December 2024

TEENS, TECH, AND TRUST:
NAVIGATING SOCIAL MEDIA IN MALAYSIA

SERI SOCIAL & ECONOMIC RESEARCH INITIATIVE

About Social & Economic Research Initiative (SERI) Malaysia:

We live in an unprecedented time of exacerbating economic and social inequality. Increasing disruption to basic needs – from basic incomes, healthcare, women and children, and improving digital literacy – are some of our biggest challenges today.

We are a nonpartisan think-tank driving evidence-based data and research in Malaysia and across the Global South, seeking to directly and positively catalyze ambitious social and economic research initiatives and policies.

Our targeted and deep research seeks to inform policies and programs effectively. We leverage empirical proof to strengthen social investments in rapidly developing economies where resources can be limited, and entrenched social issues pose risks to progressive development.

Attribution:

Please cite the work as follows: Arulthevan, Yohendran Nadar (2024) “Teens, Tech, and Trust: Navigating Social Media in Malaysia”, Kuala Lumpur: Social and Economic Research Initiative (SERI)

Acknowledgements

We wish to extend our sincere gratitude to all individuals and organisations who contributed to the successful design and execution of this exploratory study. We would like to first acknowledge Yohendran Nadar Arulthevan, the project lead for the study and the author of this white paper.

We would also like to highlight the specific contributions of the research team at SERI: Nur Sakinah Alzian for organising and moderating the focus group discussion; Violet Lee Zi Yi for coordinating survey dissemination activities and in-depth interviews;Aliya Waheedah Ahmad Lutfi for data cleaning and data visualisation and Vyshnavi Charrlotte and Claudia Ng for conducting desk research to inform the case studies. Our appreciation extends to the wider team at SERI: Syafiqa Zakaria for leading the design of the white paper and Nur Farthinie for managing the communications campaigns; and Rashaad Ali for his constructive inputs throughout the study.

Furthermore, we are grateful for the support of TikTok Malaysia for their generous support which played an instrumental role in the development and launch of this report. Furthermore, we express our sincere thanks to the Ministry of Education, along with the State Education Departments of Perlis, Perak, Selangor, Melaka, the Federal Territory of Kuala Lumpur, and the Federal Territory of Putrajaya. Their collaboration, together with the various secondary schools under their purview, was vital in facilitating the dissemination of our survey to Malaysian teenagers.

Additionally, we are thankful to the participants of our focus group discussions, including parents, teachers, and representatives from NGOs and social media platforms, whose insights were invaluable. We also acknowledge the Malaysian teenagers who took part in our survey and in-depth interviews, as their perspectives are crucial to our findings as the primary stakeholders and beneficiaries of this study.

The white paper is based on information current as of 10 December 2024.

Please contact Yohendran Nadar Arulthevan (Research Consultant, SERI) at yohendran@seri.my or Rashaad Ali (Managing Director, SERI) at rashaad@seri.my for questions, comments, or suggestions regarding the report.

Table of Contents

Executive Summary

This white paper examines the online safety concerns faced by Malaysian teenagers aged 13 to 17, who are deeply engaged with social media platforms. The study employs a mixed-methods approach, gathering both quantitative data through a survey and qualitative insights from interviews, focus group discussions, and case studies. The key findings of the study are as follows:

1. **Significance of Social Media in Teenagers' Lives:** Social media has become a central aspect of Malaysian teenagers' daily activities, offering opportunities for connection, self-expression, and access to information.
2. **Vulnerability to Online Dangers:** Despite the benefits of social media, teenagers are exposed to a range of online risks, including cyberbullying, online fraud, and harassment, leading to feelings of insecurity, anxiety and envy.
3. **Insufficient Digital Safety Knowledge:** While there is some understanding of basic digital safety practices such as managing privacy settings, teenagers often lack deeper knowledge about more complex online risks and how to protect themselves effectively.
4. **Struggles of Parents and Teachers:** Parents and teachers find it increasingly difficult to keep up with the rapid pace of change in digital platforms and emerging online threats, which limits their ability to offer comprehensive guidance on online safety.
5. **Efforts by Platforms and Government:** Social media platforms have taken steps to enhance safety features, and the Malaysian government has made strides in regulating online spaces,but awareness and trust in these efforts are still lacking.

The findings underscore the need for a comprehensive, coordinated response to safeguard teenagers in the digital environment. To address these issues, the study outlines three crucial policy recommendations, framed within the **"3Rs"**:

1. **Redesigning Reporting and Support Mechanisms**
2. **Reimagining Digital Literacy Education**
3. **Reapproaching Multi-Stakeholder Partnerships**

Adopting these strategies will contribute to the creation of a secure and supportive online environment in Malaysia, providing teenagers with the knowledge and tools needed to engage with digital spaces safely, while safeguarding their long-term well-being.

