Eurasian Journal of Social Sciences, 10(1), 2022, 37-48
DOI: 10.15604/ejss.2022.10.01.004

EURASIAN JOURNAL OF SOCIAL SCIENCES

www.eurasianpublications.com

REDUCING CYBER INCIDENTS THROUGH GOOD ONLINE BEHAVIORAL NORMS: LESSONS FROM SOUTH AFRICA

Naume Sonhera
Vaal University of Technology, South Africa
Email: vnqume@vut.ac.za

David Mhlanga
Corresponding Author: The University of Johannesburg, South Africa
Email: dmhlanga67@gmail.com

Received: January 15, 2022 Accepted: March 9, 2022

Abstract

The phenomenon of cyber incidents has grown commonplace in schools throughout the world, including South Africa. Cyber mishaps are becoming more common, affecting both learners and parents, and expecting parents to supervise their children's online activity 24 hours a day is unrealistic. Several studies have highlighted several remedies, however even with such solutions, cyber incidents are still on the rise. As a result, the study aims to use a technical tool to investigate how cyber incidents can be reduced through good online behavioral norms which is an alternative strategy for reducing cyber occurrences among learners. Using the experimental action approach, the findings revealed that if learners are given alert messages that encourage them to consider appropriate behavioral standards, the number of learners who send hurtful messages may be lower than the number of learners who wish to send hurtful messages. As a result, the study suggests that educational institutions should step up their efforts to ensure that learners receive alarm messages that encourage them to consider appropriate behavior norms.

Keywords: Cyber Incident, Learners, Online, Behavior, Message, Application, Hurting

1. Introduction

Online antisocial behavior has increased as networks and technologies have grown (Laurie-ann *et al.* 2021). The incidence of cyber incidents has spread around the world, particularly in developing countries such as South Africa (Cilliers and Chinyamurindi, 2020; Cassidy *et al.* 2013; Kowalski *et al.* 2014; Hills, 2017). Cyber events are a global occurrence that has the potential to have a global impact on learners (Cilliers and Chinyamurindi 2020, Giménez-Gualdo *et al*. 2018). It is a widespread condition that affects not only learners but also adults in the community (Campbell *et al.* 2019; Abaido, 2020). Apart from being confined to cyber victims, cyber incidents have far-reaching consequences for all learners, the school climate, and the entire educational system (Estévez *et al.* 2019). As a result, expecting parents to supervise their children's online activity 24 hours a day is unrealistic. Cyber events should be identified and tackled as a social problem, rather than being dismissed as a random acts of mischief perpetrated by learners using technology (Abd Rahman *et al.* 2014). When cyber incidents are viewed as a societal issue, response strategies are more likely to be practical, successful, and thorough.

A cyber incident is a problem based on the complexity of the human mind that can evolve into dangerous behavior in tandem with technical advancements (Abd Rahman *et al.* 2014). The number of research attempts to explore cyber security and cyber-attacks has increased. Some of these studies, on the other hand, did not properly explain the measures that can be employed to reduce cyber occurrences. Cybercrime stories are on the rise, according to Lahcen *et al.* (2020), who say that they are trying to take advantage of online obscurity and the competitiveness of the business practices they deploy. According to Lahcen *et al.* (2020), a paradigm shift in the strategies and procedures utilized to fight these issues is required. One of the areas that Lahcen *et al.* (2020) revealed as the potential for combating cyber-crime is research on behaviour issues of cyber security. Lahcen *et al.* (2020) believe that more focus should be on social and behavioural issues to ensure that cyber-attacks are reduced. Safa *et al.* (2015) also argued that cyber security should be taken very seriously because the internet is now a basic commodity like electricity. If it is not available, businesses cannot operate. Just like Lahcen *et al.* (2020), Safa *et al.* (2015) believe that it is difficult for technology to guarantee a secure environment for the information, as a result, users' behavior must be taken as an important factor.

Another study by Li *et al.* (2019) revealed that society is facing cyber risks more than ever before due to the increase in the complexity and volume of internet and mobile applications. Li *et al.* (2019) went on to extend the published literature on cyber security by defining the domains of employees' security behavior as well as developing operational measures to advance information security behavior in the workplace. Safa *et al.* (2019) also supported Li *et al.* (2019) by arguing that the breaches in privacy and security violations are critical issues for people and organizations. Li *et al*. (2019) believe that one way to reduce the risks of cyber-attacks is to seriously consider the technological aspects of information security together with human issues. All the above studies posit that the human element is critical in reducing cyber risks. As a result, reminding learners of appropriate behavioral norms online could reduce cyber incidents among them. This paper aims to use a technical tool to investigate how cyber incidents can be reduced through good online behavioral norms. The tool will be used to assist learners in reducing the chances of sending hurting messages online. The rest of the paper is organized as follows: Section 2 describes the theoretical review followed by the third section which gives the empirical literature review. The methodology and the discussion of the results are in the fourth and fifth sections respectively. The last section gives the conclusion and policy recommendation.

