Journal of Information Systems Engineering and Management
2025, 10(1s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cyberbullying Prevention in Online Games: Implementation of Malaysia Cyber Security Strategy (MCSS) through Awareness and Education

Muhammad Fakhru Rizuan Che Omar[1], Noor Aziah Abdullah[2], Mohd Nizam Saad[3], Nurulhuda Ibrahim[4]

[1]*Universiti Utara Malaysia, Malaysia. fakhru.rizuan@gmail.com*

[2,3,4]*Senior Lecturer, School of Multimedia Technology and Communication, Universiti Utara Malaysia, Malaysia*

ARTICLE INFO

Received: 02 Oct 2024

Revised: 30 Nov 2024

Accepted: 15 Dec 2024

ABSTRACT

Cyberbullying is a growing concern, particularly among adolescents and children, with the increased variety of online games available. It has been linked to various mental health problems, including social anxiety, depression, and suicidal thoughts. The purpose of this study is to explore the implementation of awareness and educational strategies within Malaysia's Cyber Security Strategy (MCSS) framework to prevent cyberbullying in online games. A semi-structured interview was conducted with four experts from various fields. The discussion revealed that the government should develop a prevention curriculum that addresses cyberbullying in online games through simulation, using viral short videos as learning materials. The government should strengthen and promote a self-regulation campaign to ensure adolescents' safety while playing online games. The commitment from peer support groups and partnerships with gaming influencers helps raise awareness about cyberbullying in online games. These findings contribute to understanding how educational and awareness strategies can be effectively implemented to combat cyberbullying in online games among Malaysian adolescents.

Keywords: Cyberbullying Behavior, Online Games, Malaysia Cybersecurity Strategies, Adolescent.

INTRODUCTION

The widespread adoption of smartphones and constant internet connectivity has transformed gaming and social interactions, particularly among youth. An impressive 95% of teenagers have access to smartphones, and a staggering 88% engage with them regularly by playing online games (Anderson & Jiang, 2018). This mobile-centric gaming society has raised some serious questions about safety because the online nature of these games makes players and their interactions much more visible—and much more vulnerable—to potential cyberbullying. Studies revealed that younger children, with their relative lack of experience and innate trustfulness, may be especially at risk for online and gaming-related dangers (Ortega-Barón et al., 2021). Players' experiences can sometimes be tricky to discuss (Hidayat et al., 2022). A survey about those big online multiplayer games showed that roughly half the folks said they had been bullied over the online platform. Interestingly, just over a third admitted to dishing out some cyberbullying while gaming (Ballard & Welch, 2017).

Cyberbullying through screens could look like mean words thrown around casually, arguing for fun or not-so-fun reasons, and making others feel small with gossip and lies (Huang et al., 2021; Kou, 2020; McLean & Griffiths, 2019). At the same time, all this is often considered part of the game's excitement for many people who play it frequently because there is an easy way to send nasty notes or spread mean stories using in-game tools (Fryling, 2018). The amount of time one spends on these digital games has something to do with how often cyberbullying happens – maybe because of anonymity. Folks sometimes cannot see who is doing what behind those screens, so figuring stuff out is challenging (McInroy & Mishna, 2017). According to research, by type of game, well—games called Multiplayer Online Battle Arena (MOBAs), where players team up, tend toward fostering such negativity

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

more than others, perhaps simply due to the potentially intense nature within them notably speaking (Wan Ahmad et al.,2022).

The effect of cyberbullying in online games is far-reaching and can have significant consequences for the individuals involved and the gaming community as a whole (Wang & Ngai, 2021). Research has shown that cyberbullying can have a profound psychological impact on its victims, leading to increased levels of stress, anxiety, and depression (Huang et al., 2021; Ijachi, 2019). Persistent harassment, humiliation, and disparaging remarks in online gaming settings foster a hostile and toxic environment, adversely impacting the mental and emotional health of affected persons (Ekiciler et al., 2022; Kordyaka et al., 2022). Research indicates that victims of in-game cyberbullying endure verbal abuse in gaming lobbies and chats, as well as intentional disruption of their gameplay through sabotage (Kurt, 2020).

Dealing with and reacting to cyberbullying in online games is necessary for encouraging a safer gaming environment and it promotes a more all-embracing atmosphere (Barlinska et al., 2018). Experts have suggested varied tactics and interventions to address cyberbullying while acknowledging its complications (Hayashi & Tahmasbi, 2022). A realistic strategy involves creating wide-ranging preventative programs that educate gamers about the effects of cyberbullying and promote empathy and respectful behavior. Awareness campaigns training modules and interactive workshops may be included in these programs to cultivate a feeling of responsibility and ethical behavior among gamers. Technical treatments such as chat filters reporting systems and moderation tools actively identify and reduce cyberbullying. Integrating educational and technical solutions promotes a more pleasant and supportive gaming environment and it deters cyberbullying behavior (Verschueren et al., 2019).

The Cyber Security Strategy for Malaysia from 2020 to 2024 comprises five key components and twelve strategies that aim to strengthen the country's cybersecurity posture (MCSS, 2020). This plan lays out what the National Cyber Security Agency (NACSA) wants to do over this period and an organization's cybersecurity strategy for success. To NACSA, these elements translate their vision into action. The five components are (1) effective governance, (2) legislative framework and enforcement, (3) innovation and growth of the cybersecurity industry, (4) capacity building, awareness, and education, and (5) global collaboration. The idea of keeping things safe in Malaysia's digital space is crucial. Still, these plans are not just there to slap on rules like preventing mean comments in online games. Some unique methods around digitally keeping things secure can help reduce bullying vibes during gaming by being all-inclusive. This study examines the implementation of awareness and education strategies under Malaysia's Cyber Security Strategy (MCSS) framework to prevent cyberbullying in online gaming environments. Piecing together what has been found from these various studies aims to pick out MCSS, which could be used to avoid cyberbullying behavior. Ultimately, based on our research queries, we hope to create an effective plan to make sense of and tackle cyberbullying behavior in online gaming.

