Journal of Education and Learning Technology (JELT)
ISSN 2720-7730 Volume 7 Issue 9 2026, 1103- 1113
Available online at: https://noyam.org/journals/jelt/
DOI: https://doi.org/10.38159/jelt.2026796

Check for updates

Exploring cybersecurity threats among school teachers and learners in South Africa

Hlungwane Matimu Tyron[1] & Michael Mbongiseni Buthelezi[1]

[1] Department of Education Studies, University of Limpopo, Polokwane City, South Africa.

ABSTRACT

The use of Information and Communication Technology in schools for the purpose of enhancing teaching and learning has dramatically increased in South African schools, particularly during the time of COVID-19. Schools surged into the use of information and communication technology without sufficient oversight, leaving many schools, both well-resourced and under-resourced, more vulnerable to a variety of cybersecurity threats. As a result, despite its multiple benefits in the teaching and learning area, it poses a substantial threat to school data as well as the safety of teachers and learners. The purpose is to explore the variety of cybersecurity threats experienced by schoolteachers and learners in the Vhembe East District of the Limpopo Province, South Africa. The qualitative research methodology was adopted, wherein a case study design was employed, using semi-structured interviews to generate the data. 24 participants, including school principals, teachers, learners, and parents, were purposively selected. The thematic analysis approach was used to analyse the data. The study's findings revealed that schools are increasingly susceptible to cyber threats and attacks such as phishing, Trojans, hacking, cyberbullying, insider threats, and inappropriate content, which not only harm school data but also jeopardise the safety of teachers and learners. Implications for the study include installing up-to-date and frequently updated antivirus software, developing a cyber policy, establishing a cyber-governing body, cyber-risk assessment committees, implementing cyber-awareness programmes, and involving school-based social workers and parents. This study contributes to policy and practice by proposing a holistic framework for strengthening cybersecurity in schools.

Keywords: Information and Communication Technology, Cyber Security, Cyber Threats, Safeguard, Cyber Awareness

INTRODUCTION

With the advent of the fourth industrial revolution (4IR), information and communication technology (ICT) is increasingly becoming part of contemporary society. ICT is used in different aspects of our lives, which include education, health, social interaction, and information gathering. In education, there was a sudden surge in the utilisation of ICT, especially following the COVID-19 pandemic. The use of ICT has had significant benefits (Abdul et al.).[1] It helped schools to continue teaching online and helped

[1] Abdul Wajid Fazil et al., "Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province," *American Journal of Education and Technology* 2, no. 4 (2023): 50–61.

CORRESPONDENCE – Michael Mbongiseni Buthelezi **Email**: michael.buthelezi@ul.ac.za
PUBLICATION HISTORY - Received : 17th March, 2026 | Accepted: 18th August, 2026 | Published: 10th November, 2026.
TO CITE THIS ARTICLE – Tyron, Hlungwane Matimu, and Michael Mbongiseni Buthelezi. "Exploring cybersecurity threats among school teachers and learners in South Africa." *Journal of Education and Learning Technology* 7, no.9 (2026): 1103 - 1113. https://doi.org/10.38159/jelt.2026796
COPYRIGHT AND LICENSING - © 2026 The Author(s). Published and Maintained by Noyam Journals.
This is an open access article under the CCBY license (http://creativecommons.org/licenses/by/4.0/).

to improve institutional record management and strengthen communication among school stakeholders. Nevertheless, improper ICT use may heighten the risk of cybersecurity threats such as Trojans, phishing, and ransomware, among others, in schools.[2]

The unobserved sudden surge in the use of ICT by schools, combined with a lack of cyber knowledge, ICT skills, and support from stakeholders, has led to a noticeable increase in cybersecurity attacks in schools.[3] As such, Schools that have adopted ICT for enhancing teaching and learning are increasingly becoming targets for cybercriminals, putting teaching and learning activities at risk of compromise. This challenge, along with other issues that have arisen due to the advent of ICT in schools, necessitated the need to explore the various cybersecurity threats experienced by both teachers and learners in schools. This was done in order to recommend safety measures or strategies to curb and ameliorate the cybersecurity threats faced by school teachers and learners to ensure safety in the use of ICT in schools, particularly in the Vhembe East District of the Limpopo Province. Furthermore, the studies that have been conducted on cybersecurity in schools can be classified as cyberbullying, cyber-attacks, the cost of service and high-quality protection, and cybersecurity awareness.[4] However, it appears that no study has been conducted on the various types of cybersecurity threats in schools, particularly in the Vhembe East District of Limpopo Province. Against this backdrop, the study was conducted in the Vhembe East District of Limpopo Province, South Africa, to investigate the different types of cybersecurity threats encountered by teachers and learners at schools. The findings are presented in subsequent sections.