2. Literature review

2.1. Theoretical literature review

In the literature on cyber occurrences, some hypotheses have gained a lot of attention and have been used to explain cyber incidents (Walker *et al.* 2013). The Social Norms Theory is based on the idea that erroneous impressions about how other individuals of a social group act or perceive an influence behavior (Espelage *et al.* 2013). According to the hypothesis, misperceived social norms might lead to behavior that exposes a victim to ridicule unnecessarily. Similarly, a learner may post hurtful remarks online, which is considered deviant behavior, because he or she believes it is appropriate.

Whatever technology technique is employed to combat cyber events, it must be remembered that the cyber incident problem is an interpersonal issue with a social context (Cowie and Myers, 2014). Personal variables and the social environment influence and are influenced by an individual's behavior. By moral rationale, online environments are considered as enabling cyber occurrences. Negative online behavior is influenced by social norms. People's opinions about the attitudes and behaviors that are typical, appropriate, or even required in each social setting are referred to as social norms (Cowie and Myers, 2014; Smith, 2012). People's views of these norms have a significant impact on their behavior in various situations. Learners are gradually normalizing online social aggressiveness, and they are growing desensitized to its negative consequences for others.

Cyberbullying has become accepted as a regular component of adolescent behavior (Acosta *et al.* 2019). The social presence theory is concerned with how people form bonds with one another when communicating (Sia *et al.* 2002). This theory assumes that a person can respond appropriately to another person based on their reaction, which is an important aspect of social development and maturity (Mark and Ratliffe, 2011). Online aggressors feel uninhibited due to the low level of social presence in digital communication and the anonymity of the internet (Willard, 2007; Kowalski *et al.* 2008; Hinduja and Patchin, 2009). As a result, cyber aggressors say and do things they would not necessarily say or do in real life (Tu, 2000; Joinson, 2001). Normal communication is difficult in the cyber world, according to the social presence theory, because there is a lack of instant feedback and learners and young people participating in cyber incidents cannot appropriately analyze each other's emotions (Mark and Ratliffe, 2011). As a result, online interaction becomes impersonal, resulting in less sensitivity and more antagonism (Shariff and Hoff, 2007).

2.2. Empirical literature review

In this study, a cyber event is defined as any criminal conduct committed by learners using electronic or digital means. A cyber incident occurs when someone sends out a series of hostile, hurtful, or aggressive messages with the intent of causing pain or discomfort to others or oneself (Hills, 2017). Learners are being educated about cyber events through educational materials provided by schools (Livingstone and Bulger, 2014). Cyber incident education is frequently mandated and offered during school assemblies or classroom courses, however, it is done distantly from where cyber events occur (Bulger *et al.* 2017). While instructional initiatives in response to cyber incidents are beneficial, they can be useless if they are divorced from the real event, both in terms of relevance and in terms of time and space. (Mhlanga, 2021a).

Most of the advice is so broad that it is not directly applicable. These solutions may or may not apply to a specific person or problem, and they are separate from the social networks where real contact occurs. Some solutions are created artificially and are not part of a learner's everyday life. They make little effort to prevent cyber accidents in naturally occurring scenarios where catastrophic injury is possible but might be avoided. Efforts, in the author's opinion, are mostly offline and lack clear practical solutions and recommendations. Technical solutions in social networking that automatically remind learners about behavioral norms, which can reduce the likelihood of sending hurtful comments online, have received little attention (Abd Rahman *et al.* 2014, Mhlanga, 2021b).

Whenever cyber incidents happen online, there is a potential for mitigation at the appropriate time and in the right place. Learners in general cannot engage correctly with one another online (Hills, 2017). While learners in South African schools are becoming more aware of the use of the internet, they are not becoming more aware of safe procedures when using ICTs (Kritzinger, 2016). Learners get inconsistent messages about online behavior as they seek digital literacy, and they do not always get the help they need (Kritzinger, 2016). According to Barlinska *et al.* (2013), enhanced empathy reduces the likelihood of learners becoming involved in cyber incidents.

The perpetrators will benefit from the greater empathy since they will be able to see how their acts can harm others. As a result, learners should be reminded of proper online behavior norms, as well as proper online communication and engagement (Barlinska *et al.* 2013; Cassidy *et al.* 2013; Hinduja and Patchin, 2014). Learners must be reminded of proper digital communication as well as the long-term ramifications of their online actions in the real world (Burton *et al.* 2016). They must recognize that damaging a learner's reputation through misleading remarks can jeopardize that learner's future (NoBullying.com, 2014). The long-term consequences of cyber incidents may be a dilemma for today's learners (Martin-Criado *et al.* 2021). Unless it is reported and removed, online information is permanent and public. It might be difficult to retrieve and eliminate internet threats that have been made or published. Because text, videos, and images are permanent, a victim may replay a harassing message multiple times or be reminded of the cyber incident by other young folks later (Mhlanga, 2020, Martin-Criado *et al.* 2021).

Due to their lower degree of maturity in capabilities such as thrill-seeking, impulse control, peer pressure, reward sensitivity, cognitive processing, and logical decision-making, learners are considerably more involved in cyber events than adults (Cohen-Almagor, 2018; Holfeld and Grabe 2012). Most parents of adolescents are aware of the peculiar behavior that adolescence tends to elicit. Parents frequently blame their children's bad behavior on their rising hormones. However, it turns out that an adolescent's prefrontal cortex, which is the part of the brain located just behind the forehead, is incapable of reasoning or making reasonable decisions in the same way that most adults are (Raisingchildren.net.au, 2019).