Cyberbullying Behavioral in Online Games

The popularity of online gaming has been paralleled by the rise of cyberbullying as an essential issue within the gaming community (Huang et al., 2021; Mishna et al., 2022). Cyberbullying in online games takes several forms, such as sending abusive messages, making hurtful and slanderous remarks, spreading untrue rumors, and engaging in various kinds of hate speech and hate acts (Ijachi, 2019). In Malaysia, the prevalence of cyberbullying is particularly concerning, leading Malaysia to rank second in Asia for cyberbullying among youth (Bernama, 2020). Some elements that can lead to cyberbullying behavior are games that contain pornographic, violent, and addictive content (Noridayu et al., 2022). The Malaysian Communications and Multimedia Commission revealed 11,235 gripes about online trouble in just the first half of 2020 (Bernama, 2020). These statistics show that online platforms, including online games, are mediums for conducting cyberbullying.

Research reveals that 28% of Malaysian youngsters have experienced internet violence (Razali et al., 2022). A study conducted in Selangor revealed minimal participation in cyberbullying behaviors among adolescents, with banning instant messaging platforms being the predominant method (Saharrudin et al., 2019). Other research indicates a significant incidence of cyberbullying among Malaysian adolescents, with online harassment being the most common kind (Sivabalan et al., 2020). Cyberbullying in online gaming typically involves three primary roles: the perpetrator, the bystander, and the victim (Barlinska et al., 2018). The offenders often exploit the anonymity of the Internet to locate and harm individuals (Zhao et al., 2023). Bystanders can either aggravate or alleviate the situation through their actions or lack thereof. Victims experience mental distress and social alienation, frequently

feeling impotent against bullying (Hellfeldt et al., 2020). The ramifications of cyberbullying range from significant psychological damage, such as anxiety, sadness, and suicidal thoughts (Andrea & Yuliati, 2019; Zhu et al., 2020), to wider effects on gaming communities (Ekiciler et al., 2022). Such acts may also represent legal infractions, especially in instances of harassment and hate speech (Fryling et al., 2015). This study aimed to mitigate bullying issues in online gaming and to assure gamers' safety during gameplay.

Malaysia Cyber Security Strategies (MCSS)

Cybersecurity includes the activities, processes, skills, and conditions necessary to safeguard information and communication systems, as well as the data they hold, against harm, unauthorized access or alteration, and exploitation (Galinec et al., 2017). From a preventative measures standpoint, tackling violent behavior on online platforms necessitates a comprehensive strategy that integrates technology solutions, user education, and policy enforcement (Kavak et al., 2021). The Malaysia Cyber Security Strategy 2020-2024 is an extensive framework delineating the components and tactics to bolster cybersecurity in Malaysia (Majlis Keselamatan Negara, 2020). In the Malaysia Cybersecurity Strategy 2020-2024 (MCSS), Ariffin et al. (2021) concentrated on the fourth of the five strategic pillars, which underscores the enhancement of capacity, capability, awareness, and education via three strategic initiatives aimed at mitigating cyberbullying on social media (refer to Figure 1). This study concentrates on mitigating cyberbullying in online games via pillar 4 of the MCSS.

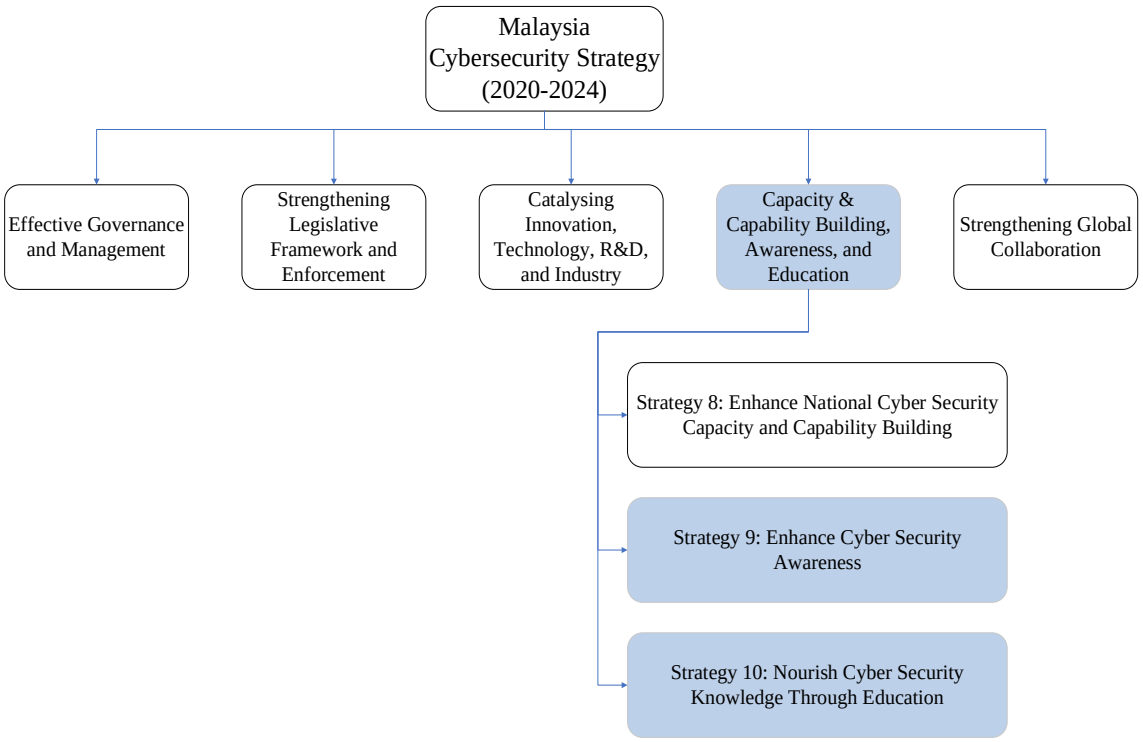

Figure 1: The Pillars of Malaysia Cybersecurity Strategy (MCSS)

This study analyzes the execution of awareness and educational methods under Pillar 4 of Malaysia's Cyber Security Strategy (MCSS) framework aimed at preventing cyberbullying in online gaming contexts. This focused strategy, endorsed by Ariffin et al. (2021), highlights knowledge dissemination and behavioral modification as essential elements in promoting safer digital environments. The choice of awareness and education tactics is particularly pertinent as they directly tackle the preventive dimension of cyberbullying by equipping users with information and comprehension of digital citizenship. This emphasis corresponds with the viewpoints of the study participants, who frequently underscored the significance of awareness and education in mitigating cyberbullying occurrences in online gaming contexts. Additionally, these tactics provide extensive engagement with various stakeholders, including gamers, parents, educators, and game producers, thereby advancing the MCSS framework's objective of fostering a more informed and responsible digital society.

