The Journal for Transdisciplinary Research in Southern Africa
ISSN: (Online) 2415-2005, (Print) 1817-4434

Securing the cybersafety of South African online high school learners beyond COVID-19

Authors:
Baldreck Chipangura[1]
Gustave Dtendjo-Ndjindja[1]

Affiliations:
[1]Department of Information Systems, Faculty of Science, Engineering and Technology, University of South Africa, Johannesburg, South Africa

Corresponding author:
Baldreck Chipangura,
chipab@unisa.ac.za

Dates:
Received: 15 June 2022
Accepted: 31 Aug. 2022
Published: 19 Dec. 2022

How to cite this article:
Chipangura B, Gustave D-N. Securing the cybersafety of South African online high school learners beyond COVID-19. J transdiscipl res S Afr. 2022;18(1), a1256. https://doi.org/10.4102/td.v18i1.1256

The unprecedented online learning that took place at several schools during the coronavirus disease 2019 (COVID-19) pandemic is predicted to continue on the same trajectory when learners return to classroom learning. Continuing with online learning implies that learners will spend most of their time learning and socialising online, which exposes them to cybersecurity risks. Hence, this study investigated strategies for securing the cybersafety of online learners at South African high schools. The study adopted an interpretivist approach, and qualitative data were collected from school teachers. Fifteen school teachers from five private high schools in Centurion, Pretoria, were interviewed, and the data were thematically analysed. All the schools were multiracial and English-medium schools. The teachers from the schools were selected to participate in the study because they had experienced online learning during the times of COVID-19. The study proposed cybersafety strategies that are centred around providing cybersafety policies, conscientising learners about cybersecurity risks (awareness), preventing cyberbullying, discouraging the consumption or production of inappropriate content and protecting learners from Internet addiction.

Transdisciplinarity Contribution: The proposed practical strategies for securing the cybersafety of online learners are valuable for promoting safe and responsible use of Internet-connected devices in online learning. The strategies encourage schools to integrate Internet-connected technologies and overcome cybersecurity risks in online learning.

Keywords: online learning; COVID-19; cyberbullying; cybersafety; cybersecurity.

Introduction

The coronavirus disease 2019 (COVID-19) pandemic is a health predicament that became an educational crisis the world over. To curb the spread of COVID-19, one of the implemented strategies was to impose curfews and lockdowns, which disrupted teaching and learning in many countries. In South Africa, schools responded to the COVID-19 crisis in varied ways, especially during the peak days of the pandemic between 2020 and 2021. There were schools that completely closed their doors from providing any form of learning. An estimated 147 million children missed half of their in-person schooling between 2020 and 2022, which negatively affected the foundational learning skills of children in low-income countries.[1] On the other hand, there were schools that implemented online learning as an alternative strategy to save learning from total shutdown. The implementation of online learning was almost 100% during peak periods of COVID-19, imposing an unprecedented remote learning experience on some of the schools. Migration to online learning was abrupt, and the move was challenged by curriculum readjustments that were not made to facilitate online learning. Curriculum readjustment relates to the alignment of syllabuses to cater for technological support, teaching, assessment and learner-centeredness.[2] Therefore, the migration happened without paying attention to the technological needs, appropriateness of home learning, psychological support and cybersafety of learners.

Despite the challenges encountered in moving to online learning, it was predicted that online learning will continue on the same trajectory beyond the COVID-19 pandemic.[3,4] This is aligned with the unparalleled investment on online learning infrastructure at many schools during the COVID-19 pandemic.[4] Investments were made in developing online learning content, establishing teaching channels and developing administrative strategies to manage online learning.[3] Moreover, parents invested in online technologies for their children, who in turn gained a good deal of online learning experience. The benefits of online learning included constructivist teaching approaches and improved access to online resources, for example, open educational resources.[5] In contrast, challenges experienced were the exclusion of marginalised learners because of limited network connection in remote areas and the cybersecurity risks.[6]

Important in this research is the cybersafety of learners because of the possible exposure to cybersecurity risks when using Internet-connected devices.[7] As evidence, a study undertaken in Australia[8] found high instances of cyberbullying (78%) and exposure to adult content (74%) amongst school learners. Learners expose themselves to cyber-risks because they lack an understanding of what constitutes acceptable, ethical and responsible use of technology.[9] The blame can be equally put on parents and guardians, as evidenced in a South African study which found that 34% of cell phone Internet activities of children were not monitored and 39% of parents never discussed cybersecurity risks with their children.[10] Furthermore, South African schools were found not ready to protect learners from cybersecurity risks, as 50% of the schools did not have cybersecurity policies,[10] and educators were found ignorant of cybersafety strategies.[11,12] South African schools' curriculum was criticised for not providing cybersafety education and teaching learners about cybersecurity risks.[13] Therefore, as South African learners spend a great deal of time learning and socialising online, there is a high likelihood that their cybersafety will be compromised. Compromised cybersecurity of learners is of concern to schools in general and teachers more so, because they are the custodians of learning. This study therefore investigated the perceptions of high school teachers on how South African schools can secure the cybersafety of online learners. The aim of this study translates to the following research question that led the investigation: 'How can schools secure the cybersafety of online learners?'