LITERATURE REVIEW

A literature review in a study is simply a part or a section that includes what other local and international scholars have written about the phenomenon under study.[5] Moreover, according to Lim et al., a literature review is a summation of scholarly research on a certain topic that can be conducted as part of a conceptual, empirical, or independent study.[6] Furthermore, a literature review aims to consolidate existing knowledge to assist and facilitate the production of new knowledge for a specific research project, as well as to connect readers to crucial areas of existing knowledge.[7] The advent of ICT in schools has affected the teaching and learning experiences in both developing and developed countries.[8] The ever-evolving cybersecurity threats that come with the use of ICT in schools keep on increasing, yet the level of adaptation of ICT by schools and school cybersecurity capability remains slow.[9] In support of this assertion, Osias et al., in a study conducted in America, highlight the dangers that educational institutions face from cybersecurity threats such as ransomware attacks, phishing scams, data breaches, and insider threats.[10] To address these risks effectively, the author recommended the adoption of proactive measures such as conducting risk assessments, establishing strong cybersecurity governance structures, providing employee education and training programs, and implementing access controls and encryption mechanisms.

---

[2] Brett Van Niekerk, "An Analysis of Cyber-Incidents in South Africa," *The African Journal of Information and Communication* 20 (2017): 113–32.

[3] K.T Osias et al., "Managing Cyber Security Risks in Educational Technology Environment: Strategies and Best Practices," *American Journal of Language, Literacy and Learning in STEM Education* 1, no. 5 (2023): 2993–2769.

[4] Parvaneh Farhangpour, Cynthia Maluleke, and Humbulani N Mutshaeni, "Emotional and Academic Effects of Cyberbullying on Students in a Rural High School in the Limpopo Province, South Africa," *South African Journal of Information Management* 21, no. 1 (2019): 1–8; Osias et al., "Managing Cyber Security Risks in Educational Technology Environment: Strategies and Best Practices"; Baldreck Chipangura and Gustave Dtendjo-Ndjindja, "Securing the Cybersafety of South African Online High School Learners beyond COVID-19," *The Journal for Transdisciplinary Research in Southern Africa* 18, no. 1 (2022): 1256; M E Eltahir and O S Ahmed, "Cybersecurity Awareness in African Higher Education Institutions: A Case Study of Sudan," *Inf. Sci. Lett* 12, no. 1 (2023): 171–83.

[5] Andrew S Denney and Richard Tewksbury, "How to Write a Literature Review," *Journal of Criminal Justice Education* 24, no. 2 (2013): 218–34.

[6] Weng Marc Lim, Satish Kumar, and Faizan Ali, "Advancing Knowledge through Literature Reviews:'What','Why', and 'How to Contribute,'" *The Service Industries Journal* 42, no. 7–8 (2022): 481–513.

[7] Lim, Kumar, and Ali, "Advancing Knowledge through Literature Reviews:'What','Why', and 'How to Contribute.'"

[8] Nurul Amirah Abdul Rahman et al., "The Importance of Cybersecurity Education in School," *International Journal of Information and Education Technology* 10, no. 5 (2020): 378–82.

[9] Denny Pencheva, Joseph Hallett, and Awais Rashid, "Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education," *IEEE Security & Privacy* 18, no. 2 (March 2020): 68–74, https://doi.org/10.1109/MSEC.2020.2969409.

[10] Osias et al., "Managing Cyber Security Risks in Educational Technology Environment: Strategies and Best Practices."

On the same note, Maqsood and Chiasson alluded to the fact that lack of cybersecurity awareness is a major concern globally by claiming that, in the contemporary digital world, tweens are massively in cyberspace, which exposes them to a large number of cyber threats such as phishing, cyberbullying, exposure to age-inappropriate content, misinformation, and privacy violations.[11] Moreover, Richardson et al. and Abdul et al. echoed the aforementioned arguments that cybersecurity threats in schools are a critical issue in the twenty-first century, citing the human factor as an underlying reason for cybersecurity threats in schools.[12] Concurrently, Abdul et al. echoed that while the internet presents vast opportunities, it simultaneously exposes young learners to potential risks, encompassing cyberbullying, privacy breaches, and security threats.[13] To mitigate these challenges, the study advocates for the cultivation of digital literacy and online safety principles across diverse age groups and fields of study.

Moyo et al. contributed by alluding to the fact that the education sector in Zimbabwe is still ill-prepared to deal with e-safety issues in schools.[14] Moreover, most parents, teachers, and learners do not have the knowledge and expertise to safeguard learners from ICT risks. Therefore, learners are highly engaged in unacceptable and risky behaviours like receiving and storing inappropriate materials on their ICT devices, agreeing to meet strangers, meeting online friends physically, and accessing pornographic material, which further exposes them to cyber risks such as inappropriate content, communicating and meeting strangers, cyberbullying, ICT addiction, and cyber harassment. Moreover, Burov et al. contend that the emergence of the COVID-19 pandemic has increased people's dependence on digital tools globally and, consequently, increased their vulnerability to cybercriminals.[15] In their argument, they claim that the human cognitive sphere becomes the target for hackers, and a learner's knowledge, way of thinking, critical abilities, and life value system can be breached through wrong content, false links, fake news, interference during teaching and learning communication, and demotivating external influence on participants in the learning process.