Cyberbullying and Cyber Security Awareness

A study on cyberbullying and cybersecurity awareness in online gaming uncovers notable results and identifies study constraints. Research conducted in Malaysia by Nurul Ain and Nooraini (2019) revealed significant deficiencies in youths' comprehension of online privacy, despite their frequent internet usage. Awareness initiatives utilizing social media have demonstrated more efficacy than traditional methods (Ye et al., 2020), and peer influence along with gaming personalities considerably affect online behavior (Kaloeti et al., 2021). Collaborative strategies involving educational institutions, game developers, and cybersecurity organizations yield more effective outcomes in mitigating cyberbullying (Siddiqui & Schultze-Krumbholz, 2023). Nonetheless, researchers encounter significant obstacles. The anonymity of gaming platforms hinders the assessment of prevention program efficacy (Manzuoli et al., 2019). Cultural disparities and regional discrepancies in definitions of cyberbullying impede uniform preventative initiatives (Timotheou et al., 2023). The ongoing advancement of gaming platforms generates new avenues for cyberbullying that existing awareness initiatives find challenging to tackle (Cui et al., 2022). Furthermore, current prevention measures struggle to engage younger gamers, who frequently eschew formal awareness initiatives and are reluctant to report incidences of cyberbullying.

Cyberbullying and Cyber Security Knowledge Through Education

Recent studies reveal significant advancements in educational strategies for cyberbullying prevention and cybersecurity awareness. School-based preventative initiatives have successfully enhanced digital literacy and reduced incidences of online harassment (Tanrikulu, 2018). A subsequent study indicates that integrating cybersecurity awareness into current curricula has enhanced students' online safety behaviors (Ezedy et al., 2024). Research on peer-led initiatives illustrates their efficacy in promoting constructive online conduct among youth (Lukács J et al., 2023). The research underscores the essential function of well-qualified educators in fostering safe digital learning environments (Panosso et al., 2023). Current research in gaming contexts examines the use of cybersecurity methods via the Theory of Planned Behavior framework to combat gaming-related cyberbullying (Che Omar et al., 2024). These findings together underscore that effective cyberbullying prevention via education necessitates holistic strategies that integrate digital literacy, peer support, and pragmatic cybersecurity training. Nevertheless, just a single study concentrates on online gaming (Che Omar et al., 2024), whereas other research pertains to general cyberbullying avoidance.

METHODOLOGY

This study employed a semi-structured interview, and four informants were selected, adhering to the principle that fewer participants often yield more detailed and in-depth information (Sandelowski, 1995; Vasileiou et al., 2018). Furthermore, (Romney et al., 1986), as cited in (Guest et al., 2006), suggest that samples as small as four individuals can provide highly accurate information if participants have high expertise in the studied domain, the cultural context is well-defined, and there is high agreement among participants. Under these conditions, (Romney et al., 1986) calculated that four highly competent participants could yield information with a 0.999 confidence level. Using purposive sampling, informants were selected based on their expertise and potential to contribute insights at the intersection of cybersecurity, online gaming, and behavioral theory. The criteria for selection included academic qualifications, years of experience, role, and expertise in the field (Baker et al., 2006). The characteristics and possible contributions of each informant are summarized in Table 4.1.

Table 4.1: List of Informants

Informant	Academic qualifications	Years of experience	Role
Informant A	PhD Holder	10 years	Game Developer
Informant B	PhD holder	10-15 years	Counsellor
Informant C	Advanced Diploma	30 years	Cybersecurity Expert

Informant D	PhD holder	10-15 years	Academician

Measurement Instrument

The questionnaire consisted of three main sections following the suggestion (Patton, 2015). The researcher began by introducing the study, explaining confidentiality measures, obtaining consent, and asking permission to record. This was followed by opening questions about the participant's professional background and field experience. The core interview questions explored cybersecurity measures for online gaming cyberbullying and their impact on player behavior, using the Theory of Planned Behavior Framework TPB (Ajzen, 1991) and Malaysia Cybersecurity Strategies (MCSS) to examine attitudes, social norms, and behavioral control. In the closing question, the researcher asked if there were any other ideas for improving this study.

Data Collection

The researcher conducted interviews by following systematic procedures, including thorough preparation (Creswell, 2013), obtaining informed consent (Sanjari et al., 2014), managing equipment and schedules, and implementing data verification protocols (Sutton & Austin, 2015). The interview session was conducted between January and April 2023. The discussions take sixty to ninety minutes to complete of the interview session. The interviews were performed in the subjects' preferred language, either English or Bahasa Melayu, given that the informants come from various backgrounds. To ensure accurate transcription and the inclusion of all pertinent material, the researcher will take notes while recording the interviews with the consent of the informants (Creswell, 2013; Sharan B. Merriam, 2014).

Data Analysis

The interview data was processed using NVivo 14 software, following (Braun & Clarke, 2006) six-phase thematic analysis approach: data familiarization, coding, initial theme generation, theme development and review, theme refinement and naming, and final write-up. This approach systematically organizes participants' responses into main themes and sub-themes.