The study was carried out as a qualitative study, and 15 high school teachers were interviewed from five selected private schools in the Centurion suburb of Pretoria, South Africa. The following section focuses on literature analysis of cyber-risks in learning.

Cybersafety risks in learning

This section discusses cybersafety risks that can harm online learners. The risks discussed in this section were themes that came from literature analysis in this study. The identified risks were cyberbullying, online fraud, content risks and addiction.

Cyberbullying

Cyberbullying is defined as 'an aggressive, intentional act carried out by an individual or a group using electronic forms of contact, repeatedly over time, against a target who cannot easily defend him or herself'.[13] As learners spend much of their time socialising and learning online, school bullying is no longer bounded to school premises but pursues learners to their homes. Research conducted in the United States of America found that 37% of surveyed school learners had experienced cyberbullying.[14] Globally, research conducted in 28 countries found that 51% of cyberbullying happened amongst classmates, with most incidents recorded in the United Kingdom (74%), Canada (68%) and South Africa (67%).[15] In South Africa,[15] it was reported that 54% of the parents knew at least one child who had been cyberbullied. Reasons for cyberbullying were found to be due to power domination over other learners, jealousy, peer pressure or revenge.[16] Instances of cyberbullying included hurtful comments, offensive name calling, or spreading of false rumours through platforms such as phone calls, e-mails, texting or social media.[17] Consequently, victims of cyberbullying suffer from mental health–related conditions and show symptoms associated with depression, anxiety, isolation, lower self-esteem and suicide.[16] In worst cases of bullying, effects of cyberbullying were found to be harmful to perpetrators, victims and bystanders.[18] Therefore, the question that arose was: 'How do schools prevent cyberbullying from happening?'

Online fraud

Over the years, online fraud has been used to deceive Internet users, and academics have called for measures to protect the users.[19,20,21] Recently, several online deceptions were reported, and Google blocked 126 million fraud scams related to COVID-19 in one week.[22] Online fraud mostly targets adolescents because they are stimulated by short-term rewards.[20] Moreover, adolescents are targeted because they are influenced by online purchases. If adolescents are attracted to online products, they convince their parents to make a purchase; otherwise, if they have some money, they often spend recklessly.[21] To defraud adolescents, scammers use several gimmicks to fish for personal details; these include gaming, online dating, bitcoins or gambling.[19]

Adolescents sometimes establish relationships with strangers they have never met in person, a predicament known as stranger danger.[21] Stranger danger occurs when a perpetrator employs acts such as catfishing or cyberstalking to identify, entice, brainwash and attack. Perpetrators build an emotional and trusting connection with victims before they attack.[23] Online attacks can result in victims losing money, identity theft or sexual harassment. Bacıoğlu[24] described a case where a perpetrator arranged and met a victim physically and committed sexual harassment. Similar reports have been reported in the South African media where online dating has turned into a crime scene. Evidence presented here alerts us to the dangers of online fraud. It is a challenge that alarms schools, and the question that arose was: 'How do schools protect learners from online fraud?'

Content-related risks

The Internet is an open repository of information where anyone can create or access content, irrespective of their age group. Some content is harmful, offensive or inappropriate to adolescents.[13] Adolescents may be influenced to produce or distribute harmful content on social media or the Internet, which they later regret due to digital ignorance.[25] To minimise the risk of accessing or producing harmful content, adolescents should be digitally literate. Digital literacy comprises skills, knowledge and understanding that enable safe practices with digital technologies.[26] This can be interpreted to mean that adolescents should be ethical and know whether information accessed from the Internet is valuable or harmful. Protecting adolescents is the responsibility of school teachers, parents or guardians, who should teach them digital literacy and monitor the content that they access, because they can use digital devices with little thought.[27] The analysis presented here revealed that children can consume or produce inappropriate content. Hence, the question that arose was: 'How do schools protect learners from accessing or producing inappropriate content?'

Internet addiction

Internet addiction is not a cybersecurity risk; however, it has adverse health behavioural risks to adolescents.[28] Research has claimed that Internet addiction depends on the frequency at which people engage in certain online activities or applications.[29,30] Internet addiction is biased towards excessive use of social media platforms, trading, gambling and gaming amongst young people more than old people. Online trading and gambling were found to have high likelihood of addiction and adverse effects amongst adolescents.[30] Chou and Chou[30] explained that addiction to gambling and online trading are associated with the pleasure of making good deals and quick returns amongst the adolescents. Even though Internet addiction was found prevalent in young people, excessive use of Internet on school-related work was found not to be related to addiction.[31] Nevertheless, excessive use requires parental monitoring to ensure that adolescents do not stray from schoolwork to social media.[32] Therefore, the question that arose was: 'How do schools protect online learners from Internet addiction?'

