Research Methods and Professional Practice Unit 7 Literature Review

Title: Implementing cybersecurity tools/techniques to reduce cyberbullying for students.

Research question: To what extent can cybersecurity tools and techniques reduce cyberbullying for students?

Contents

Introduction

The growing accessible landscape for social technology platforms and IoT devices has led to rising cases of students being easily targeted by cyberbullies. The student's health can be deeply affected physically, emotionally and socially, causing distress in academic performance and personal development.

Whilst many schools and agencies provide positive education frameworks in learning, there are gaps in how students can protect and support themselves to minimise impact. There is also limited scope in how cybersecurity tools and techniques can support the well-being of students.

The audience is aimed to be age-related students, parents, associated family members, academic and pastoral teaching staff, cybersecurity researchers and professionals.

Secondary sources were selected and acquired through online library databases and search engines. Use search tools such as "_" for key terminology + and – to add or remove unwanted search results.

The scope of the review will focus on students' cybersecurity practices, the relationship between online behaviour patterns and cyberbullying and the implementation of techniques and tools to manage cyberbullying.

Student practices towards cybersecurity

Cyberbullying can leave students feeling helpless and unable to escape the taunts that perpetrators direct at victims. Students with technology integrated into curriculums may feel there is no realm to remove themselves as institutions have more methods to reach their students. Therefore, students need to be cyber aware of practices and means to manage cyberbullying threats. The risk of being cyberbullied increases as students follow through year groups, particularly if they have been cyberbullied.

As discovered in North American studies, students who were cyberbullied in the early years of secondary education were more than three times more likely to be cyberbullied in the older year groups (Beran et al., 2012). In conjunction with this, we understand that the more time spent online, mainly using social media platforms, the higher the risk students are likely to experience cyberbullying (Çelik et al., 2012). The findings by Choi et al. (2019) support this view and further suggests that riskier behaviour patterns in online environments trend a link to a higher risk of cyberbullying victimisation.

Assessment using numerical measurement tool surveys such as 'The Ability to Ensure Personal Cybersecurity Scale' and 'Cyberbullying Awareness Scale' (Zorlu, 2022) suggests females in all probability to be cyber aware compared to males from a small survey 401 participants. A further limitation is that 75.1% of these participants were females, which suggests further research could be conducted. However, Zorlu (2022) indicates that there is little to no relationship between students deemed to be cyberbullying aware and cyberbullying other students.

In contrast, the view of Elçi & Seçkin (2019) indicates that users who have cyber awareness could be cyberbullying perpetrators. The study undertaken through quantitative methods used students who were technologically minded on an information system discipline course; identified responses of knowing cyberbullying takes place within the cohort and male students being considered more aware than female students (Elçi & Seçkin, 2019).

Nonetheless, Zorlu (2022) suggests from a quantitative study that students who regularly use the internet are more likely to be cyber-aware. In the United States, 46% of students aged 13-17 have experienced cyberbullying (Vogels, 2022), with older female students the more likely to report, which supports Zorlu (2022). Therefore we can deduce that educational lessons on personal security would benefit all users regardless of their assessed level of online protection knowledge.

Online lifestyle approaches and the risk of cyberbullying

Riskier behaviour would be deemed as providing personal information on social networks or online communities (Choi et al., 2019). The study by Choi et al. (2019) is helpful due to its person-centred approach, and we understand that the relationship between online lifestyles can influence cyberbullying victimisation.

However, the claims are limited to the location of the study and may not necessarily be a fair global representation of students' online lifestyle behaviours. The study itself was collected on predominately primary research, and limited secondary research has limited the overall analysis. The research gaps could be explored further. Therefore students require cyber awareness and privacy knowledge to mitigate potential cyberbullying.

Cybersecurity awareness may help mitigate the risks of cyberbullying, yet students' practices and trends in applying this must be consistent. Nicholson et al. (2021) findings using a mixed research method approach, found that generally, students' awareness was good and improved as expected after workshop training.

Educational training does emerge as a common mitigation strategy to reduce cyberbullying, yet parental responsibilities should not be overlooked. Gunduz et al. (2021) found that cyberbullying behaviour decreased as students grew in age. Students became more sensitive and careful regarding their behaviour with maturity; however, the study highlighted that parental education level and their involvement in technology guidelines for their child played a crucial mitigation role (Gunduz et al., 2021). Whilst the limitation of this study was based on one urban city school using quantitative method scales, we can take a helpful insight into the supportive parent/guardian role in reducing cyberbullying. The opportunity of a qualitative approach could have offered an understanding of the reasons for engaging in cyberbullying behaviour across the age range.