RESULTS

The research revealed multiple preventions that helped reduce the occurrence of online aggression and cyberbullying behaviors in online games. All informants agreed that the four pillars of MCSS are fundamental and can be explored as a foundation for preventing cyberbullying in online games while increasing cybersecurity awareness among teenagers. Informant D addresses his view: ".... these fourth pillars of MCSS are important to reduce bullying in online games. It focuses on making people understand this problem while training people who handle online games...." Followed by informant C stressed, "... these pillars aim to build awareness and skills for players to protect themselves and others online, including in games. However, it is a long-term process. You cannot change people's attitudes overnight." Then, the developer game also agrees and explains, "The elements in the fourth pillar focus on methods to minimize both the impact and occurrence of cyberbullying." Informant B also supports and mentions, "... Yes, these fourth pillars of MCSS are essential. We can see now that many kids play online games, but not many understand the dangers. Like I said before, online gaming is like another world. People can become anyone they want. There are good people, there are bad people. So we must teach these kids how to protect themselves in this gaming world." The examination of data reveals that Informant A acknowledges the fourth pillar of MCSS as essential for preventing cyberbullying in online games.

Cyberbullying and Cyber Security Awareness

All informants identified awareness regarding cyberbullying and cybersecurity as a significant resource to reduce and resolve cyberbullying conflicts between youth. Our participants were most likely to discuss the best method, specifically as a strategy to prevent or intervene in cyberbullying situations. Informants B and C described a typical situation where teenagers must be self-aware online through the campaign.

"Okay, to create this awareness, we need to take several steps. First of all, teenagers need to be self-aware. The government has done all sorts of advertisements and campaigns at universities and schools to raise student awareness. However, we need to make sure this message truly reaches teenagers." (Informant B)

"Government agencies like CyberSecurity Malaysia have conducted many awareness campaigns. The purpose of these campaigns is to make our society 'self-regulate.' This means we want the public to be able to manage their behavior when using the Internet, including when playing online games." (Informant C)

"One concept we use for cyber ethics is 'digital citizenship.' This concept comes from the US, introduced by Mike Ribble. He has approximately nine elements that focus on how to behave in the digital world, especially for students. We take this concept as a starting point for 'self-regulation' in the Malaysian context. However, it is indeed difficult to measure its effectiveness." (Informant C)

Informant D believed that using 'viral' trends in Malaysia increases cyberbullying awareness. The academician explains, "I suggest we use a 'viral' strategy. This means we need to turn the issue of cyberbullying in online games into a topic of conversation on social media. We should make real cases go viral. Let it become like 'agenda setting.' For example, we can make a short video about a teenager bullied in PUBG until they refused to leave their house. Make it viral on TikTok, Instagram, and Twitter. Let everyone discuss it." Then, the academician continued, "We need to find cases that can become a talking point for all of Malaysia. Maybe we can collaborate with popular streamers and ask them to share their experiences of being bullied in games. After that, we need to utilize the strength of our 'netizen army." When asked about the other method that can address the online platform value of teaching youth, the academician also stressed the importance of hashtags and designing posters on social media regarding cyberbullying and cybersecurity awareness.

"We can use this strength to educate people about the dangers of cyberbullying in games. For example, create a hashtag challenge and ask people to share their experiences of being bullied in games. However, we must guide it properly; do not let it become a witch hunt." (Informant D)

"Create an anti-cyberbullying poster design contest, but it must be shared on social media." (Informant D)

"Maybe we can collaborate with gaming influencers or professional e-sports players to deliver messages about the dangers of cyberbullying." (Informant C)

Informant C believes online game firms must address cyberbullying and cybersecurity messages. The expert explains, "We also need to involve game development companies. Maybe we can ask them to include awareness elements in their games." This approach is strongly supported by counselors, given the importance of all parties in reducing bullying problems in online games." The counselor stressed, "We must involve all parties - not just schools and universities, but parents, game developers, and gaming platforms. We can ask game developers to include cybersecurity tips in-game tutorials. Informant A also explained, "Before starting the game, we will have a sort of explanation about cybersecurity. That is one way for developers to provide exposure to their players, so before they begin the game, they are already informed." When asked about the awareness level among teenagers, most informants said it is still moderate and low.

"I have conducted research related to cybersecurity and cybersecurity awareness. It involved zones in the north, south, east, and west, as well as Sabah and Sarawak. We had quite a large number of respondents, around more than 2,000. Our findings showed that cybersecurity awareness among us is still moderate." (Informant D)

"We still do not have sufficient awareness levels regarding privacy issues. However, issues involving passwords and transactions and such can be considered high. Perhaps because these issues have been around for a long time, right? However, issues involving personal data and privacy are shallow." (Informant D)

"I feel there is no awareness level among them regarding cybersecurity; there is not. Looking at this context, whether children, teenagers, or even adults themselves, they will not think about these issues when playing games. However, they will acknowledge these things only after they have become victims. As for preparation beforehand, there is not any." (Informant A)

"If we look at several studies conducted, the results show that teenagers' awareness level regarding cybersecurity is still low. Many students are still unaware of cybersecurity risks such as malware attacks, which we mentioned as viruses earlier." (Informant C)

Cyberbullying and Cyber Security Knowledge Through Education

Most informants described the importance of ongoing awareness of cyberbullying and cybersecurity as an effective means of prevention. The informant D emphasized the importance of ongoing anti-bullying education: "We need to explain what cyberbullying means clearly. For example, criticisms, threats, body shaming—all of these fall under the category of cyberbullying." The academician continued, "We need to teach them what actions they can take if they are bullied, and we need to give real examples, like the case of a student who jumped from a building because they could not handle being bullied." Informant C has a similar sentiment: "We also need to teach them about the effects of cyberbullying, not only on the victims but also on themselves as bullies. As discussed earlier, we can introduce a code of ethics for players. This can guide teenagers in online games." Informant B view "also teaches critical thinking skills. So they can differentiate between normal joking and bullying. Teach them how to respond when bullied and be an 'upstander' when they see others being bullied in games. Then, the counselor continued to explain, "Teach teenagers about laws related to cyberbullying. Let them know that bullying in online games can also face legal consequences. But don't present it in a way that frightens them; focus more on raising awareness." The counselor and academician also suggested classroom activities to enhance cyberbullying and cybersecurity awareness.

"We need to create a platform for teenagers to share their experiences, such as a support group, where they can discuss issues they face in online games. This can serve as peer education, where they can learn from others' experiences." (Informant B).