Introduction

Social media has become an integral part of daily life for Malaysian teenagers, providing spaces for social interaction, creativity, and learning. However, digital immersion brings its own range of risks, exposing young users to online harms such as cyberbullying, harassment, and exploitation. Recent high-profile incidents, such as the tragic death of a young influencer linked to cyberbullying and the widely publicised "Abang Bas" case involving nonconsensual filming of underage schoolgirls, underscores the urgent need for effective measures to protect young users and promote responsible digital citizenship.[1] [2]

To address these challenges, this study examines the online safety of Malaysian teenagers aged 13 to 17 who actively engage with social media and messaging platforms. The platforms covered include WhatsApp, Telegram, Instagram, Facebook, TikTok, X (formerly Twitter), and Discord. Specifically, the research focuses on three main types of online threats[3] faced by teenagers: (1) aggressive threats such as cyberbullying and harassment, (2) sexual threats including sextortion and grooming,[4] and (3) commercial threats like scams and fraudulent activities.

The study also assesses the roles of parents and teachers, as well as the institutional, legal, and regulatory frameworks, in protecting young users on these platforms.

To address these challenges, a mixed-methods approach was employed, combining quantitative and qualitative methods. Primary data was collected through a survey, four semi-structured interviews, a focus group discussion (FGD), and two case studies that highlight international best practices. This multidimensional approach provides a comprehensive view of the issues and challenges involved (see Appendix A for detailed information on the Research Methodology). The findings offer evidence-based recommendations aimed at enhancing digital safety and supporting the well-being of teenagers.

This white paper seeks to inform policymakers, industry stakeholders, parents, and teachers insights into online safety, offering actionable recommendations for creating stronger protections and fostering a safer online environment. By prioritising these safeguards, young Malaysians will be better equipped to navigate social media responsibly and thrive in a digital world.

1. See New Rules Mulled After Activist's Death, Charles Ramendran and Geraldine Tong, The Star, July 7, 2024
2. See TikToker 'Abang Bas' arrested for filming schoolgirls, even calling some of them his 'crush', Ben Tan, Malay Mail, September 6, 2024
3. See Child Safety Online: Global Strategies and Challenges, MCMC Webinar Slides, UNICEF Malaysia
4. Due to the sensitive nature of sexual threats, including sextortion and grooming, these issues were addressed indirectly in the study by referring to them as unwanted advances and blackmail. This approach was adopted in consideration of the age group involved (13-17years) and the need to protect participants from exposure to explicit content or distressing topics.

Social Media Experiences

Teenagers' interactions with social media are influenced by a range of behaviours, challenges, and risks. This section will examine how young people engage with social media, highlighting both the positive and negative aspects of their online activities. It will address the various threats they face, including cyberbullying, harassment, unwanted advances, blackmail, doxxing, and scams. The section will also explore how these experiences shape teenagers' awareness of online safety and the strategies they use to protect themselves, emphasising the need for effective multi-stakeholder interventions to safeguard their well-being.

Online Presence

Figure 01:
More than three in four teens use the internet frequently for social media.

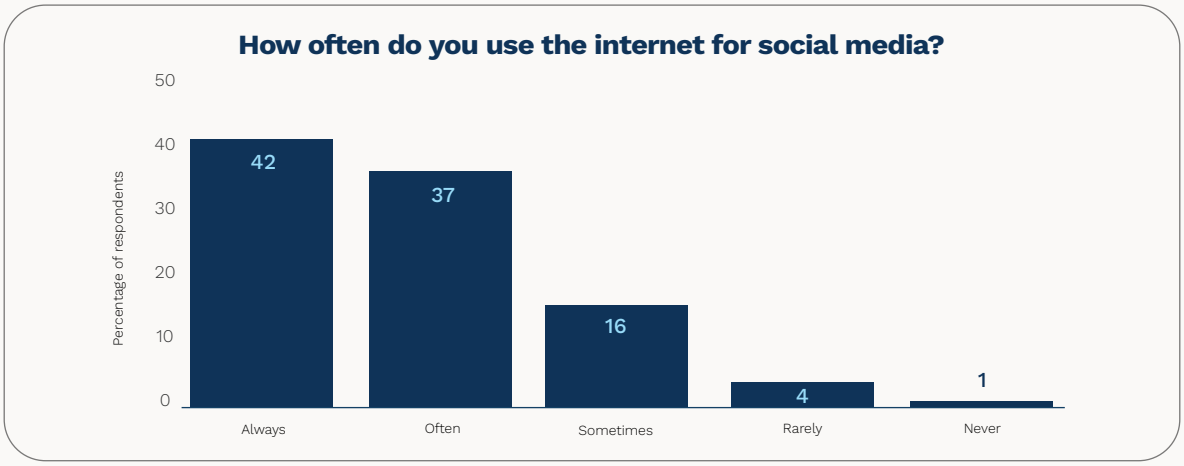


Figure 02:
Nearly three in four teens use the Internet frequently for watching or streaming videos.