While young people's feet may cease growing by the end of high school, their brains may not, according to a neuroscience study. The brain does not fully mature until the early twenties (Raisingchildren.net.au, 2019). As a result, learners are more inclined to act on impulse rather than pausing to consider the repercussions of their actions before doing (Raisingchildren.net.au, 2019). According to Hills (2017), some messages made online by learners now may come back to haunt them tomorrow or later in life. Years later, hurtful words published online may prohibit some learners from getting jobs. Employers nowadays look for information (about qualified individuals) online before making a hiring decision. When it comes to cyber incidents, you cannot simply turn off the computer and anticipate everything will go back to normal. Even if the victim disconnects from the internet or other electronic devices, the cyber event can find its way back into the victim's school, office, or home. Using incorrect, inappropriate, or obscene language can produce resentment and damage a victim's or aggressor's reputation.

Siyam and Hussain (2021) argued that several colleges were to re-evaluate the material of their cyber-safety policies and examine it to ensure that it operates both within and outside of the school's grounds. Siyam and Hussain (2021) examined the cyber-safety policy of 20 private schools in Dubai, United Arab Emirates, and discovered that even though some schools are putting attention on cyber-safety issues, the emphasis remains on cyberbullying events. Siyam and Hussain (2021) also discovered that the formulation of cyber-safety rules lacks input from the relevant authorities, whose ultimate obligation is to create the main principles and regulations that schools must follow. According to Scott and Kyobe (2021), the volume of organizational cybersecurity risks is increasing every year because technology improves. Quite often, businesses believe that putting in place systems security controls such as firewalls and anti-virus software will eliminate cyber threats. However, even the most powerful security systems are subject to threats, according to Scott and Kyobe (2021). Factors that contribute to these hazards, such as human behavior, are often outside of an organization's control, according to Scott and Kyobe (2021). Again, Scott and Kyobe (2021) emphasized key cybersecurity management issues such as “risky security behaviors displayed by employees, social engineering, current limitations in machine learning insider threat detection, machine learning enhanced cyber threats, and the cybersecurity domain's underinvestment challenges”. Aderibigbe *et al.* (2021) also argued that cybertechnology has become a fundamental part of educational institutions, with the student’s routine to use these technologies to communicate, learn and play, causing a need for understanding the impact and general principles of ethical computer use in academia. The application of cyber ethics in these circumstances, according to Aderibigbe *et al.* (2021), has brought several obstacles to colleges and universities.

3. Research methodology

The research strategy employed was an experimental action approach, which was centred on the researcher and participants' cooperation and collaboration (Bergold and Thomas, 2012; Macdonald, 2012). It offered a space where people could get involved in the process and learn more about the consequences of hurting others online (Macdonald, 2012). The application tool was made for a school computer lab and was designed to assess learners’ inclination to transmit hurtful remarks via the internet. A timer was used to create a sense of competition like that found in online games or technical tools. The reward was offered as a technique for determining the factors that influence learners' cyber incident behavior and attitude. Popper (1945) suggested that social research must be performed as an experimental study, and this study followed the footsteps of Popper (1945) in conducting the experimental action research. Bozkus and Bayrak (2019) argued that action research, is normally conducted as action research in the format of social experiments. Adelman (1993) argued that most of Lewin's research took the form of "quasi-experimental and field investigations". There are several studies in the literature which studied action research experiments including Clark (1976); Burgoyne (1973); Krishnaswamy *et al*. (2009); Waardenburg *et al.* (2020); Koykka *et al.* (2019) among others.

4. Purposive sampling technique

Purposive sampling, also known as purposeful selection, was used to choose samples for this study (Maree, 2010). The study focused on learners in South African schools because the number of cyber incidents in schools is on the rise, and learners are often unaware of proper internet etiquette. Learners are the ones who suffer the most in cyberspace, whether they are active participants or passive observers (Hymel and Swearer, 2015). The sample included learners from a variety of schools and provinces across South Africa. Even though these learners were first-year university students, they still remembered high school cyber issues. In 2018, the University of Technology, where the students were enrolled, granted ethical permission for the project. Two tasks were completed to collect data. The overall sample consisted of 220 learners who took part in both the first and second tasks. Male learners outnumbered female learners by a small margin. Males made up 54 percent of the group, while females made up 46 percent. Most of the learners were between the ages of 19 and 20. (That is 54 male learners, which is equal to 25 percent of the learners). The learners' ages ranged from 17 to 22, with the majority being first-year students, who had just graduated from high school. The consenting sample numbers are listed in Table 1. There was no personal information gathered.

Table 1. Sample selection

Age	Male Learners	Female Leaners	Total
17	11	21	32
18	18	27	45
19	36	18	54
20	22	12	34
21	18	11	29
22	13	13	26
Total	118	102	220

Source: Author's own preparation

The overall portion of learners who were involved in the research was 220, as shown in Table 1. Male learners outnumbered female learners by a small margin. As previously stated, 54 percent of the population was male, and 46 percent was female.

