. In *Learning in Doing: Social, Cognitive and Computational Perspectives*. Cambridge University Press. https://doi.org/DOI: 10.1017/CBO9780511803932