However, the inconsistency in the delivery of security messages means students often neglect to apply their personal security measures. Also, the usability of password managers and considering personal data privacy becomes cumbersome. So students implement it initially, then begin to disregard the security measures over time as they prefer the convenience of the software application rather than maintaining cybersecurity principles (Nicholson et al., 2021). Fagan et al. (2017) strengthen this view, concluding that users unfamiliar with the understanding of the password manager technology are less likely to use it due to security concerns and can emotively feel suspicious towards users of password managers. The lack of understanding of the cybersecurity tool suggests that educational training in the technology is needed for students to implement safer online behaviour (Fagan et al., 2017).

Implementing cybersecurity techniques/tools to manage to cyberbully

Cybersecurity tools can be practical to help mitigate the risks of cyberbullying. Quayyum et al. (2021) suggest that students generally understand managing their privacy online, which supports earlier claims by Nicholson et al. (2021). Nonetheless, students tend to have limited awareness, and in-depth granular research on student privacy cyber risk is lacking (Quayyum et al., 2021). Whilst this research offers evaluative research in quantitative and qualitative methods, the assessment tools to measure how effective cybersecurity tools or techniques in mitigation strategies are scarce.

The concept of merging entertainment and security concepts can be practical. However, studies indicate that through educational training, students can improve their awareness of risks if the methods are posed in an engaging and relevant manner. The use of interactive comics (Zhang-Kennedy et al., 2017) proved that students significantly improved their online behaviour and retained the key learning objectives over a week later. The training should be pitched at the intended age cohort of students to maximise engagement.

Despite this, to maintain the entertainment aspect, developers of interactive programs should be mindful of usability. Suppose the user interface is too simplistic and not challenging enough. In that case, users do not learn security concepts as effectively (Meng et al., 2012) and challenge earlier views by suggesting students trust social network applications to protect users when online, with additional training or awareness, deemed unnecessary. When considering the security, functionality and usability triangle (Bada et al., 2019), developers must consider students' usability at the forefront in planning not to demotivate or disengage learners.

Cyberbullying can result from the information students may disclose online. Students' online behaviours can commonly engage in gaming, discussions or social media. Therefore cybersecurity game-based learning programs have shown indications as an effective technique to raise awareness. A strength is evident in the studies suggesting that standalone applications with the development of motivation models can increase the performance of students' knowledge and understanding (Giannakas et al., 2019). However, the limitations of this study show that the findings came from elementary students rather than older-aged students.

Furthermore, whilst there seems to be limited development in cybersecurity tools and techniques to raise awareness for online behaviour, there are also very few resources for teachers and curriculum planning to deliver. The social network simulator study (Bioglio et al., 2019) was a fine example of a valuable tool to mitigate online behaviour risks which supported teachers but also highlighted the void in the development of teaching or parental material to support students. Choi (2015) provides supportive findings indicating that awareness programmes and online ethical practice guidelines should be introduced early in curriculums and adapted to a rapidly changing online landscape (Choi, 2015).

Conclusion

Cybersecurity tools and techniques play a significant role in supporting students in cyberbullying. Whist cyberbullying cannot be mitigated entirely, from carefully planned education training through gamification or interactive applications; cyberbullying can be reduced (Quayyum et al., 2021). Quayyum et al. (2021) research contributes significant findings in identifying approaches and technologies to develop students' knowledge in cyber protection.

Whilst this is valuable, the evident gaps in research remain regarding details on effective designs of interactive applications. The significant challenge to reducing cyberbullying is the students' consistency of application and retention of cybersecurity techniques to manage themselves online. Should students not adhere to learned practices, whether due to software application usability or ignorance, then the risk of cyberbullying remains exposed.

Furthermore, as the development of techniques and tools is still emerging, there is limited research on any adverse effects of using such tools or techniques on the student. In addition, there is no standardised, consistent definitive measurement tool to assess students' online behavioural awareness. Therefore whilst the research gaps remain, building a holistic profile of the student's learning needs with be limited. The first impression of the awareness training might be demotivating, or the learning may not embed. From a software developer's perspective, they will not have the data to design applications suitable for specific age groups of students.

The literature review is further justified by suggesting more research is required in the extended community involving parents, teachers or caregivers. In the UK, dedicated learning time on cybersecurity tools and techniques is not embedded across the curriculum and often has minimal time in particular subject areas (UK Council for Internet Safety, 2022). There are few supportive resources and guaranteed curriculum time in these areas.