4.2. Application design

The planned application tool for this study was installed in a computer lab that was connected to a server. For this experimental application, Windows 7 Professional, Windows 10 server, Xamp webserver for the virtual server, JAVA script, Netbeans, MYSQL Database, and PHP were utilized, as shown in Figure 1.

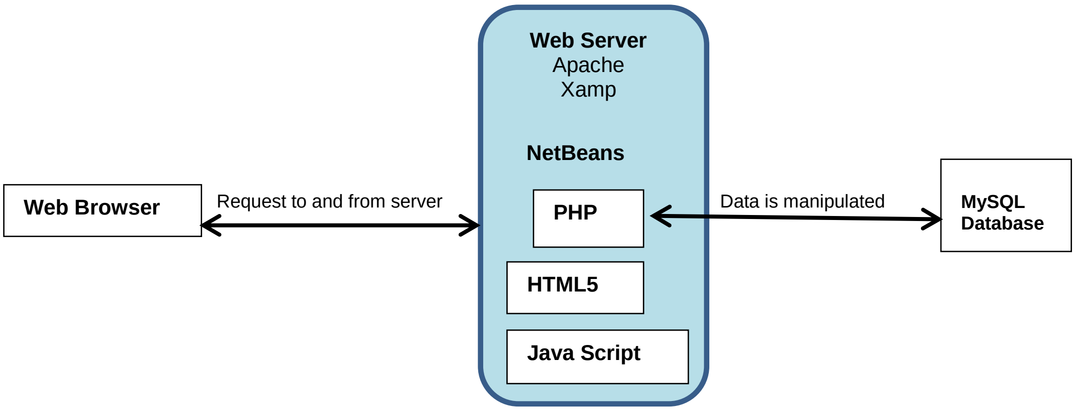

Figure 1. Application software linked together
Source: Author's own preparation

Completing two tasks was part of the experimental application. The first activity required learners to fill in a given blank space with a harsh statement to assess their willingness to transmit cruel communications online. Learners were given the option of posting the message by clicking "Yes" or "No." The application then detected a hurtful message by recognizing threatening or offensive terms inside a string of text after a learner clicked "Yes." After recognizing a hurtful term, an algorithm based on certain keywords in the database triggered a reflective alert message.

The learner was then prohibited from instantly sending the message. Noswearing.com was utilized to collect the hurtful words spoken during the experiment. When the system detected a potentially harmful message, it increased the "counter" of messages sent without being reconsidered or sent after reconsideration and resubmitting. The answers were recorded and preserved in a database. In practice, though, the learner will be allowed to send the threatening letter at his or her own risk. The experiment's second task involved incorporating the issue of incentives for the participants. The program included a reward system to encourage learners to feel accomplished after completing the process. The incentive was given to see what causes learners' cyber incident behavior and attitude to change. To keep the learner's attention, the experiment used a timing technique. At the end of the segment, the learners were given a grade.

5. Results and discussion

The data was compiled when the tasks were completed. To construct graphs, the data was exported from the MySQL database to Excel. The information was grouped into Figure 2 to Figure 3.

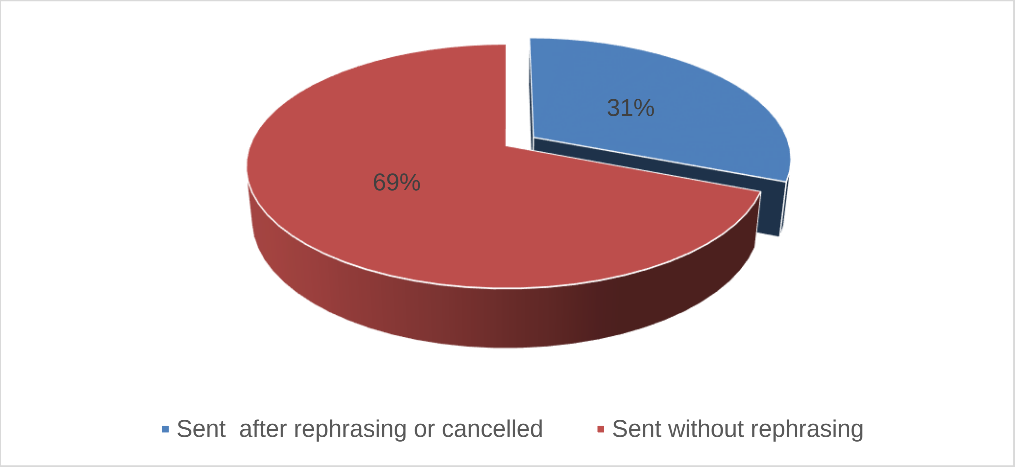

Figure 2. Task one with no incentive

The learners were not given any incentives during the experiment. 68 learners sent the message without rephrasing it, accounting for 31% of the total number of learners. 152 learners had their messages rephrased or canceled, representing a 69 percent rephrasing or cancelation rate.