"We need to give teenagers real experience—not just talk about it but show the real impact of cyberbullying. Maybe we can create simulations in games to show how it feels to be bullied. When they experience it themselves, then they will understand. For example, create a mini-game that simulates the experience of being bullied, then discuss it in class." (Informant D)

Regarding school curriculum, considering the influence of online games on teenagers, Informants B and C suggest incorporating elements of cybersecurity and online gaming ethics into school education. This method will increase awareness about bullying in online games.

"We need to include topics on cybersecurity and ethics in online gaming within the school curriculum. We are not just teaching theory; we must also include practical aspects. For example, we can simulate bullying situations in games and then ask students to think about handling such situations. However, this education cannot be boring. We need to use methods that appeal to teenagers. Like creating viral short videos, using influencers who are popular among teenagers to deliver the message". (Informant B)

"Most crucially, we must integrate this topic into the curriculum or develop specialized school programs. This educational approach is vital as it goes beyond providing information – it can potentially transform teenagers' attitudes and behaviors in the digital realm." (Informant C)

Informant C explained that, with the development of digital technology, "We must educate teenagers about responsible technology and internet use. This is known as digital literacy." Upon examination of the data, it became apparent that experts advocate for a multi-faceted approach to cyberbullying prevention that combines education, technology, practical experience, and curriculum integration to foster responsible online behavior among teenagers in gaming environments.

DISCUSSION

The findings from this comprehensive study reveal critical insights into cyberbullying and cybersecurity awareness among youth in online gaming environments. Our research indicates that despite widespread internet usage among teenagers, cybersecurity and cyberbullying awareness remains low, particularly regarding privacy issues. This observation aligns with (Nurul Ain & Nooraini, 2019) study of the young generation across Malaysia, which found that only a small portion of participants demonstrated an adequate understanding of online privacy risks despite being regular internet users. The strategic approaches proposed by our participants emphasize leveraging social media and viral content as awareness-raising tools, supported by (Ye et al., 2020), a longitudinal study showing that social media-based initiatives achieved significantly higher engagement rates than traditional methods. Additionally, (Kaloeti et al., 2021) research demonstrated that peer-influenced educational content was substantially more effective in modifying teenage online behavior than conventional approaches, supporting our participants' emphasis on utilizing gaming influencers and viral content for awareness campaigns.

The study highlights the importance of multi-stakeholder involvement in cyberbullying prevention, encompassing educational institutions, game developers, parents, gaming platforms, cybersecurity agencies, and social media influencers. (Siddiqui & Schultze-Krumbholz, 2023) conducted a successful narrative review of seventeen interventions applied worldwide, strongly supporting this approach. Their findings demonstrate that integrated multi-stakeholder programs achieved markedly higher success rates in reducing cyberbullying incidents than single-stakeholder initiatives. Furthermore, incorporating digital citizenship frameworks, particularly Mike Ribble's model, presents opportunities and challenges in developing cyber ethics awareness. (Manzuoli et al., 2019) reviewed the implementation of digital citizenship in research conducted over the last ten years. Their findings revealed that while such frameworks provide valuable guidelines, their effectiveness varies significantly based on cultural context and implementation strategies, supporting our participants' emphasis on adapting international frameworks to local Malaysian contexts.

Our analysis emphasizes the significance of experiential learning and curriculum integration in cyberbullying prevention. (Torgal et al., 2021) meta-analysis revealed that interventions combining theoretical and practical components showed substantially higher effectiveness rates than purely theoretical approaches. This finding is further reinforced by (Suzuki et al., 2012) research, which found that students participating in simulated cyberbullying scenarios demonstrated marked improvements in empathy and understanding compared to those receiving traditional lecture-based education. The counselor's recommendation for peer support groups is supported by (Topping, 2023) study showing that peer-led groups achieved notably higher engagement rates in prevention programs than teacher-led interventions.

Integrating cybersecurity and online gaming ethics into school curricula became fundamental to effective prevention strategies. A comprehensive study of digital literacy integration in K-12 education found that schools with integrated digital citizenship curricula reported significantly fewer cyberbullying incidents than schools with standalone programs (Stange, 2019). Our research points out that an anti-cyberbullying poster design contest also emerged as an essential component, supported by (Syed Hussein & Mohd Shuib, 2018) research on adolescents, which showed that students involved in the social media campaign poster were considerably more likely to intervene positively in cyberbullying situations. The digital literacy education and cyberbullying study (Thompson et al., 2023) further supports this integrated approach, identifying comprehensive digital literacy education as crucial in reducing online harassment and promoting responsible online behavior.

Our research indicates that collaboration with gaming influencers should be integrated into broader cyberbullying prevention strategies rather than functioning as standalone initiatives. This finding is supported by (Timotheou et al., 2023), a comprehensive review of digital safety programs that found that multi-channel approaches incorporating traditional educational methods and influencer-led content achieved better outcomes in promoting positive online behavior. (Cui et al., 2022) analysis of digital prevention campaigns showed that when gaming influencers shared personal experiences with cyberbullying, young audiences demonstrated increased playbors' game loyalty and understanding of the issue's significance. This integrated approach allows for reinforcing anti-bullying messages across different platforms and contexts, reaching young gamers most receptive to these messages.

Based on these findings and supporting literature, we recommend several practical strategies for cyberbullying awareness and educational institutions regarding cyberbullying in online games among adolescents. First, schools should develop comprehensive curricula integrating cyberbullying prevention, digital literacy, and online gaming ethics. Second, educational programs should incorporate simulation-based learning experiences and peer support groups to reflect the demonstrated effectiveness of experiential learning approaches. Third, institutions should utilize diverse delivery methods, including anti-cyberbullying posters, digital content, and interactive simulations. Fourth, The programs should establish collaborations with gaming influencers and professional esports players to enhance message delivery and student engagement. Fifth, regular evaluation of program effectiveness should be implemented through quantitative and qualitative measures. Finally, special attention should be paid to the cultural adaptation of international frameworks, particularly in the Malaysian context, where social media penetration rates are exceptionally high. These recommendations aim to address the current reactive nature of cybersecurity awareness and establish more proactive, preventive measures for combating cyberbullying in online gaming environments.