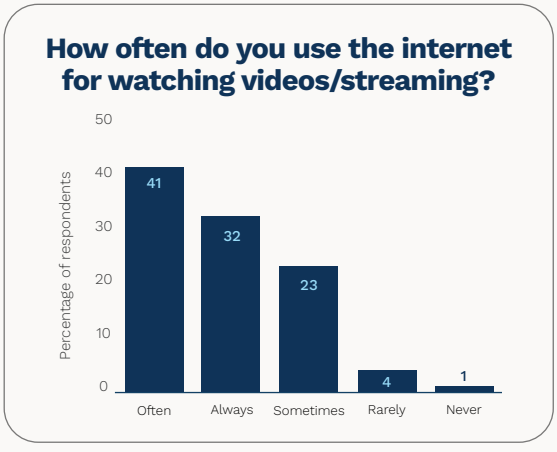


Figure 03:
More than three in five teens use the Internet frequently for schoolwork/ homework.

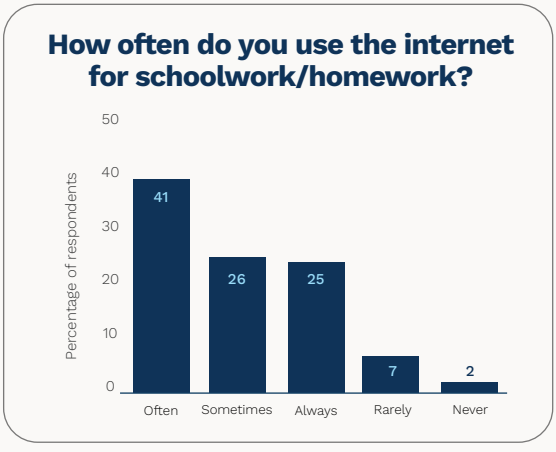


Figure 04:
Less than two in five teens use the Internet frequently for gaming.

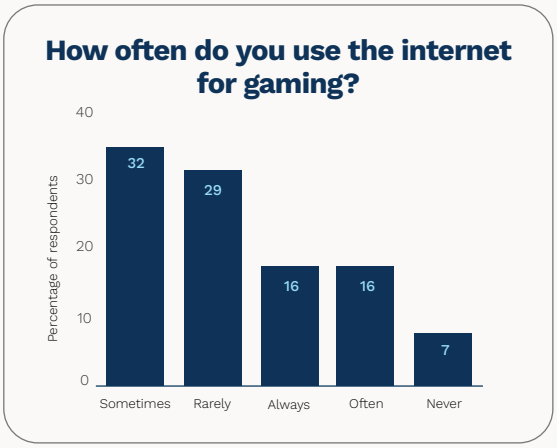
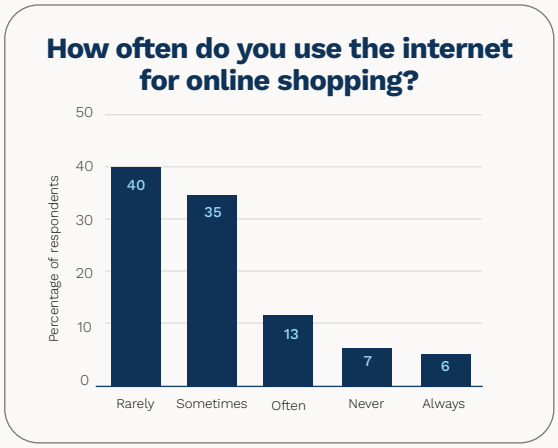


Figure 05:
Less than one in five teens use the Internet frequently for online shopping.



Source: SERI Malaysia (Author's Findings from Survey, 2024)

Our survey findings indicate that the internet is primarily used by teens for social and entertainment purposes, with the majority engaging frequently in social media (Figure 1), watching or streaming videos (Figure 2), and schoolwork or homework (Figure 3). While gaming (Figure 4) and gaming (Figure 5) are slightly less common, the differences in frequency across these activities are minimal, suggesting that all of them are integral parts of teens' online routines. This highlights the dominant role of the internet in daily life, particularly for entertainment, social interaction, and leisure.

These trends also align with another survey, late teenagers have the highest rate of handphone usage, and that smartphone ownership is notably high among young Malaysians.[5][6] This widespread smartphone ownership likely facilitates the frequent engagement of young people with mobile-first activities such as social media, video streaming, and gaming—activities that are confirmed by our survey findings.