Methodology

An interpretivist approach was adopted, and qualitative data were collected through semistructured interviews from school teachers. School teachers were targeted because they are the custodians of learning and understand cybersafety of learners. The sampled school teachers were from five private high schools that serve middle-income families in the Centurion suburb of Pretoria, South Africa. The schools are multiracial in terms of student population and the teachers. The schools are English medium; however, other South African languages are taught at the schools.

The schools were conveniently selected from 10 private schools invited to participate through e-mails sent to the principals. Five schools were selected on the criteria that they had used online teaching when schools were closed due to COVID-19 between April 2020 and August 2021. The principals of the schools recommended three school teachers per school to participate in the interviews. Fifteen teachers were selected based on their knowledge of information and communications technology (ICT) integration in teaching and learning. There were 11 female and 4 male school teachers. The interview protocol was developed from the questions that arose from the literature analysis. The protocol had four open-ended questions:

- How does your school prevent cyberbullying from happening?
- How does your school protect learners from online fraud?
- How does your school protect learners from accessing or producing inappropriate content?
- How does your school protect learners from Internet addiction?

The interviews were conducted face to face between August 2021 and November 2021, at a time when schools in South Africa had resumed classroom teaching. Each interview lasted between 45 min and 60 min. Interviews were recorded with the permission of participants, transcribed verbatim and cleaned in preparation for analysis.

Data analysis was completed by the author with the help of a research assistant. The identities of the schools and participants were anonymised during data transcription. The five schools were given pseudonyms: A, B, C, D and E. The participants were given pseudonyms that reflected their school; for example, participants from school A were named Participant A1 and Participant A2; for school B, Participant B1 and Participant B2.

A deductive thematic analysis was employed in the data analysis phase.[33] Themes from literature analysis helped structure the deductive coding and served as priori themes; however, new themes that were observed were also recorded. Data familiarisation started during the transcription phase, and interesting ideas were captured. Coding and generation of themes was carried out independently between the two researchers and was recursive. The analysis involved three cycles of coding, generating and reviewing themes. This was followed by debriefing meetings between researchers to discuss and agree on the emanating themes from the analysis of the transcripts.

This study was limited by the fact that only private schools that implemented online learning during COVID-19 participated in the study. The perspectives of school teachers from schools that implemented online learning during COVID-19 could be different from those of teachers from schools that did not implement it. Schools that might not have implemented online learning during COVID-19 include rural and township schools in South Africa. However, the views of the participants are admissible because cyber-risks equally affect all learners who use online learning tools, irrespective of geographical location, race, culture, or economic status. Cyberattacks happen in virtual space, and anyone who is connected to the Internet is equally vulnerable to cybercriminals.

Ethical considerations

Ethical approval to conduct this study was obtained from the University of South Africa (UNISA) College of Science, Engineering and Technology's (CSET) Research and Ethics Committee (ref. no. 009/DNG/2019/CSET_SOC).

Results

This section presents the results from the analysed interview data. The results are presented under the following themes: (1) cyberbullying, (2) content risks, (3) online fraud, (4) awareness and (5) addiction.

Cyberbullying

The sampled school teachers acknowledged that cyberbullying was happening at their schools. To protect the learners from cyberbullying and put a stop to it, the schools have policies to guard against this. The teachers perceived their schools as having policies that safeguard learners when using Internet-connected devices. Policies at the schools compelled learners to only use Internet-connected devices under the supervision of school teachers. Participants from Schools B and D indicated that at enrolment, each learner is given the policy, which their parents sign. In this:

> 'Cyberbullying is rife amongst teenagers and that is just not acceptable, and we have zero tolerance of that. Our safe technology use policy keeps the learners safe. Learners are not given carte blanche to be on their devices all the time.' (Participant B5)

> 'The policy restricts bad things than the good things. It is a way to prevent all the bad things from happening, like cyberbullying, playing games and not doing schoolwork.' (Participant E13)

School D discouraged cyberbullying by persuading learners to speak out about any instances of bullying. Any learner at the school who has been bullied or witnessed anyone being bullied was to report to teachers. Reporting minimises bullying, and learners develop confidence to defend themselves:

> '… Yes. Issues of gender discrimination and bullying are things of the past and common in older age groups. My kids [*learners*] will quickly tell you, "Sir, you are being unfair." They speak out; that is a good thing.' (Participant D12)

Public display of penitence was used as a strategy for stopping cyberbullying at School E. It is a psychological strategy that converts perpetrators into advocates against bullying. The schools found the strategy more effective in stopping bullying than any other form of punishment:

> 'There is a lot of cyberbullying happening on social media groups, and that's a huge concern. What we did in the past when we picked up that there was cyberbullying, we took the girls who were involved, and they had to make a speech on cyberbullying in front of the whole school during assembly.' (Participant E15)

To make sure that cyberbullying does not happen at all, the learners were banned from using technological devices within the school premises at School C. Similarly, at other schools, learners were not given access to Wi-Fi, and learners could only use devices under the supervision of teachers:

> 'Even at school grounds, learners are not allowed to use their devices. The reason for that is the protection of the children and because we do not want cyberbullying to be taking place or them taking pictures and distributing them on social media when it's not moderated.' (Participant C8)

Content risks

All schools had restrictive policies that ensured that learners do not access or create harmful and inappropriate online content. The policies stop learners from taking pictures or videos and uploading them on social media or Internet in general. In that respect, one of the participants emphasised:

> 'I said, learners are not allowed to access Wi-Fi connection. This is to prevent them from using their tablets, laptops or cell phones from inappropriate use such as video recordings or taking pictures and uploading it on social media.' (Participant B6)

The teachers were aware that the Internet is an open repository of content where anyone can access anything, irrespective of age. To ensure that learners are protected from harmful or inappropriate online content, the schools restricted learners from having unsupervised access to Internet:

> '... Learners are not allowed to access Wi-Fi connection or Internet. This is to prevent them from Googling noneducational content. Learners are not allowed to use their tablet or a laptop or a cell phone unless they are supervised by a teacher.' (Participant C9)

> 'Due to typing in one wrong word and you end up in a bad site. You don't want to expose children to bad content; for example, you cannot give children a laptop connected to Internet and not supervise them. What are our children exposed to?' (Participant C7)

The strictness of the schools in protecting learners from inappropriate online content was stressed by a participant from School A, who underscored that the school operated under Christian ideology and had no room for misdemeanours:

> 'Yes, because we are a Christian school, we don't just allow free internet access by students, so obviously it's under supervision … We cannot allow our kids to access content that can be harmful to them.' (Participant A3)

School E was concerned about protecting learners from the misconduct of plagiarism. Learners are prone to copying and pasting content from the Internet and using it in their assignments without referencing. The teachers were aware that plagiarism discourages learners from achieving learning outcomes:

> '... for example, plagiarism is a big issue and is something that we picked up and we are strict on that. Plagiarism, copying and pasting have negative effects on the cognitive growth of kids.' (Participant E15)

Online fraud

Schools used software applications such as firewalls and antivirus software to protect learners from cyber-attacks.

Firewalls and antivirus software are essential for protecting learners from malware and hackers. Hackers are a threat to learning material, data and personal information. Firewalls are employed as filters to block websites considered undesirable for learners to visit, for example, social media sites that include Facebook, WhatsApp and Instagram:

> 'Our ICT policy gives clear guidelines to the learners as to which sort of websites should be avoided, and there are firewalls and antivirus technologies installed on all the computers to prohibit unsafe Internet usage.' (Participant A2)

> 'Not all the kids with smartphones have antivirus software. Whenever students share files, there is a risk.' (Participant E13)

Teachers from School D were concerned that learners would sometimes stray away from lessons to Internet browsing, gaming, or online chatting. Teachers get irritated by learners who do this as they end up getting lost during class. As a solution, Participant D11 suggested that schools should implement a classroom management system that can help with monitoring and controlling learners during classes:

> 'We need to implement a proper classroom management software to be able to monitor to see that everybody is where I want them to be … Sometimes I will be busy explaining and demonstrating, but someone at the back there is doing something else.' (Participant D11)

Awareness

The teachers were cognisant that ignorance of cybercrime would not spare learners from cyberattacks. To teach learners about cybersafety, Schools B and D integrated cyberawareness in their curriculums. The schools have a subject that is focused on teaching cybersafety:

> 'We have a subject for this at Grade 8 and 9, where learners attend once a week and learn about various mobile technologies, social media platforms and safety rules relating to that.' (Participant B5)

All the schools have cybersafety policies, and teachers are responsible for distributing and interpreting the policies to the learners. To make sure that the parents are aware of the policies, learners received the policies, which their parents signed. When new learners join a school, the teachers are responsible for explaining the policy to learners and their parents:

> 'Remember, if you come to school as a new kid, you are given the policies. It's something that we really discuss with the kid and the parent, to say, "The policy say[*s*] this and that, and it should be followed this way."'(Participant D11)

School D appointed cybersafety advocacy champions to teach about cybersafety to learners and teachers. The champions are tech-savvy teachers who committed themselves to teach about the dangers of cyberspace. They organise and drive seminars at the schools and are available to help learners with issues that pertain to cybersafety:

> '... because we have a policy, we had to appoint what we call a champion. A champion that drives the aspect of cybersafety at the school. Champion reports on the progress made at regular intervals.' (Participant D12)

Addiction

Learners need to be protected from excessive use of mobile devices, because that negatively affects learning. Teachers at School B disclosed that learners at most schools were struggling with handwriting because of excessive use of devices in learning. To improve the writing skills of learners, the schools were prohibiting the use of tablets:

> 'What is trending on social media now is that schools are ditching iPads [*and*] tablets, going back to pen and paper, because we are creating a generation which cannot write and read. (Participant B5)

The teachers revealed that when tablets were introduced at School C, some parents were against it, because they wanted their children to learn the basics of reading and writing. They did not want their children to learn by viewing videos or pictures. More so, the teachers indicated that parents were worried that their children will develop compulsive dependence on mobile devices. The teachers identified causes of mobile device obsession due to gaming, social media or texting:

> 'On one hand, technology is very good, and on the other hand, our children can't read anymore; they don't know how to read from books anymore because they just want to see the movies, pictures or play games. They can't read anymore.' (Participant C7)

In summary, most schools use different methods to ensure the safety of learners online. However, only two school policies seemed to provide guidance on how to ensure the online safety of learners. It is therefore important that school policies include all methods that should be used to protect learners online, provide direction and enforce compliance at the school.