CONCLUSION

This study has provided valuable insights into cyberbullying prevention strategies in online gaming environments, mainly focusing on awareness and education approaches within the MCSS framework. The findings reveal that effective prevention requires a multi-faceted approach combining digital literacy, peer support, and practical cybersecurity training. The research emphasizes the crucial role of awareness campaigns, educational programs, and stakeholder collaboration in creating safer online gaming spaces. The study's participants consistently highlighted the importance of leveraging social media, viral content, and gaming influencers to reach young audiences effectively. Integrating cybersecurity and online gaming ethics into school curricula and simulation-based learning experiences and peer support groups emerged as fundamental components for preventing cyberbullying. Furthermore, the findings underscore the necessity of adapting international frameworks to local Malaysian contexts while maintaining a proactive rather than reactive approach to cyberbullying prevention.

Several significant limitations emerged in this study's exploration of cyberbullying in online games. First, the small sample size of four experts, while providing in-depth insights, may not represent all perspectives on cyberbullying prevention strategies. Second, the rapidly evolving nature of online gaming platforms and communication methods creates challenges in developing long-term prevention strategies as new forms of cyberbullying continuously emerge. Third, the study's focus on the Malaysian context may limit the generalizability of findings to other cultural settings. Fourth, the effectiveness of proposed prevention strategies, particularly those involving gaming influencers and viral content, lacks long-term evaluation data. Finally, the research predominantly relied on expert opinions rather than direct input from young gamers themselves, potentially missing crucial perspectives from the primary stakeholders affected by cyberbullying in online gaming environments.

ACKNOWLEDGMENT

This research was supported by the Ministry of Higher Education (MoHE), the Fundamental Research Grant Scheme (FRGS) FRGS/1/2021/SS0/UUM/02/20, and Universiti Utara Malaysia (UUM).

REFERENCES

[1] Ahmad Razali, N., Nawang, N. I., & Syed Nong Mohamad, S. N. A. (2022). Cyberbullying In Malaysia: An Analysis Of The Existing Laws. International Journal of Law, Government, and Communication, 7(30). https://doi.org/10.35631/ijlgc.730011

[2] Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, Academic Press, Inc., pp. 50, 179–211.

[3] Anderson, M., & Jiang, J. (2018). Teens, Social Media & Technology 2018 | Pew Research Center. In Pew Research Centre.

[4] Ariffin, A., Mohd, N., Rokanatnam, T., Malaysia, C., My, A., & My, N. (2021). Cyberbullying via Social Media: Case Studies in Malaysia. Journal of Cyber Security, 3(1), 21–30.

[5] Ballard, M. E., & Welch, K. M. (2017). Virtual Warfare: Cyberbullying and Cyber-Victimization in MMOG Play. Games and Culture, 12(5), 466–491. https://doi.org/10.1177/1555412015592473

[6] Barlett, C. P., & Kowalewski, D. A. (2018). Learning to Cyberbully: An Extension of the Barlett Gentile Cyberbullying Model. Psychology of Popular Media Culture, 8(4), 437–443. https://doi.org/10.1037/ppm0000183

[7] Barlinska, J., Szuster, A., & Winiewski, M. (2018). Cyberbullying among adolescent bystanders: Role of affective versus cognitive empathy in increasing prosocial cyber bystander behavior. Frontiers in Psychology, 9(MAY), 1–13. https://doi.org/10.3389/fpsyg.2018.00799

[8] Bernama. (2020, August). MCMC addresses over 11,000 complaints within the first six months of this year. BERNAMA. https://themalaysianreserve.com/2020/08/12/mcmc-addresses-over-11000-complaints-within-first-six-months-this-year/

[9] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. January. https://doi.org/10.1191/1478088706qp063oa

[10] Calvo-Morata, A., Alonso-Fernández, C., Freire, M., Martínez-Ortiz, I., & Fernández-Manjón, B. (2020). Serious games to prevent and detect bullying and cyberbullying: A systematic serious games and literature review. Computers and Education, 157, 103958. https://doi.org/10.1016/j.compedu.2020.103958

[11] Che Omar, M. F. R., Abdullah, N. A., & Saad, M. N. (2024). Prevention of Cyberbullying in Online Games: Intervention of Cybersecurity Strategies. Pakistan Journal of Life and Social Sciences (PJLSS), 22(1), 5450–5464. https://doi.org/10.57239/pjlss-2024-22.1.00402

[12] Creswell, J. W. (2013). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). Sage Publication. https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=1485543

[13] Cui, Y., Li, J., & Zhang, Y. (2022). The impacts of game experience and fanwork creation on game loyalty: Mediation effect of perceived value. Technological Forecasting and Social Change, 176. https://doi.org/10.1016/j.techfore.2022.121495

[14] Ekiciler, A., Ahioğlu, İ., Yıldırım, N., Ajas, İ. İ., & Kaya, T. (2022). The Bullying Game: Sexism Based Toxic Language Analysis on Online Games Chat Logs by Text Mining. Journal of International Women's Studies, 24(3).

[15] Ezedy, K., Rahman, A., Abdullah, Y., Dzulkifly, S., & Lakulu, M. M. (2024). Inculcating Cybersecurity Awareness Among School Students through the Application of Courseware. Journal of Advanced Research in Applied Sciences and Engineering Technology, 1(1), 175–189.

[16] Fryling, S. (2018). Gender, Over Sharing, and Cyberbullying in Online Multi-Player Gaming (Mmog) Environments. Issues In Information Systems, 19(2), 140–148. https://doi.org/10.48009/2_iis_2018_140-148

[17] Galinec, D., Moznik, D., & Guberina, B. (2017). Cybersecurity and cyber defense: a national level strategic approach. Automatika, 58(3). https://doi.org/10.1080/00051144.2017.1407022

[18] Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. Field Methods, 18(1). https://doi.org/10.1177/1525822X05279903

[19] Hayashi, Y., & Tahmasbi, N. (2022). Psychological Predictors of Bystanders' Intention to Help Cyberbullying Victims Among College Students: An Application of Theory of Planned Behavior. Journal of Interpersonal Violence, 37(13–14), NP11333–NP11357. https://doi.org/10.1177/0886260521992158

[20] Hellfeldt, K., López-Romero, L., & Andershed, H. (2020). Cyberbullying and psychological well-being in young adolescence: the potential protective mediation effects of social support from family, friends, and teachers. International Journal of Environmental Research and Public Health, 17(1). https://doi.org/10.3390/ijerph17010045

[21] Hidayat, Z., Permatasari, C. B., & Mani, L. (2022). Cyber Violence and Bullying in Online Game Addiction: a Phenomenological Study. Journal of Theoretical and Applied Information Technology, 100(5), 1428–1440.