Justification for this review can be considered further concerning assessment awareness tools. Without a standardised protocol measuring tool, normative data will unlikely be produced, which could support educators in understanding students' levels of awareness and be comparative across different backgrounds. This would help the validity and reliability of the data produced.

Furthermore, research into the current awareness programme's effects would also be beneficial with valid data. The extent of adverse effects, such as emotional or social distress, after completing such awareness programmes has very little research and consideration of the long-term behavioural change of the students in managing their own cyber awareness or bullying issues as they progress through schooling. This could support the well-being profiles of the student.

Following this review, the recommended outcomes would be to support research in developing standardised assessment tools and cyber awareness programmes. There could be different levels which would be student-centred and another for educators, parents or guardians. As part of the awareness programmes, the research could be conducted to understand the effects on the students after educational training.

Ensuing, an evaluation of the long-term behavioural changes of students in managing cyberbullying incidents either as victims or potential cyberbullies could be implemented.

References

Bada, M., Sasse, A. M. & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Available from: https://arxiv.org/abs/1901.02672 [Accessed 11 March 2023].

Beran, T., Rinaldi, C., Bickham, D. & Rich, M. (2012). Evidence for the need to support adolescents dealing with harassment and cyber-harassment: Prevalence, progression, and impact. *School Psychology International,* 33, 562-576.

Bioglio, L., Capecchi, S., Peiretti, F., Sayed, D., Torasso, A. & Pensa, R. G. (2019). A Social Network Simulation Game to Raise Awareness of Privacy Among School Children. *IEEE Transactions on Learning Technologies,* 12, (4): 456-469.

Çelik, S., Atak, H. & Erguzen, A. (2012). The effect of personality on cyberbullying among university students in Turkey. *Egitim Arastirmalari - Eurasian Journal of Educational Research*, (49): 129-150.

Choi, K.-S. (2015). *Cybercriminology and digital investigation*. LFB Scholarly Publishing.

Choi, K.-S., Cho, S. & Lee, J. R. (2019). Impacts of online risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimisation among Korean youth: Application of cyber-routine activities theory with latent class analysis. *Computers in Human Behavior,* 100, 1-10.

Elçi, A. & Seçkin, Z. (2019). Cyberbullying Awareness for Mitigating Consequences in Higher Education. *Journal of Interpersonal Violence,* 34, (5): 946-960.

Fagan, M., Albayram, Y., Khan, M. M. H. & Buck, R. (2017). An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences,* 7, (1): 12.

Giannakas, F., Papasalouros, A., Kambourakis, G. & Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. *Information Security Journal,* 28, (3): 81-106.

Gunduz, Ş., Akgun, F. & Özgur, H. (2021). Determination of Secondary School Students' Levels of Sensitivity towards Cyberbullying and Cyberbullying Behaviour. Available from: https://dergipark.org.tr/en/pub/per/issue/56834/722009 [Accessed 12 March 2023].

Meng, M., Zakaria, N., Bindahman, S., Asrol Alias, N. M. & Husain, W. (2012). "PrivacyDoc": A Study on Privacy Protection Tools for Children in SNS. *International Journal of Smart Home,* 6, (3): 41-48.

Nicholson, J., Terry, J., Beckett, H. & Kumar, P. (2021). *Understanding Young People's Experiences of Cybersecurity*. *Proceedings of the 2021 European Symposium on Usable Security.* Karlsruhe, Germany: Association for Computing Machinery.

Quayyum, F., Cruzes, D. S. & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction,* 30, 100343.

Uk Council for Internet Safety. (2022). Online safety in schools and colleges: Questions from the Governing Board (2022). Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1105569/Online_safety_in_schools_and_colleges.Questions_from_the_Governing_Board__2022_.pdf [Accessed 11 March 2023].

Vogels, E. (2022). Teens and Cyberbullying 2022. Available from: https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/ [Accessed 11 March 2023].

Zhang-Kennedy, L., Baig, K. & Chiasson, S. (2017). Engaging Children About Online Privacy Through Storytelling in an Interactive Comic. Available from: https://www.scienceopen.com/hosted-document?doi=10.14236/ewic/HCI2017.45 [Accessed 11 March 2023].

Zorlu, E. (2022). An Examination of the Relationship between College Students' Cyberbullying Awareness and Ability to Ensure their Personal Cybersecurity. *Journal of Learning and Teaching in Digital Age*.