De Barros and Lazarek also support the aforementioned by bringing the side view of Mozambique on this issue. They stated that Mozambique is one of the African countries in which the initiatives of raising cyber security awareness and educating primary and secondary schools on cyber security, such as cyber awareness campaigns, games, and the introduction of cyber safety topics in the school curriculum, are still in their infancy.[16] Meanwhile, in the insights attributed to local studies, it is evident that the use of ICT in schools to enhance teaching and learning has been on the rise in South African schools more than it ever was before the COVID-19 pandemic, causing an increase in vulnerability to cybersecurity threats for school teachers and learners.[17] Moreover, South African schools are deeply faced with the challenges of a lack of ICT infrastructure, coupled with a lack of knowledge of ICT and cybersecurity.[18] Therefore, it is of paramount significance to note that the academic arguments provided offer valuable insights into cybersecurity threats in South African schools and globally. They cover recent attacks, common threats, and recommended strategies to combat such threats. However, the discussion falls short of delving deeply into the specific

[11] Sana Maqsood and Sonia Chiasson, "Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens," *ACM Transactions on Privacy and Security (TOPS)* 24, no. 4 (2021): 1–37.

[12] Michael D Richardson et al., "Planning for Cyber Security in Schools: The Human Factor.," *Educational Planning* 27, no. 2 (2020): 23–39; Fazil et al., "Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province."

[13] Fazil et al., "Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province."

[14] Abel Moyo et al., "An E-Safety Framework for Secondary Schools in Zimbabwe," *Technology, Knowledge and Learning* 27, no. 4 (2022): 1133–53.

[15] O Yu Burov et al., "Cybersecurity and Innovative Digital Educational Environment," *Інформаційні Технології і Засоби Навчання* 6, no. 80 (2020): 414–30.

[16] Martina J Zucule De Barros and Horst Lazarek, "A Cyber Safety Model for Schools in Mozambique," in *Proceedings of the 4th International Conference on Information Systems Security and Privacy, Funchal, Portugal*, 2018, 22–24.

[17] Elmarie Kritzinger, "Short-Term Initiatives for Enhancing Cyber-Safety within South African Schools," *South African Computer Journal* 28, no. 1 (2016): 1–17; Claudette Leppan, *Analysis of a South African Cyber-Security Awareness Campaign for Schools Using Interdisciplinary Communications Frameworks* (Nelson Mandela University, 2017); Farhangpour, Maluleke, and Mutshaeni, "Emotional and Academic Effects of Cyberbullying on Students in a Rural High School in the Limpopo Province, South Africa."

[18] Kritzinger, "Short-Term Initiatives for Enhancing Cyber-Safety within South African Schools."

cybersecurity threats experienced by teachers and learners in South Africa, particularly in the Vhembe East District of the Limpopo province.

THEORETICAL FRAMEWORK

Varpio et al. described a theoretical framework as a logically established and interconnected set of concepts and premises derived from one or more theories that a researcher constructs to scaffold a study. The authors further articulate that in order to build a theoretical framework, the researcher must define any concepts and theories that will serve as the foundation for the research, connect them logically, and relate these concepts to the study under investigation.[19] Moreover, Grant and Osanloo argue that the theoretical framework is a framework that is derived from an existing theory (or theories) in the literature that has already been tested and validated by others and is considered a generally acceptable theory in the scholarly literature.[20] Many theoretical frameworks can serve as lenses to guide the conduct of a study. To select the proper theoretical framework, a full grasp of the study problem, goal, significance, and research question thereof is required, ensuring that it closely corresponds with and intricately weaves together all four dimensions.[21] Therefore, in this study, Urie Bronfenbrenner's ecological systems theory was selected because it best fits the research problem, goal, relevance, and research question; also, it explicitly elucidates the several environmental systems that would drive the study's procedure. This theory recognises that individuals do not exist in isolation; rather, their experiences are influenced by interconnected systems, including the school, family, community, educational policies, and broader societal and technological environments.[22]