[22] Huang, J., Zhong, Z., Zhang, H., & Li, L. (2021). Cyberbullying in social media and online games among Chinese college students and its associated factors. International Journal of Environmental Research and Public Health, 18(9). https://doi.org/10.3390/ijerph18094819

[23] Ijachi, O. O. (2019). Social Media Access and Cyberbullying- A Nigerian Perspective. International Journal of Innovative Studies in Medical Sciences, 3(3), 5–9. http://ijisms.com/wp-content/uploads/2019/05/IJISMS-030113.pdf

[24] Kaloeti, D. V. S., Manalu, R., Kristiana, I. F., & Bidzan, M. (2021). The Role of Social Media Use in Peer Bullying Victimization and Onset of Anxiety Among Indonesian Elementary School Children. Frontiers in Psychology, 12. https://doi.org/10.3389/fpsyg.2021.635725

[25] Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: State of the art and future directions. Journal of Cybersecurity, 7(1), 1–13. https://doi.org/10.1093/cybsec/tyab005

[26] Kordyaka, B., Krath, J., Park, S., Wesseloh, H., & Laato, S. (2022). Understanding toxicity in multiplayer online games: The roles of national culture and demographic variables. Proceedings of the 55th Hawaii International Conference on System Sciences. https://doi.org/10.24251/hicss.2022.359

[27] Kou, Y. (2020). Toxic Behaviors in Team-Based Competitive Gaming. Chi Play '20, 81–92. https://ukie.org.uk/sites/default/files/eSports whitepaper.pdf

[28] Kurt, W. (2020). Cyberbullying in online gaming. https://www.ghostgb.co.uk/cyber-bullying-in-online-gaming/

[29] Lukács J, Á., Takács, J., Soósné Kiss, Z., Kapitány-Fövény, M., Falus, A., & Feith, H. J. (2023). The Effects of a Cyberbullying Intervention Programme Among Primary School Students. Child and Youth Care Forum, 52(4). https://doi.org/10.1007/s10566-022-09714-9

[30] Majlis Keselamatan Negara. (2020). Malaysia Cyber Security Strategy 2020-2024. https://asset.mkn.gov.my

[31] Manzuoli, C. H., Vargas, M. A., Erika, S. M., & Bedoya, D. (2019). Digital Citizenship: A Theoretical Review of the Concept and Trends. Turkish Online Journal of Educational Technology - TOJET, 18(2).

[32] McInroy, L. B., & Mishna, F. (2017). Cyberbullying on Online Gaming Platforms for Children and Youth. Child and Adolescent Social Work Journal, 34(6), 597–607. https://doi.org/10.1007/s10560-017-0498-0

[33] McLean, L., & Griffiths, M. D. (2019). Female Gamers' Experience of Online Harassment and Social Support in Online Gaming: A Qualitative Study. International Journal of Mental Health and Addiction, 17(4), 970–994. https://doi.org/10.1007/s11469-018-9962-0

[34] MCSS. (2020). Malaysia Cyber Security Strategy 2020-2024. Malaysia Cyber Security, 53(9).

[35] Mishna, F., Birze, A., & Greenblatt, A. (2022). Understanding Bullying and Cyberbullying Through an Ecological Systems Framework : The Value of Qualitative Interviewing in a Mixed Methods Approach. International Journal of Bullying Prevention, 4(3), 220–229. https://doi.org/10.1007/s42380-022-00126-w

[36] Noridayu, S., Fakulti, A. N., Moden, B., Komunikasi, D., Abdul, H., & Fakulti, H. (2022). Pengaruh Positif Dan Negatif Dalam Permainan Games Di Internet Kepada Psikologi Kanak-Kanak. Jurnal Ilmi Ilmi Journal, 12(2022), 68–83.

[37] Nurul Ain, A., & Nooraini, O. (2019). Information Privacy Awareness Among Young Generation in Malaysia. Information Privacy Awareness among Young Generation in Malaysia, 5(2), 1–10. https://jostip.org/index.php/jostip/article/download/84/50

[38] Ortega-Barón, J., González-Cabrera, J., Machimbarrena, J. M., & Montiel, I. (2021). Safety.Net: A pilot study on a multi-risk internet prevention program. International Journal of Environmental Research and Public Health, 18(8). https://doi.org/10.3390/ijerph18084249

[39] Panosso, M. G., Kienen, N., & de Faria Brino, R. (2023). Teacher Training for Prevention and Management of School Bullying Situations: A Systematic Literature Review. Psicologia: Teoria e Pesquisa, 39. https://doi.org/10.1590/0102.3772E39310.PT

[40] Patton, M. Q. (2015). Qualitative Evaluation and Research Methods (T. Oaks (ed.)). Sage. https://www.scirp.org/(S(351jmbntvnsjt1aadkozje))/reference/references papers. asp?referenceid=1838631

[41] Przybylski, A. K. (2019). Exploring Adolescent Cyber Victimization in Mobile Games: Preliminary Evidence from a British Cohort. Cyberpsychology, Behavior, and Social Networking, 22(3). https://doi.org/10.1089/cyber.2018.0318

[42] Romney, A. K., Weller, S. C., & Batchelder, W. H. (1986). Culture as Consensus: A Theory of Culture and Informant Accuracy. American Anthropologist, 88(2). https://doi.org/10.1525/aa.1986.88.2.02a00020

[43] Saharrudin, N. F., Ghazali, A. H. A., Samah, A. A., Ahmad, A., & Abdullah, H. (2019). Cyberbullying among Malaysian Youth: The Case of Selangor. International Journal of Academic Research in Business and Social Sciences, 9(3). https://doi.org/10.6007/ijarbss/v9-i3/5761

[44] Sanjari, M., Bahramnezhad, F., Fomani, F. K., Shoghi, M., & Ali Cheraghi, M. (2014). Ethical challenges of researchers in qualitative studies: The necessity to develop a specific guideline. In Journal of Medical Ethics and History of Medicine (Vol. 7).