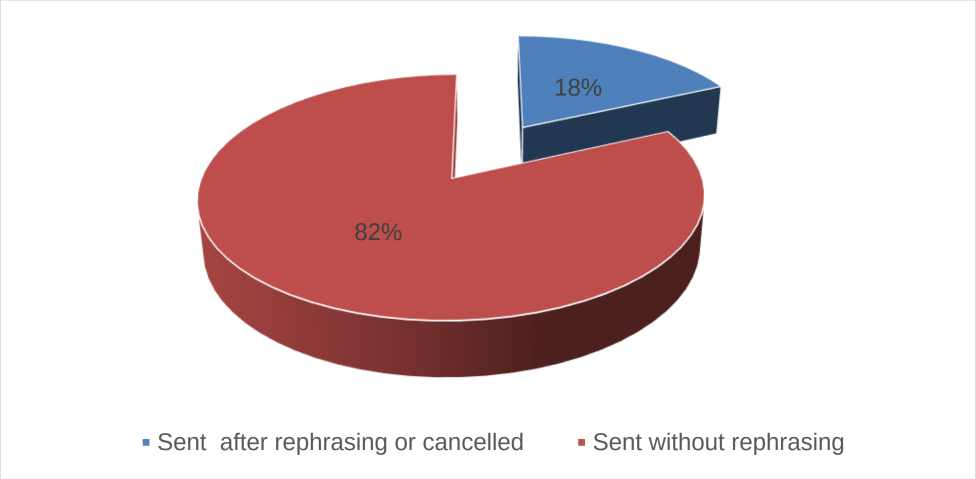

Figure 3. Task two with incentive

In task two, 180 learners sent the message without rephrasing, accounting for 82 percent of the total number of students. 40 learners rephrased or canceled their classes, accounting for 18% of the total. The practical exercises were created to assess learners' behavior and attitudes against transmitting hurtful messages. This experimental application has been built to assess the online behavior of the learners pleasantly, based on the theory of normative behavior, where attitudes and behavior are impacted by perceptions of social norms (Cowie and Myers, 2014).

The goal of introducing an application-based solution was to entice the younger generation to join by appealing to their curiosity about online applications while also gathering enough data about cyber incident behavior and attitude. There were 220 learners in all, 118 of whom were male and 102 of them female. Because this is a generation that has grown up with technology, learners had no difficulty using computers. The adoption of a technological tool provided the benefit of learners becoming quite familiar with digital communications nowadays. In task one, 69 percent of learners rewrote or deleted their hurtful messages. This occurred after the learners had received the pop-up warning forbidding them from sending hurtful remarks. Learners were encouraged to follow positive digital behavioral norms and proper internet etiquette because of the application. The goal was to provide learners with the opportunity to think about what they send online. Before sending nasty texts, learners were given a second chance to reconsider their decision. The program provided learners time to consider and reflect on their choices, after which they may choose to revise or delete their remarks entirely.

The advice was immediately actionable and had a significant impact on the outcome. Due to the incentive that was included, task two had different results in terms of percentages than task one. According to the findings, 82 percent of respondents sent the messages without rephrasing them. They did not even call to cancel. Learners wanted to win and receive a prize, which meant that the editing would take up some of their time. Only 18% canceled or rescheduled. The incentive was presented to see what causes learners' behavior and attitude when it comes to cyber issues. The timer was used to create a competitive environment, which is common in online technical tools (Abd Rahman *et al.* 2014, Martinez-Otero and Perez, 2015).

It has been demonstrated in the first task that providing learners with a mechanism to think about their decision before publishing harmful messages makes them less likely to send the hurtful message. The first activity lowered the number of unpleasant messages that learners were willing to write on the internet. The findings of the second test demonstrated that learners' ambition to win, to be great, and be popular can lead to cyber mishaps. The usage of a technological tool had the benefit of learners being familiar with digital communications. In some cases, people prefer digital communication to face-to-face conversation (Abd Rahman *et al.* 2014 Hills 2017). As a result, creating digital tools to educate learners on the right behavior will lessen cyber incidents while also providing digital solutions for a generation that is glued to screens. Fighting technology with technology may be the most effective way of preventing this prevalent and damaging behavior. Instead of having someone look over them, the tool might enable learners to make better decisions. According to the findings of this study, if learners are given alert messages that encourage them to reflect on good behavior standards before sending hurtful messages, the number of learners who send hurtful messages may be lower than those who do not. Negative remarks posted online may have simply been sent due to a lack of good judgment and logic, as well as hurried decisions, leaving the aggressor, the victim, or both, humiliated, injured, or tormented. Learners must be kind and respectful to one another online, whether they are sending an email, chatting in a chat room, or discussing in a forum. In any case, learners should treat one another as they would like to be treated.

In the same way that one should treat others with respect in the physical world, one should treat others with respect online. Learners may act rashly and send nasty, humiliating, and embarrassing messages online, which they may come to regret later. The usage of an application tool could be a proactive technological behavioral approach that allows learners to consider their actions before sending threatening or hurtful communications. One of the best strategies to prevent cyberbullying, according to Deletecyberbullying.org (2014), is to consider before publishing. Thus, the most effective strategy to prevent cyber incidents is to remind learners to pause and think before sending messages online, to consider their options and implications, and to choose to make the best judgments possible. The outcome of this application could serve as a starting point for developing better software for both preventing and detecting cyber events among South African learners. There are no guarantees that cyber events will not occur, however, there are steps that may be taken to decrease the number of cyber incidents. Because the program did not reach out to people most vulnerable to cyber incidents, the victims' voices were not heard. This is an essential topic to think about in the future.