Urie Bronfenbrenner developed the ecological framework in response to what he described as the science of children in strange situations. Urie Bronfenbrenner's ecological systems theory elucidates how human development is shaped by various environmental factors.[23] According to him, this theory encompasses four interconnected types of environmental systems: the micro, meso, exo, and macro systems. However, this theory, developed in the twentieth century, did not consider the impact of development in the digital age. In response to this, Navarro and Tudge saw it as fitting that the theory be significantly modified to reflect most of the ubiquitous contexts in which adolescents learn, play, and grow for the theory to stay relevant even in the era of technology.[24] This theory has been used as a lens for this study, adopting the modification. The theory was appropriate and relevant for this study because it explains how human development is influenced by different types of environmental systems. It also recognises the impact of technology in the development of humans. In this study, the theory helped to examine how cybersecurity threats such as cyberbullying, phishing, hacking, and exposure to inappropriate online content are influenced by factors operating at different ecological levels. For example, the microsystem includes the direct interactions of learners and teachers with digital technologies at school and home; the mesosystem highlights the relationships between schools, parents, and the community in promoting online safety; the exosystem considers the influence of school management, district support structures, and internet service providers; the macrosystem reflects national cybersecurity policies, cultural attitudes, and legal frameworks; and the chronosystem captures changes over time, such as the increased use of information and communication technologies during and after the COVID-19 pandemic.[25]

By applying Bronfenbrenner's Ecological Systems Theory, the study demonstrates that addressing cybersecurity threats requires coordinated efforts across these interconnected systems rather

[19] Lara Varpio et al., "The Distinctions Between Theory, Theoretical Framework, and Conceptual Framework," *Academic Medicine* 95, no. 7 (July 12, 2020): 989–94, https://doi.org/10.1097/ACM.0000000000003075.
[20] Cynthia Grant and Azadeh Osanloo, "Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for Your 'House,'" *Administrative Issues Journal Education Practice and Research* 4, no. 2 (2014).
[21] Grant and Osanloo, "Understanding, Selecting, and Integrating a Theoretical Framework in Dissertation Research: Creating the Blueprint for Your 'House.'"
[22] Wafaa El Zaatari and Imad Maalouf, "How the Bronfenbrenner Bio-Ecological System Theory Explains the Development of Students' Sense of Belonging to School?," *Sage Open* 12, no. 4 (2022): 21582440221134090.
[23] Jessica L Navarro and Jonathan R H Tudge, "Technologizing Bronfenbrenner: Neo-Ecological Theory," *Current Psychology* 42, no. 22 (2023): 19338–54.
[24] Navarro and Tudge, "Technologizing Bronfenbrenner: Neo-Ecological Theory."
[25] Navarro and Tudge, "Technologizing Bronfenbrenner: Neo-Ecological Theory."

than focusing solely on the actions of individual teachers or learners. In the twenty-first century, society finds itself living in institutions of learning, such as schools, that have rushed into the use of ICT without sufficient supervision, making both teachers and learners more vulnerable to the myriad cybersecurity threats. Hence, the use of this theory for this study was considered the most relevant because it explains in detail how a child's development should be handled in the digital era. This theory allowed the study to address the research question, "What cybersecurity threats do the school teachers and learners face in schools, particularly in the Vhembe East District of the Limpopo Province?" primarily because the century itself not only requires but also demands that, in times like these, these youths be acquainted with ICT. In using ICT, learners interact with their parents, teachers, and society at large. It influences human behaviour in daily activities.

METHODOLOGY

Research Approach

This study adopted a qualitative methodological approach, guided by the interpretive school of thought. The interpretivism paradigm was deemed fit for this study because it recognises that individuals' interpretations and experiences create multiple, subjective realities. This approach emphasises understanding the unique perspectives of participants, who are the school principals, teachers, learners, and parents, regarding the various cybersecurity threats faced by school teachers and learners.[26] Again, the researchers deemed it befitting to use a case study research design for this study, for it was meant to be conducted in three different school settings about the various cybersecurity threats faced by teachers and learners in schools.

Data Collection

In this study, an instrumental case study has been used, whereby semi-structured interviews and document review were used as instruments to generate data from participants, who are school principals, teachers, learners and parents. The decision to use this type of case study lies in the fact that this study is used as a lens to dive deeply into the various cybersecurity threats faced by school teachers and learners in the Vhembe East District of the Limpopo Province.

Population and Sampling

The study's fieldwork took place in three schools within the Malamulele Central Circuit, Vhembe East District, Limpopo Province, South Africa. The selection criteria for the schools, comprising one rural and two township schools, aimed to enhance the credibility and generalizability of the study's findings by incorporating diverse geographical settings. The purposive sampling strategy was employed to select 24 participants, which included three principals (one from each school), six parents (two from each school), six (6) teachers (two teachers per school), and nine (9) learners from three different schools (three learners per school) who are aged between 14 and 21 years. These participants were selected because they had direct knowledge and experience of the use of ICT in schools and the cybersecurity threats associated with its use. Data collection continued until data saturation was achieved. Saturation was considered to have occurred when no new themes, categories, or meaningful insights emerged from successive interviews, and the data became repetitive across participant groups. The final interviews confirmed and reinforced the themes already identified rather than generating new information, indicating that sufficient data had been collected to address the research objectives.