Discussion

This section discusses the question, 'How can schools secure the cybersafety of online learners?' Through interviewing school teachers, data analysis revealed strategies that help with securing the cybersafety of online learners at South African high schools. Strategies for mitigating cybersecurity risks include enacting cybersafety policies at schools, stopping cyberbullying, stopping access to inappropriate content, cyber awareness and alleviating Internet addiction.

Enacting cybersafety policy

The first line of defence in securing the cybersafety of learners is to enact a policy. The enacted policy should identify cybersafety risks that learners will be exposed to and articulate prevention strategies and retributions. For example, this study identified cybersafety risks at schools as cyberbullying, inappropriate content, online fraud and Internet addiction. Prevention strategies against the risks were supervised access to devices, no access to Wi-Fi, no access to social media and confiscation of devices. Robertson and Corrigan[34] highlighted that learner supervision was fundamental to ensure safe, responsible and healthy use of technology in learning. However, the prevention strategies at the schools were strict, which indicate that schools are fearful of unethical cyberbehaviour of learners. It is advised that the design of cybersafety policies should support the use of technology in teaching and learning.[35] On the other hand, the policies should allow learners to grow naturally in the cyberenvironment that they live in and to develop resilience mechanisms to cyber-risks. To ensure that the enacted policies are implemented and followed, schools should run awareness campaigns to teach learners and their parents about cybersafety. Awareness is a strategy that has been used in technology adoption and has proved to work.[36] Moreover, the parents of learners should accept and sign the policy.

Stopping cyberbullying

To stop cyberbullying at the schools, it was established that the schools were employing strategies that included policies, speaking out (reporting), public penitence and banning of mobile devices. All the schools were strict on cyberbullying and made parents and their children sign the cyberbullying policy. The policies emphasised that learners can only use mobile devices under supervision and must not access the Internet when at school. Blocking Internet access ensures that learners do not access social media, platforms where most bullying happens. Prior research[37,38] found that effective cyberbullying prevention methods should include the creation of anticyberbullying policies and regulations that learners must comply with. Låftman et al. contended that good school leadership in containing cyberbullying is seen through good policies.[38]

Cyberbullying can be contained by encouraging learners to report on incidents that happen at schools. Reporting must be made by the victims who have been harassed or any learners who have witnessed the harassment. Witnesses of cyberbullying are encouraged to reprimand the perpetrator to stop harassing other learners, and they must report to the school. Data analysis established that the teachers perceived this strategy as effective in stopping cyberbullying. This finding supports a study[20] that found that cyberbullying can be controlled if bystanders and victims are encouraged to report bullying.

Public penitence by learners who are caught or reported for cyberbullying was found effective as a strategy. Students who are guilty of harassing other learners are made to make a public apology before the whole school, and the apology must be remorseful. Moreover, the guilty learner must be assigned an activist role, responsible for advocating for the cessation of cyberbullying at the school.

Blocking access to risk content

Learners must be protected from producing and accessing inappropriate content online. This study identified sources of harmful online content to be search engines, social media, blogs and websites in general. Harmful content that affects learners included hate speech, pornography and violent games. Data analysis revealed that learners can intentionally or accidentally access harmful content on the Internet or on social media. Learners can be protected from harmful content if they are digitally literate. A digitally literate learner has the knowledge and skills to critically analyse and evaluate content from the Internet.[26,39] Digital literacy of learners is determined by their cultural and academic background;[39] therefore, parents and teachers have a role to play in enhancing the digital literacy of learners.

Even though generating content for online sharing has been commended as an act of civic engagement and knowledge making,[40] the results of this study found that production of harmful content tarnishes the image of learners. If private content is shared, learners risk giving away personal information that can be misused by criminals. Sharing of private pictures or videos can go viral, which may destroy the reputation of the learner and can have negative psychological effects. Apart from producing personal content, learners can generate content in the form of violent games or suicidal content and share this on social media. Adolescents who consume and produce harmful content online and on social media have a high risk of engaging in the exact same behaviour in real life.[41]

To protect learners from accessing and producing harmful content, data analysis found that the schools used firewalls and antivirus software strategies, allowing learners to only access the Internet under teacher supervision, and banned learners from accessing social media. The strategies are restrictive mechanisms and protect the learners from cyber-risks. However, enforcing stringent cybersafety rules on children does not correct or prevent misbehaviour.[27] To encourage good cyberbehaviour, cybersafety strategies should be negotiated between the parents, children and the school.[21] Moreover, the protection strategies found in this study are school-bound and do not protect learners when they are at home. In this respect, learner supervision should go beyond the school premises and include parental supervision.[42] Therefore, inclusive strategies that protect learners are required at schools.