6. Conclusion

The phenomenon of cyber incidents has grown commonplace in schools throughout the world, including in South Africa. The goal of this study was to employ a technical instrument to investigate how excellent online behavioral norms may help prevent cyber incidents. The study enlisted the participation of 220 freshly enrolled first-year university students from various schools and provinces. The rationale for selecting learners was forced by the rise in cyber events in South African schools, even though most learners are unaware of proper internet etiquette. Learners, whether active participants or bystanders are the ones who are most affected in cyberspace. According to the findings, if learners are given alert messages that encourage them to consider appropriate behavior standards, the number of learners who send hurtful messages may be lower than the number of learners who wish to send hurtful messages. Thus, the most effective strategy to prevent cyber incidents is to remind learners to pause and think before sending messages online, to consider their options and implications, and to choose to make the best judgments possible. The outcome of this application could serve as a starting point for developing better software for both preventing and detecting cyber events among South African learners. As a result, the study suggests that educational institutions should step up their efforts to ensure that learners receive alarm messages that encourage them to consider appropriate behavior norms.

The research was carried out at the Vaal University of Technology in South Africa. To get the most out of the study, it will be an academic initiative to expand it to all schools in South Africa and Africa.

References

Abaido, G. M., 2020. Cyberbullying on social media platforms among university students in the United Arab Emirates. *International Journal of Adolescence and Youth*, 25(1), pp. 407-420. https://doi.org/10.1080/02673843.2019.1669059

Abd Rahman, N., Razali, N. S., Ali, S. A. M., Malim, N. H. A. H., Husin, M. H., and Singh, M. M., 2014. Digital etiquette: educating primary school children via mobile game application. In: Proceeding of Knowledge Management International Conference (Kmice) 2014, Vols 1 and (Vol. 2, pp. 676-681).

Acosta, J., Chinman, M., Ebener, P., Malone, P. S., Phillips, A., and Wilks, A., 2019. Understanding the relationship between perceived school climate and bullying: A mediator analysis. *Journal of School Violence*, 18(2), pp. 200-215. https://doi.org/10.1080/15388220.2018.1453820

Adelman, C., 1993. Kurt Lewin and the origins of action research. *Educational Action Research,* 1(1), pp. 7-24. https://doi.org/10.1080/0965079930010102

Aderibigbe, N., Ocholla, D., and Britz, J., 2021. Differences in the ethical cyber behavioural intention of Nigerian and South African students: A multi-group analysis based on the theory of planned behaviour. *Libri,* 71(4), pp. 389-406. https://doi.org/10.1515/libri-2019-0062

Barlinska, J., Szuster, A. and Winiewski, M., 2013. Cyberbullying among adolescent bystanders: Role of the communication medium, a form of violence, and empathy. *Journal of Community & Applied Social Psychology,* 23(1), pp. 37–51. https://doi.org/10.1002/casp.2137

Bergold, J. and Thomas, S., 2012. Participatory research methods: A methodological approach in motion. *Forum Qualitative Sozialforschung / Forum : Qualitative Social,* 13(1), pp. 1–27.

Bozkus, K., and Bayrak, C., 2019. The application of a dynamic teacher professional development approach through experimental action research. *International Electronic Journal of Elementary Education*, 11(4), pp. 335-352. https://doi.org/10.26822/iejee.2019450792

Bulger, M., Burton, P., O'Neill, B., and Staksrud, E., 2017. Where policy and practice collide: Comparing United States, South African and European Union approaches to protecting children online. *New Media & Society*, 19(5), pp. 750-764. https://doi.org/10.1177/1461444816686325

Burgoyne, J. G., 1973. An action research experiment in the evaluation of a management development course. *The Journal of Management Studies,* 10(1), pp. 8-14. https://doi.org/10.1111/j.1467-6486.1973.tb00497.x

Burton, P., Leoschut, L. and Phyfer, J., 2016. South African kids online: A glimpse into children's internet use and online activities, Cape Town. [online] Available at: <http://www.cjcp.org.za/uploads/2/7/8/4/27845461/south_africa_kids_online_full_report.pdf> [Accessed on 21 November 2021].