Data Analysis

In this study, the generated data were presented and analysed thematically to discover useful information and answer the research questions of the study. A thematic data analysis was used. Thematic analysis is a set of methods for developing and interpreting patterns of meaning across

[26] Nasrin Pervin and Mahani Mokhtar, "The Interpretivist Research Paradigm: A Subjective Notion of a Social Context," *International Journal of Academic Research in Progressive Education and Development* 11, no. 2 (2022): 419–28.

qualitative data.[27] The data was generated from the different perspectives of the school principals, teachers, learners, and parents of the three different schools. For the purpose of presenting the analysed data, codes and pseudonyms were used to preserve the anonymity of the participants, which has been maintained throughout the study.

Ethical Considerations

Throughout the study, we made sure to stick to the ethical principles laid out in the Declaration of Helsinki, which is a guide for doing ethical research with people.

PRESENTATION OF FINDINGS AND DISCUSSION

The use of ICT in schools by teachers and learners

The various interviewed school stakeholders from different schools that served as settings indicated that schools are immensely diving into the use of ICT. However, it should be noted that some schools have enough ICT resources for both the teachers and learners, while other schools only have them for teachers and do not cater to the learners. This study found that the schools that are geographically located in rural settings (villages) that served as settings for the study solely provide ICT equipment for teachers and school administrators and not for the learners, while those that are located in a township are able to provide ICT for learners, especially because they have well-equipped computer labs and internet connections, while other schools have tablets and laptops for the learners supplied by private companies through donations. This is what one of the school principals, whose school is located in a township, had to say:

> *"In my school, each and every teacher has a laptop provided by the school, including the administrative staff. We also have external drives for SMT, and we have projectors for all departments. For the learners, each and every Grade 12 learner is given either a laptop or a tablet that is connected to the school network."*

A study conducted by Pencheva et al. supports this finding by advancing that schools in rural areas are characterised by a lack of resources and limited access to cybersecurity, as compared to the schools that are located in township areas.[28] It was also discovered during the interviews with the stakeholders that learners from both township and rural schools were allowed to use their personal ICT gadgets at home to connect with their teachers and classmates on educational matters. This has greatly increased the likelihood of teacher-learner interactions outside of the normal pedagogical time, which was impossible before the advent of ICT in schools, where interactions had to occur physically only. Furthermore, it has been revealed by this study that despite the fact that some of the schools did not fully cater to ICT equipment for both teachers and learners, the use of ICT in schools remains a useful and relevant tool for enhancing teaching and learning in the 21st century in which we live. This is also consistent with the findings of Farhangpour et al., which indicated that the use of ICT in schools to improve teaching and learning has increased in South African schools more than ever before the COVID-19 pandemic, causing an increase in vulnerability to cybersecurity threats from school teachers and learners.[29]

Cybersecurity threats commonly faced by teachers in schools

The study findings reveal that in the 21st century, as institutions of learning have quickly adapted to using ICT to enhance teaching and learning, teachers have become significantly more vulnerable to cybersecurity threats such as hacking, phishing, Trojans, and information breaches. The school principal, during interviews, had this to say:

> *"Aside from the learners' cyber cases, teachers are also victims of cyber threats such as hacking, phishing, Trojans and information breaches. Moreover, I recently heard my head of*

[27] Virginia Braun and Victoria Clarke, "Using Thematic Analysis in Psychology," *Qualitative Research in Psychology* 3, no. 2 (2006): 77–101.

[28] Pencheva, Hallett, and Rashid, "Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education."

[29] Farhangpour, Maluleke, and Mutshaeni, "Emotional and Academic Effects of Cyberbullying on Students in a Rural High School in the Limpopo Province, South Africa."

department say that some educators fail to meet deadlines because the information disappeared from their laptops."

The findings of this study further highlight the lack of knowledge about these threats, limited access to ICT or digital resources, as well as the lack of cyber policies in schools, as the primary contributing factors to the increase in the vulnerability of teachers to cybersecurity threats in schools, particularly in the Vhembe East District of Limpopo Province. This overview emanates from the expressions of teachers and school principals who vowed that:

"We can confirm to you that our knowledge of cyber issues is insufficient because they are still new, and the department has not yet provided us with any training on them, policies, or ICT resources. However, we are aware of cyberbullying and inappropriate content because learners often report it."

Moreover, this position has gained support from the literature, as argued by Kritzinger, who argued that the lack of proper knowledge and training on cyber safety by teachers and learners is the primary reason behind cyber threats.[30] Furthermore, the findings indicate that most of the teachers who fall victim to cybersecurity threats do so as a result of their own negligence in the use of ICT gadgets. The participants in the interviews contended that it is the responsibility of teachers as ICT users to protect themselves against cybersecurity threats when using ICT devices. This can be achieved by maintaining strong passwords, regularly updating them, and avoiding the sharing of devices. However, within schools, teachers have normalised the practice of using laptops without passwords and frequently share devices.