Cybersafety awareness

Learners are protected from cyber-risks if they are aware of threats, content and activities that compromise their safety. The results of data analysis revealed that learners can be conscientised about their cybersafety through training. Training raises awareness around good and bad digital etiquette and for learners to understand cybersafety policies. Cyberpolicies give guidance on what is ethical to do and help with reducing inappropriate cyber behaviour. The findings of this study are consistent with research that calls for the integration of cybersafety awareness within the school curriculum.[11] The cybersafety curriculum should be designed to change the behaviour of learners rather than just passing on cyberknowledge.[43] Learners are expected to gain practical knowledge that enables them to understand, analyse and manoeuvre within cyberspace. This is possible if the learners know the severity of cyber-risks that they can get exposed to. Cyber-risks identified in this study were consuming or producing inappropriate content, associating with strangers, sharing personal information online, cyberbullying and cyberaddiction. To defend learners from these risks, the curriculum should teach learners how to overcome the risks. Firstly, learners should be conscientised to know that they are the first line of defence in protecting themselves. Secondly, learners should know how to use technical cybersolutions for protecting themselves, for example, antiviruses, firewalls and software updates, just to mention the important ones. The findings of this study build on the study that found that if users have a greater cybersecurity awareness, they will have greater cybersecurity behaviours.[44]

The awareness interventions discussed are school-bound and did not extend out of school boundaries. Some research suggests that the best practice would be that cyberawareness be extended to parents, because they have the responsibility of protecting their children.[20] Hence, adolescents are best protected from cyberthreats if their knowledge is synchronised with that of their parents. If adolescents dominate cyberknowledge, it would be difficult for the parents to protect them. The cybersafety of learners can be improved if the above-discussed interventions are implemented.

Preventing addiction to Internet

Learners become addicted to Internet-connected devices, and they need to be protected from excessive use. Two symptoms of excessive device use were observed in this study. The, excessive use of tablets was observed to adversely affect the development of handwriting skills of learners. Secondly, overdependence on Internet-connected devices results in learners consulting the devices for anything, including Googling to find basic facts. These are cognitive-threating behaviours that need to be controlled in learning. This is in line with research that found that excessive use of online devices may result in reduced grades of learners.[45] Some research[17] found that cyberaddiction of children can be controlled if restrictive mediation strategies are employed, which is applicable to the cases observed in this study. To protect learners and to improve their writing skills, schools should limit the use of tablets at schools. Apart from restriction, Vondráčková and Gabrhelík[46] argued that learners can be protected from excessive use of connected devices by making learners aware of the negative consequences of addiction.

Future work

Future work on this study area should focus on two things: firstly, the construction of a cybersafety awareness model for teaching digital literacy and how to become a responsible digital citizen in online learning; secondly, providing strategies for securing remote access to learning content through student devices. Students use personal devices to access online study material, and some of the devices may be insecure.

Conclusion

This study identified cybersecurity risks and mitigating strategies for protecting learners when learning online. Cybersecurity risks identified were cyberbullying, online fraud, Internet addiction and inappropriate content. The mitigating strategies for these risks are centred around providing cybersafety policies at schools, conscientising learners about cybersecurity risks (awareness), stopping cyberbullying, discouraging the consumption or production of inappropriate content and protecting learners from Internet addiction. The first line of defence against these risks is for schools to implement cybersecurity policies. The policies should identify each of the potential risks and the mitigating strategies for overcoming the risks. After policies are approved, schools should run awareness campaigns to conscientise teachers, learners and parents about the contents of the policies. The cybersafety policies and the mitigating strategies should be cognisant of online learning advantages. That is, the policies and strategies should not block online learning at schools because of the fear of cybersecurity risks. Applying the mitigating strategies would secure the cybersafety of online learners, while at the same time promoting safe and responsible use of Internet-connected devices at schools.

The authors trust that these strategies will help schools and learners overcome cybersecurity risks. The strategies are applicable to all online learners, irrespective of geographical location, economic status, race, or culture, because information technologies create a global village that exposes online learners to the same cybersecurity risks.

Acknowledgements

The authors acknowledge the schools and teachers who participated in this research.

Competing interests

The authors declare that they have no financial or personal relationships that may have inappropriately influenced them in writing this article.

Authors’ contributions

B.C. conceptualised the study and carried out the literature analysis, data analysis and writing of the paper. G.D-N. managed the project, collected and analysed the data.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability

The data that support the findings of this study are available, upon reasonable request from the corresponding author, B.C.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any affiliated agency of the authors.