[45] Sharan B. Merriam, E. J. T. (2014). Qualitative Research: A Guide to Design and Implementation, 4th Edition (4th ed.). Jossey-Bass. https://www.wiley.com/en-us/Qualitative+Research%3A+A+Guide+to+Design+and+Implementation%2C+4th+Edition-p-9781119003618

[46] Siddiqui, S., & Schultze-Krumbholz, A. (2023). Successful and Emerging Cyberbullying Prevention Programs: A Narrative Review of Seventeen Interventions Applied Worldwide. In Societies (Vol. 13, Issue 9). https://doi.org/10.3390/soc13090212

[47] Sivabalan, T. V., Ahmad Zaki, R., & Choo, W. Y. (2020). The prevalence of cyberbullying and its associated factors among young adolescents in Penang, Malaysia. Journal of Health and Translational Medicine, 23.

[48] Stange, R. (2019). Increase K-12 Cyber Competency to Prevent Cyberbullying. https://doi.org/10.1145/3287324.3293770

[49] Sutton, J., & Austin, Z. (2015). Qualitative research: data collection, analysis, and management. The Canadian Journal of Hospital Pharmacy, 68(3), 226–231.
[50] Suzuki, K., Kashibuchi, M., Kumazaki, A., & Horiuchi, Y. (2012). Use of Gaming Simulation for Cyberbullying Prevention. Refereed Paper, 22, 39.
[51] Syed Hussein, S. N. A. S., & Mohd Shuib, A. S. (2018). The Effectiveness of Social Media Campaign Poster to Prevent Cyberbullying Among Teenagers in Malaysia Through Illustration. Ideology Journal, 3(2), 157–162. https://doi.org/10.24191/idealogy.v3i2.75
[52] Tanrikulu, I. (2018). Cyberbullying prevention and intervention programs in schools: A systematic review. School Psychology International, 39(1). https://doi.org/10.1177/0143034317745721
[53] Timotheou, S., Miliou, O., Dimitriadis, Y., Sobrino, S. V., Giannoutsou, N., Cachia, R., Monés, A. M., & Ioannou, A. (2023). Impacts of digital technologies on education and factors influencing schools' digital capacity and transformation: A literature review. Education and Information Technologies, 28(6). https://doi.org/10.1007/s10639-022-11431-8
[54] Topping, K. J. (2023). Advantages and Disadvantages of Online and Face-to-Face Peer Learning in Higher Education: A Review. Education Sciences, 13(4). https://doi.org/10.3390/educsci13040326
[55] Torgal, C., Espelage, D. L., Polanin, J. R., Ingram, K. M., Robinson, L. E., El Sheikh, A. J., & Valido, A. (2021). A Meta-Analysis of School-Based Cyberbullying Prevention Programs' Impact on Cyber-Bystander Behavior. School Psychology Review. https://doi.org/10.1080/2372966X.2021.1913037
[56] Verschueren, S., Buffel, C., & Stichele, G. Vander. (2019). Developing theory-driven, evidence-based serious games for health: Framework based on research community insights. JMIR Serious Games, 7(2). https://doi.org/10.2196/11565
[57] Wan Ahmad, W. M. I. F., Mohd, S. M., Abdul Wahab, A. N., Mohamad Jan, N., Kamarudin, S., & Kaco, H. (2022). Online Game: Current Trend Among Malaysian Secondary School's Students. International Journal of Education, Psychology and Counseling, 7(45), 492–500. https://doi.org/10.35631/ijepc.745037
[58] Wang, L., & Ngai, S. S. Y. (2021). Cyberbullying Perpetration Among Chinese Adolescents: The Role of Power Imbalance, Fun-seeking Tendency, and Attitude Toward Cyberbullying. Journal of Interpersonal Violence, 37(23–24). https://doi.org/https://doi.org/10.1177/08862605211062988
[59] Ye, X., Zhao, B., Nguyen, T. H., & Wang, S. (2020). Social Media and Social Awareness. In Manual of Digital Earth. https://doi.org/10.1007/978-981-32-9915-3_12
[60] Zhao, Y., Chu, X., & Rong, K. (2023). Cyberbullying experience and bystander behavior in cyberbullying incidents: The serial mediating roles of perceived incident severity and empathy. Computers in Human Behavior, 138. https://doi.org/10.1016/j.chb.2022.107484

AUTHOR BIOGRAPHIES

Muhammad Fakhru Rizuan Che Omar is a Ph.D. student at Universiti Utara Malaysia, specializing in Media Management. As a Graduate Research Assistant, he investigates new media, communication, online games, cyberbullying behavior, and cybersecurity.

Noor Aziah Abdullah is a Senior Lecturer at UUM's School of Multimedia Technology and Communication, with a Ph.D. in Communication from UKM (2017). With 18 years of experience as a Ministry of Home Affairs Enforcement Officer, her research centers on Media Law and Public Policy.

Mohd Nizam Saad is a Senior Lecturer at UUM's School of Multimedia Technology and Communication. He holds Bachelor's and Master's degrees in IT from UUM and a Ph.D. in medical image processing from UKM. He developed a new model for medical image annotation and has extensive experience in human-computer interaction, focusing on usability enhancement through expert reviews using cognitive walk-through techniques.

Nurulhuda Ibrahim a Senior Lecturer at UUM's School of Multimedia Technology and Communication. She is an Information System professional with over ten years of experience, holding a B.Sc. in Computer Science from Universiti Teknologi Malaysia and a Master of Computing from Monash University. She led an FRGS grant on electronic reading functionalities and now researches the impact of online visuals on user behavior.