Cybersecurity threats commonly faced by learners in schools

In educational institutions, learners are often viewed as passive recipients of knowledge, while teachers are regarded as custodians of that knowledge. Consequently, learners tend to depend heavily on their teachers for guidance and protection against cybersecurity threats associated with the use of ICT in teaching and learning. The study results clearly indicate that the inadequate supervision from both teachers and parents regarding learners' use of ICT gadgets, combined with a lack of knowledge about cybersecurity and insufficient awareness campaigns, has led to the misuse of these devices. An interviewed learner expressed the following support for this notion:

"I find these platforms to be a very complex environment that requires a lot of guidance and supervision. I am saying this because cell phones are being hacked, allowing other learners to access the private information of other learners; some are being bullied on WhatsApp and Facebook, and I also know of a particular gang at our school who have been spotted downloading and viewing pornography during study time in the computer lab."

This misuse ultimately increases learners' vulnerability to various cybersecurity threats, including cyberbullying, exposure to inappropriate content, data breaches, and hacking.

"As a class teacher, I have received a lot of complaints in my office from learners about cyberbullying, hacking of cell phone passwords, privacy breaches, and inappropriate content, some of which happen at home."

Said a teacher who has been tasked with the responsibility of handling learners' cyber-related cases at his school. In support of this assertion, Pencheva et al. asserted that learners lack guidance and supervision from adults to leverage their capabilities in the cyber environment and to navigate safely in the cyber environment, making them more vulnerable to cyber threats such as cyberbullying, cyber addiction, phishing, and identity theft, among others.[31]

[30] Kritzinger, "Short-Term Initiatives for Enhancing Cyber-Safety within South African Schools."
[31] Pencheva, Hallett, and Rashid, "Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education."

The cybersecurity threats that are prevalent in schools

It is evident from the empirical findings of this study and the literature review that, in the 21st century of the fourth industrial revolution, phishing, ransomware, hacking, cyberbullying, privacy breaches, and inappropriate content, among others, have become prevalent in schools. The school principal in one of the schools visited during data collection contributed the following:

> *"The most prevalent cybersecurity threats that are frequently reported by both the educators and learners include cyberbullying, hacking, Trojans, information breaches, phishing and inappropriate content."*

This is also evident in the literature reviewed, whereby Maqsood and Chiasson claimed that, in the contemporary digital world, teachers and learners are massively in cyberspace, which exposes them to a large number of cyber threats such as phishing, cyberbullying, exposure to age-inappropriate content, misinformation, and privacy violations.[32]

> *"As a class teacher, I have been receiving a lot of complaints in my office from the learners about cyberbullying, hacking of cell phone passwords, privacy breaches, and inappropriate content, some of which happen at home."*

From the expression above, the teacher from one of the schools visited in the Vhembe East District highlighted that there is no strict supervision of ICT usage, both at school and at home, by both the teachers and parents. In line with this finding, Pencheva et al. asserted that learners lack guidance and supervision from adults to leverage their capabilities in the cyber environment and to navigate safely in the cyber environment, making them more vulnerable to cyber threats such as cyberbullying, cyber addiction, phishing, and identity theft, among others.[33]

RECOMMENDATIONS

In an effort to combat these cybersecurity threats faced by school teachers and learners, schools should consider implementing the following proactive and counteractive strategies for managing cybersecurity threats.

- Install and frequently update antivirus software such as Bitdefender, Norton, McAfee, Avast, Avira, and AVG to fend off malicious attacks such as phishing, Trojans, ransomware, and hacking, to name a few.
- Develop a school cyber policy that is aligned to the Cybercrimes Act 19 of 2020, to guard against cybersecurity threats linked to human error or misbehaviour, such as cyberbullying, inappropriate content, insider threats and privacy breaches, amongst others.
- Establish a robust cyber-governing body comprising the school management team, school governing body (SGB), ICT-active teachers and school-based social workers.
- Initiate cyber awareness programmes and campaigns championed by school-based social workers. Given that the majority of 21st-century learners are engaged in cyberspace, it is imperative to develop cyber awareness messages on the internet, particularly on social media, to educate users about cyber hygiene. To maximise learner safety in the use of ICT, schools should promote cyber hygiene by developing and displaying cyber posters on all school notice boards and participating in National Cyber Day (NCD), which is observed annually on November 30th.
- When establishing a cyber risk assessment programme, it is recommended that schools consider creating a cyber risk assessment programme to identify and curb malicious attacks, such as Trojans, phishing, ransomware, hacking, among others, that compromise school data.
- Initiating educators' training on cyber security threats to capacitate the educators with the cyber security knowledge needed to counter and ameliorate the cyber security threats faced by school teachers and learners. The training should be focused on equipping the educators with the

[32] Maqsood and Chiasson, "Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens."
[33] Pencheva, Hallett, and Rashid, "Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education."

necessary knowledge of cybersecurity threats, such as the benefits of ICT use, cybersecurity threats associated with the use of ICT in schools, and how to be safe and ensure the safety of others in the use of ICT.