References

1. United Nations Children's Fund (UNICEF). Are children really learning? Exploring foundational skills in the midst of a learning crisis [homepage on the Internet]. 2022 [updated 2022 Mar; cited 2022 May 14]. Available from: https://data.unicef.org/resources/are-children-really-learning-foundational-skills-report/
2. Dayagbil FT, Palompon DR, Garcia LL, Olvido MMJ. Teaching and learning continuity amid and beyond the pandemic. Front Educ [serial on the Internet]. 2021;6:1–12 [cited 2022 Jun 14]. https://doi.org/10.3389/feduc.2021.678692
3. Nworie J. Beyond COVID-19: What's next for online teaching and learning in higher education. Educause Rev. 2021;11:10–21. https://doi.org/10.1038/s41928-020-00534-0
4. Lockee BB. Online education in the post-COVID era. Nat Electron. 2021;4(1):5–6.
5. Müller AM, Goh C, Lim LZ, et al. Covid-19 emergency e-learning and beyond: Experiences and perspectives of university educators. Educ Sci. 2021;11(1):19. https://doi.org/10.3390/educsci11010019
6. Maatuk AM, Elberkawi EK, Aljawarneh S, Rashaideh H, Alharbi H. The COVID-19 pandemic and E-learning: Challenges and opportunities from the perspective of students and instructors. J Comput High Educ. 2021;34:1–18. https://doi.org/10.1007/s12528-021-09274-2
7. Kaluarachchi C, Warren M, Jiang F. Responsible use of technology to combat cyberbullying among adolescents. Australas J Inf Syst. 2020;24:1–17. https://doi.org/10.3127/ajis.v24i0.2791
8. Cross D, Shaw T, Hadwen K, et al. Longitudinal impact of the cyber friendly schools program on adolescents' cyberbullying behavior. Aggressive Behav. 2016;42(2):166–180. https://doi.org/10.1002/ab.21609
9. Walters M, Gee D, Mohammed S. A literature review – Digital citizenship and elementary education. Int J Technol Educ. 2019;2(1):1–21.
10. Kritzinger E. Growing a cyber-safety culture amongst school learners in South Africa through gaming. S Afr Comput J. 2017;29(2):16–35. https://doi.org/10.18489/sacj.v29i2.471
11. Kritzinger E. Improving cybersafety maturity of South African schools. Information. 2020;11(10):471. https://doi.org/10.3390/info11100471
12. Scholtz D, Kritzinger E, Botha A. Cyber safety awareness framework for South African schools to enhance cyber safety awareness. Adv Intell Syst Comput. 2020;1226:216–223. https://doi.org/10.1007/978-3-030-51974-2_19
13. Von Solms, S and Von Solms, R. 2014. Towards cyber safety education in primary schools in Africa. In: Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014), Plymouth; 2014.
14. Patchin JW, Hinduja D. It is time to teach safe sexting. J Adolesc Health. 2020;66(2):140–143. https://doi.org/10.1016/j.jadohealth.2019.10.010
15. Newall M. Cyberbullying: A global advisor survey. Ipsos [homepage on the Internet]. 2018 [updated 2018 Jun; cited 2022 May 14]. Available from: https://www.ipsos.com/sites/default/files/ct/news/documents/2018-06/cyberbullying_june2018.pdf
16. Erişti B, Akbulut Y. Reactions to cyberbullying among high school and university students. Soc Sci J. 2019;56(1):10–20. https://doi.org/10.1016/j.soscij.2018.06.002
17. Ho SS, Chen L, Ng AP. Comparing cyberbullying perpetration on social media between primary and secondary school students. Comput Educ. 2017;109:74–84. https://doi.org/10.1016/j.compedu.2017.02.004
18. Sourander A, Klomek AB, Ikonen M, et al. Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study. Arch Gen Psychiatry. 2010;67(7):720–728. https://doi.org/10.1001/archgenpsychiatry.2010.79
19. Wang F and Zhou X. Persuasive Schemes for Financial Exploitation in Online Romance Scam: An Anatomy on Sha Zhu Pan (杀猪盘) in China. Victims & Offenders [serial on the Internet]. 2022: 1–28. [cited 2022 June 14]. Available from https://doi.org/10.1080/15564886.2022.2051109
20. De Kimpe L, Walrave M, Ponnet K, et al. Internet safety. In: Hoobs R, Milailidis P, editors. The international encyclopedia of media literacy. Hoboken, NJ: John Wiley and Sons, 2019; p. 1–11.
21. Muir K, Joinson A. An exploratory study into the negotiation of cyber-security within the family home. Front Psychol. 2020;11:424. https://doi.org/10.3389/fpsyg.2020.00424
22. Kumaran N, Lugani S. Protecting against cyber threats during COVID-19 and beyond [homepage on the Internet]. 2020 [updated 2020 Apr 16; cited 2014 Jun 14]. Available from: https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond
23. Paat Y, Markham C. Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. Soc Work Ment Health. 2021;19(1):18–40. https://doi.org/10.1080/15332985.2020.1845281