Campbell, M., Whiteford, C., and Hooijer, J., 2019. Teachers' and parents' understanding of traditional and cyberbullying. *Journal of School Violence,* 18(3), pp. 388-402. https://doi.org/10.1080/15388220.2018.1507826

Cassidy, W., Faucher, C. and Jackson, M., 2013. Cyberbullying among youth: A comprehensive review of current international research and its implications and application to policy and practice. *School Psychology International,* 34(6), pp. 575–612. https://doi.org/10.1177/0143034313479697

Cilliers, L., and Chinyamurindi, W., 2020. Perceptions of cyber bullying in primary and secondary schools among student teachers in the Eastern Cape Province of South Africa. *The Electronic Journal of Information Systems in Developing Countries*, 86(4), e12131. https://doi.org/10.1002/isd2.12131

Clark, A. W., 1976. *Experimenting with organizational life: The action research approach*. New York: Plenum. https://doi.org/10.1007/978-1-4613-4262-5

Cohen-Almagor, R., 2020. Cyberbullying, moral responsibility, and social networking: Lessons from the Megan Meier tragedy. *European Journal of Analytic Philosophy,* 16(1), pp. 75-98. https://doi.org/10.31820/ejap.16.1.4

Cowie, H. and Myers, C., 2014. Bullying amongst university students in the UK. *International Journal of Emotional Education,* 6(1), pp. 66–75.

Deletecyberbullying.org, 2014. Delete cyberbullying - Preventing cyberbullying. [online] Available at: <http://www.deletecyberbullying.org/preventing-cyberbullying/> [Accessed on 1 March 2019].

Espelage, D. L., Rao, M. A. and Craven, R. G., 2013. Theories of cyberbullying. In: S. Bauman, D. Cross, and J. Walker, eds. 2013. *Principles of cyberbullying research: Definitions, measures, and methodology*. Milton Park: Routledge/Taylor & Francis Group. pp. 49-67.

Estévez, E., Estévez, J. F., Segura, L., and Suárez, C., 2019. The influence of bullying and cyberbullying in the psychological adjustment of victims and aggressors in adolescence. *International Journal of Environmental Research And Public Health*, 16(12), 2080. https://doi.org/10.3390/ijerph16122080

Giménez-Gualdo, A. M., Arnaiz-Sánchez, P., Cerezo-Ramírez, F., and Prodócimo, E., 2018. Teachers' and students' perception about cyberbullying. Intervention and coping strategies in primary and secondary education*. Comunicar. Media Education Research Journal*, 26(56), pp. 29-38. https://doi.org/10.3916/C56-2018-03

Hills, C. A., 2017. *Developing a law and policy framework to regulate cyber bullying in South African schools.* Doctoral dissertation. University of South Africa.

Hinduja, S. and Patchin, J. W., 2009. *Bullying beyond the schoolyard: Preventing and responding to cyberbullying.* Thousand Oaks, CA: Sage Publications (Corwin Press).

Hinduja, S. and Patchin, J. W., 2014. Cyberbullying: Identification, prevention, & response. *Cyberbullying Research Center.* [online] Available at: <http://cyberbullying.org/Cyberbullying-Identification-Prevention-Response.pdf> [Accessed on 1 March 2019].

Holfeld, B. and Grabe, M., 2012. 'Middle school students' perceptions of and responses to cyberbullying. Special issue (Digital Pathologies). *Journal of Educational Computing Research*, 46(4), pp. 395-413. https://doi.org/10.2190/EC.46.4.e

Hymel, S. and Swearer, S. M., 2015. Four decades of research on school bullying: An introduction. *American Psychologist*, 70, pp. 293-299. https://doi.org/10.1037/a0038928

Joinson, A. N., 2001. Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European Journal of Social Psychology*, 31(2), pp. 177-192. https://doi.org/10.1002/ejsp.36

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., and Lattanner, M. R., 2014. Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin,* 140(4), 1073. https://doi.org/10.1037/a0035618

Kowalski, R. M., Limber, S. P. and Agatston, P. W., 2008. *Cyberbullying: Bullying in the digital age*. 2nd eds. New Jersey: John Wiley & Sons. https://doi.org/10.1002/9780470694176

Koykka, K., Absetz, P., Araújo-Soares, V., Knittle, K., Sniehotta, F. F., and Hankonen, N., 2019. Combining the reasoned action approach and habit formation to reduce sitting time in classrooms: Outcome and process evaluation of the Let's Move It teacher intervention. *Journal of Experimental Social Psychology,* 81, pp. 27-38. https://doi.org/10.1016/j.jesp.2018.08.004

Krishnaswamy, K. N., Sivakumar, A. I. and Mathirajan, M., 2009. *Management research methodology: Integration of principles, methods and techniques*. New Delhi: Pearson Education India.

Kritzinger, E., 2016. Short-term initiatives for enhancing cyber-safety within South African schools. *South African Computer Journal,* 28(1), pp. 1-17. https://doi.org/10.18489/sacj.v28i1.369

Lahcen, R. A. M., Caulkins, B., Mohapatra, R., and Kumar, M., 2020. Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity,* 3(1), pp. 1-18. https://doi.org/10.1186/s42400-020-00050-w

Laurie-ann, M. H., Crespi, I., Hendry, B., and Fermani, A., 2021. Extending the Current Theorization on Cyberbullying: Importance of Including Socio-Psychological Perspectives. *Italian Journal of Sociology of Education*, 13(3), pp. 85-110.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., and Yuan, X., 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behaviour. *International Journal of Information Management*, 45, pp. 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Livingstone, S. and Bulger, M., 2014. A global agenda for children's rights in the digital age: Recommendations for developing Unicef's research strategy. *Journal of Children and Media,* 8(4), pp. 317–335. https://doi.org/10.1080/17482798.2014.961496

Macdonald, C., 2012. Understanding participatory action research: A qualitative research methodology option. *Canadian Journal of Action Research*, 13(2), pp. 34–50.