- Involving school-based social workers and parents to identify and ameliorate cybersecurity threats linked to human error or misbehaviour, the school-based social workers should be involved for their expertise in dealing with sensitive issues, and particularly to deal with cyber behaviour that may have emotional effects on both the teachers and the learners, such as cyberbullying, privacy breaches, and inappropriate content. The parents should also take part by ensuring strict supervision and monitoring of the use of ICT by the learners at home to promote healthy cyber practices.

CONCLUSION

This study examined the various cybersecurity threats faced by teachers and learners in schools amid the growing integration of Information and Communication Technology (ICT) into education in the twenty-first century and the Fourth Industrial Revolution. Adopting a qualitative research approach, the study involved key school stakeholders, including principals, teachers, learners, and parents. The findings, supported by relevant existing literature, revealed that schools face numerous cybersecurity threats, including hacking, phishing, ransomware, Trojan horse attacks, information breaches, exposure to inappropriate online content, and cyberbullying. These threats underscore the need for comprehensive and proactive measures to safeguard school communities and promote the safe and responsible use of ICT in educational settings.

In response to these challenges, the study recommends a range of strategies to strengthen cybersecurity in schools. The effective implementation of these measures requires a collaborative approach involving school administrators, teachers, learners, parents, and other relevant stakeholders. Ultimately, strengthening cybersecurity in schools is essential not only for protecting sensitive information and digital resources but also for creating a safe, secure, and supportive digital learning environment.

BIBLIOGRAPHY

Barros, Martina J Zucule De, and Horst Lazarek. “A Cyber Safety Model for Schools in Mozambique.” In *Proceedings of the 4th International Conference on Information Systems Security and Privacy, Funchal, Portugal*, 22–24, 2018.

Braun, Virginia, and Victoria Clarke. “Using Thematic Analysis in Psychology.” *Qualitative Research in Psychology* 3, no. 2 (2006): 77–101.

Burov, O. Yu., O. B. Butnik-Siversky, Olena Orliuk, and K. A. Horska. “Cybersecurity and Innovative Digital Educational Environment.” *Інформаційні Технології і Засоби Навчання* 6, no. 80 (2020): 414–30.

Chipangura, Baldreck, and Gustave Dtendjo-Ndjindja. “Securing the Cybersafety of South African Online High School Learners beyond COVID-19.” *The Journal for Transdisciplinary Research in Southern Africa* 18, no. 1 (2022): 1256.

Denney, Andrew S., and Richard Tewksbury. “How to Write a Literature Review.” *Journal of Criminal Justice Education* 24, no. 2 (2013): 218–34.

Eltahir, M. E., and O. S. Ahmed. “Cybersecurity Awareness in African Higher Education Institutions: A Case Study of Sudan.” *Inf. Sci. Lett* 12, no. 1 (2023): 171–83.

Farhangpour, Parvaneh, Cynthia Maluleke, and Humbulani N Mutshaeni. “Emotional and Academic Effects of Cyberbullying on Students in a Rural High School in the Limpopo Province, South Africa.” *South African Journal of Information Management* 21, no. 1 (2019): 1–8.

Fazil, Abdul Wajid, Musawer Hakimi, Saidamin Sajid, Mohammad Mustafa Quchi, and Khudai Qul Khaliqyar. “Enhancing Internet Safety and Cybersecurity Awareness among Secondary and High School Students in Afghanistan: A Case Study of Badakhshan Province.” *American Journal of Education and Technology* 2, no. 4 (2023): 50–61.

Grant, Cynthia, and Azadeh Osanloo. “Understanding, Selecting, and Integrating a Theoretical

Framework in Dissertation Research: Creating the Blueprint for Your 'House.'" *Administrative Issues Journal Education Practice and Research* 4, no. 2 (2014).

Kritzinger, Elmarie. "Short-Term Initiatives for Enhancing Cyber-Safety within South African Schools." *South African Computer Journal* 28, no. 1 (2016): 1–17.

Leppan, Claudette. *Analysis of a South African Cyber-Security Awareness Campaign for Schools Using Interdisciplinary Communications Frameworks*. Nelson Mandela University, 2017.

Lim, Weng Marc, Satish Kumar, and Faizan Ali. "Advancing Knowledge through Literature Reviews:'What', 'Why', and 'How to Contribute.'" *The Service Industries Journal* 42, no. 7–8 (2022): 481–513.