24. Bacıoğlu SD. Cyber risks awaiting children and young people in the 21st century. Psikiyatr Guncel Yaklasimlar. 2022;14(1):29–37. https://doi.org/10.18863/pgy.896800
25. Martin F, Wang C, Petty T, et al. Middle school students' social media use. J Educ Technol Soc. 2018;21(1):213–224.
26. Hague C, Payton S. Digital literacy across the curriculum. Curriculum Leadership [homepage on the Internet]. 2011 [updated 2011 Apr 08; cited 2014 June 14]. 9(10). Available from: http://www.curriculum.edu.au/leader/default.asp?id=33211&issueID=12380
27. Cassidy W, Faucher C, Jackson M. What parents can do to prevent cyberbullying: Students' and educators' perspectives. Soc Sci. 2018;7(12):251. https://doi.org/10.3390/socsci7120251
28. Mıhcı Türker P, Kılıç Çakmak E. An investigation of cyber wellness awareness: Turkey secondary school students, teachers, and parents. Comput Schools. 2019;36(4):293–318. https://doi.org/10.1080/07380569.2019.1677433
29. Bae S. The relationship between the type of smartphone use and smartphone dependence of Korean adolescents: National survey study. Child Youth Serv Rev. 2017;81:207–211. https://doi.org/10.1016/j.childyouth.2017.08.012
30. Chou H, Chou C. A quantitative analysis of factors related to Taiwan teenagers' smartphone addiction tendency using a random sample of parent-child dyads. Comput Hum Behav. 2019;99:335–344. https://doi.org/10.1016/j.chb.2019.05.032
31. Jeong S, Kim H, Yum J, Hwang Y. What type of content are smartphone users addicted to?: SNS vs. games. Comput Hum Behav. 2016;54:10–17. https://doi.org/10.1016/j.chb.2015.07.035
32. Ahmad N, Arifin A, Asma'Mokhtar U, et al. Parental awareness on cyber threats using social media. J Komuni: Malays J Commun. 2019;35(2):485–498. https://doi.org/10.17576/JKMJC-2019-3502-29
33. Braun V, Clarke V. Successful qualitative research: A practical guide for beginners. London: Sage, 2013.
34. Robertson L, Corrigan L. Do you know where your students are? Digital supervision and digital privacy in schools. Systemat Cybern Informat. 2018;16(2):36–42.
35. Moraes EB, Kipper LM, Kellermann ACH, et al. Integration of Industry 4.0 technologies with Education 4.0: Advantages for improvements in learning. Interact Technol Smart Educ. 2022. https://doi.org/10.1108/ITSE-11-2021-0201
36. Mohammad T, Hussin NAM, Husin MH. Online safety awareness and human factors: An application of the theory of human ecology. Technol Soc. 2022;68:101823. https://doi.org/10.1016/j.techsoc.2021.101823
37. Kavuk-Kalender M, Keser H. Cyberbullying awareness in secondary and high schools. World J Educ Technol: Curr Issues. 2018;10(4):25–36. https://doi.org/10.18844/wjet.v10i4.3793
38. Låftman SB, Östberg V, Modin B. School leadership and cyberbullying – A multilevel analysis. Int J Environ Res Public Health. 2017;14(10):1226. https://doi.org/10.3390/ijerph14101226
39. Hatlevik IK, Hatlevik OE. Students' evaluation of digital information: The role teachers play and factors that influence variability in teacher behaviour. Comput Hum Behav. 2018;83:56–63. https://doi.org/10.1016/j.chb.2018.01.022
40. Hooft Graafland J. New technologies and 21st century children: Recent trends and outcomes. OECD education working papers. Paris: OECD Publishing, 2018; p. 179.
41. George M. The importance of social media content for teens' risks for self-harm. J Adolesc Health. 2019;65(1):9–10. https://doi.org/10.1016/j.jadohealth.2019.04.022
42. Martin-Criado J, Casas J, Ortega-Ruiz R, Rey RD. Parental supervision and victims of cyberbullying: Influence of the use of social networks and online extimacy. Rev Psicodidáctica. 2021;26(2):160–167. https://doi.org/10.1016/j.psicoe.2021.04.002
43. Brittan T, Jahankhani H, McCarthy J. An examination into the effect of early education on cyber security awareness within the UK. In Jahankhani H, editor. Cyber criminology. Advanced sciences and technologies for security applications. Cham: Springer, 2018; p. 291–306.
44. Lee CS and Kim D. Pathways to Cybersecurity Awareness and Protection Behaviors in South Korea. Journal of Computer Information Systems [serial on the Internet]. 2022:1–13. [cited 2022 June 14]. Available from https://doi.org/10.1080/08874417.2022.2031347
45. Caldwell C, Cunningham T. Internet addiction and students: Implications for school counsellors [homepage on the Internet]. 2022 [updated 2022 Feb; cited 2022 May 14]. Available from: https://www.counseling.org/docs/default--ource/vistas/vistas_2010_article_61.pdf?sfvrsn=9f4a95cc_11
46. Vondráčková P, Gabrhelík R. Prevention of internet addiction: A systematic review. J Behav Addict. 2016;5(4):568–579. https://doi.org/10.1556/2006.5.2016.085