Maree, K., 2010. *First steps in research*. Pretoria: Van Schaikk.

Mark, L. and Ratliffe, K. T., 2011. Cyber worlds: New playground for bullying. *Computers in the Schools,* 28(2), pp. 92–116. https://doi.org/10.1080/07380569.2011.575753

Martin-Criado, J. M., Casas, J. A., Ortega-Ruiz, R., and Del Rey, R., 2021. Parental supervision and victims of cyberbullying: Influence of the use of social networks and online extimacy. *Revista de Psicodidáctica (English ed.),* 26(2), pp. 160-167. https://doi.org/10.1016/j.psicoe.2021.04.002

Martinez-Otero Perez, V., 2015. Bullying and cyber-bullying in a sample of high school students. *Revista de Currículum y Formación de Profesorado*, 21(3), pp. 277-298.

Mhlanga, D., 2020. Industry 4.0: The challenges associated with the digital transformation of education in South Africa. In: O. Aydin, ed. 2020.*The Impacts Of Digital Transformation*, Istanbul:Efe Academy. pp. 13-27.

Mhlanga, D., 2021a. Financial inclusion in emerging economies: The application of machine learning and artificial intelligence in credit risk assessment. *International Journal of Financial Studies*, 9(3), 39. https://doi.org/10.3390/ijfs9030039

Mhlanga, D., 2021b. The fourth industrial revolution and COVID-19 pandemic in South Africa: The opportunities and challenges of introducing blended learning in education. *Journal of African Education*, 2(2), pp. 15-43. https://doi.org/10.31920/2633-2930/2021/v2n2a1

NoBullying.com, 2014. *Cyberbullying in South Africa*. [online] Available at: <http://nobullying.com/cyberbullying-in-south-africa/> [Accessed on 1 March 2019].

Popper, K. R., 1945. *The open society and its enemies*. London: Routledge & Kegan Paul.

Raisingchildren.net.au, 2019. *Teenage brain development* | Raising Children Network, The Australian Parenting Website. [online] Available at: <https://raisingchildren.net.au/pre-teens/development/understanding-your-pre-teen/brain-development-teens> [Accessed on 1 March 2019].

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., and Sookhak, M., 2019. Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems*, 97, pp. 587-597. https://doi.org/10.1016/j.future.2019.03.024

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A. and Herawan, T., 2015. Information security-conscious care behaviour formation in organizations. *Computers & Security*, 53, pp. 65-78. https://doi.org/10.1016/j.cose.2015.05.012

Scott, J., and Kyobe, M., 2021. *Trends in cybersecurity management issues related to human behaviour and machine learning.* In: 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) IEEE. pp. 1-8. https://doi.org/10.1109/ICECET52533.2021.9698626

Shariff, S. and Hoff, D. L., 2007. Cyberbullying: Clarifying legal boundaries for school supervision in cyberspace. *International Journal of Cyber Criminology*, 1(1), pp. 76–118.

Sia, C., Tan, B. C. Y. and Wei, K., 2002. Group polarization and computer-mediated communication: Effects of communication cues, social presence, and anonymity. *Information Systems Research*, 13(1), pp. 70-90. https://doi.org/10.1287/isre.13.1.70.92

Siyam, N., and Hussain, M., 2021. Cyber-safety policy elements in the era of online learning: a content analysis of policies in the UAE. *TechTrends,* 65(4), pp. 535-547. https://doi.org/10.1007/s11528-021-00595-8

Smith, P. K., 2012. Cyberbullying and cyber aggression. In: S. R., Jimerson, A. B. Nickerson, M. J., Mayer, and J. Furlong, eds. 2012. *Handbook of school violence and school safety: International research and practice.* New York: NY: Routledge, pp. 93-103.

Tu, C., 2000. On-line learning migration: from Social Learning Theory to Social Presence Theory in a CMC environment. *Journal of Network and Computer Applications,* 23(1), pp. 27-37. https://doi.org/10.1006/jnca.1999.0099

Waardenburg, M., Groenleer, M., de Jong, J., and Keijser, B., 2020. Paradoxes of collaborative governance: investigating the real-life dynamics of multi-agency collaborations using a quasi-experimental action-research approach. *Public Management Review*, 22(3), pp. 386-407. https://doi.org/10.1080/14719037.2019.1599056

Walker, J., Craven, R. and Tokunaga, R. S., 2013. Principles of cyberbullying research: Definitions, measures, and methodology: Introduction. In: S. Bauman, D. Cross, and J. Walker, eds. 2013. *Principles of cyberbullying research: Definitions, measures, and methodology.* pp. 1-3.

Willard, N., 2007. *An educator's guide to cyberbullying and cyberthreats. Center for Safe and Responsible Internet Use (CSRIU).* [online] Available at: <http://csriu.org/cyberbully/documents/educatorsguide1.pdf> [Accessed on 1 March 2019].