Maqsood, Sana, and Sonia Chiasson. "Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens." *ACM Transactions on Privacy and Security (TOPS)* 24, no. 4 (2021): 1–37.

Moyo, Abel, Theo Tsokota, Caroline Ruvinga, and Colletor T Chipfumbu Kangara. "An E-Safety Framework for Secondary Schools in Zimbabwe." *Technology, Knowledge and Learning* 27, no. 4 (2022): 1133–53.

Navarro, Jessica L., and Jonathan R. H. Tudge. "Technologizing Bronfenbrenner: Neo-Ecological Theory." *Current Psychology* 42, no. 22 (2023): 19338–54.

Niekerk, Brett Van. "An Analysis of Cyber-Incidents in South Africa." *The African Journal of Information and Communication* 20 (2017): 113–32.

Osias, K.T., V.I. Nerissa, M.S. Aima, F.K. Cara, T.A. Mervin, and A.C. Glennifer. "Managing Cyber Security Risks in Educational Technology Environment: Strategies and Best Practices." *American Journal of Language, Literacy and Learning in STEM Education* 1, no. 5 (2023): 2993–2769.

Pencheva, Denny, Joseph Hallett, and Awais Rashid. "Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education." *IEEE Security & Privacy* 18, no. 2 (March 2020): 68–74. https://doi.org/10.1109/MSEC.2020.2969409.

Pervin, Nasrin, and Mahani Mokhtar. "The Interpretivist Research Paradigm: A Subjective Notion of a Social Context." *International Journal of Academic Research in Progressive Education and Development* 11, no. 2 (2022): 419–28.

Rahman, Nurul Amirah Abdul, Izzah Hanis Sairi, Nurul Akma M Zizi, and Fariza Khalid. "The Importance of Cybersecurity Education in School." *International Journal of Information and Education Technology* 10, no. 5 (2020): 378–82.

Richardson, Michael D., Pamela A. Lemoine, Walter E. Stephens, and Robert E. Waller. "Planning for Cyber Security in Schools: The Human Factor." *Educational Planning* 27,no.2(2020):23–39.

Varpio, Lara, Elise Paradis, Sebastian Uijtdehaage, and Meredith Young. "The Distinctions Between Theory, Theoretical Framework, and Conceptual Framework." *Academic Medicine* 95, no. 7 (July 12, 2020): 989–94. https://doi.org/10.1097/ACM.0000000000003075.

Zaatari, Wafaa El, and Imad Maalouf. "How the Bronfenbrenner Bio-Ecological System Theory Explains the Development of Students' Sense of Belonging to School?" *Sage Open* 12, no. 4 (2022): 21582440221134090.

ACKNOWLEDGEMENT

The authors would like to thank all the participants in this research for their voluntary participation and for sharing their experiences. Also, the researchers acknowledge the assistance provided by the anonymous peer reviewers.

DECLARATION OF INTERESTS

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

FUNDING
This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

AUTHOR'S CONTRIBUTIONS
The authors contributed to the study design, collected the data and conducted the analysis and interpretation. The authors critically revised the paper and contributed to the revision of the manuscript. The authors read and approved the final manuscript.

ABOUT AUTHORS
Michael Mbongiseni Buthelezi has a PhD in Educational Psychology from the University of KwaZulu-Natal (UKZN), an MEd in Inclusive Education from the University of South Africa (UNISA), and a BEd (Hons in Special Needs Education from North West University (NWU). He is a Senior Lecturer in the Department of Education Studies at the University of Limpopo. Dr Buthelezi has taught at all levels of education: Primary school, High School, Technical and Vocational Education and Training College (TVET), and University. Dr Buthelezi, as an e-tutor at UNISA, has taught the following modules from 2014 to 2025: Psychology of Education, learning and learning problems, and child development. Dr Buthelezi has also served as a National Evaluator for 9 years in the Evaluation & Accreditation Unit at UMALUSI before he became an Accreditation Council Committee (ACC) member at UMALUSI. His research includes psychology, student development, inclusive education, sustainable learning, psychosocial support, and rural development. He has authored books and book chapters and has also published academic research papers in national and international journals. He has presented his articles at national and international conferences. He is currently supervising BEd (Hons, PGCE, Master's, and PhD students.

Matimu Tyron Hlungwane holds a Master's Degree in Education Studies, an Honours Degree in Educational Management, and a Bachelor of Education Degree from the University of Limpopo (Turfloop Campus). Professionally, he is employed by the Department of Basic Education in South Africa as a primary school teacher. He has more than ten years of teaching experience in the public school sector and has also served as a lecturer at Ekurhuleni West TVET College for one year. Throughout his teaching career, he has demonstrated a commitment to excellence in education and learner development. In recognition of his outstanding contribution to teaching and learning, he received two National Teaching Awards at the provincial level.