5. See Hand Phone Users Survey 2021, MCMC, 2021
6. See Figures A7 and A8 in Appendix B for further details.

Online Behaviours and Habits

Figure 06:
Among teenagers, the most popular social media platform is Instagram, while the most popular messaging platform is WhatsApp.*

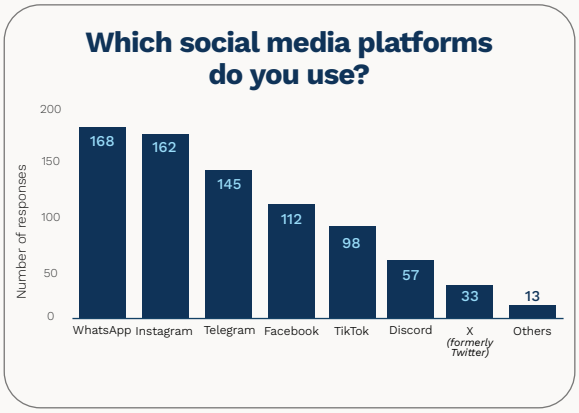


Figure 07:
Teenagers also spend the majority of their time on Instagram, far outpacing other platforms.

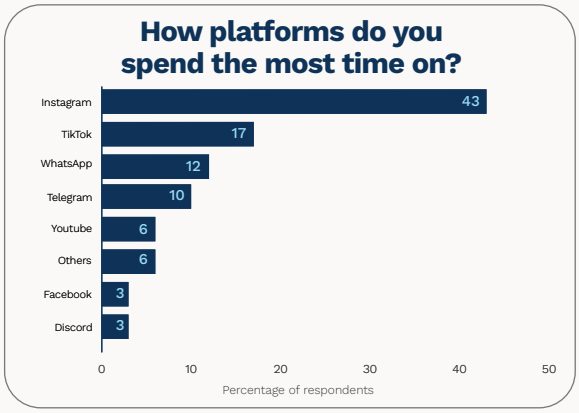


Figure 08:
Almost half of the teens spend at least 3 hours or more daily on social media.

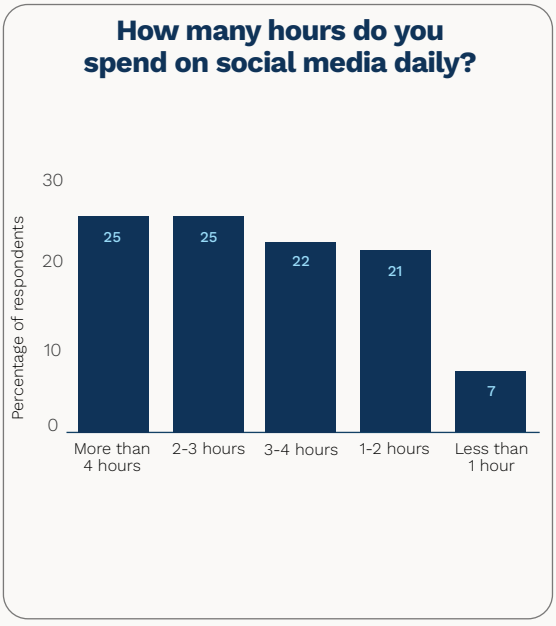
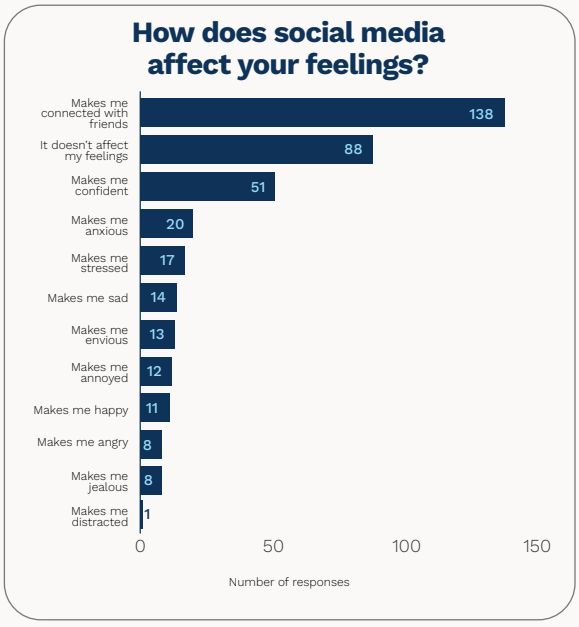


Figure 09:
Most teens feel more connected to their friends through social media, while a significant proportion feel it has no impact on their emotions.*



Source: SERI Malaysia (Author's Findings from Survey, 2024)
Note: * Indicates survey questions where respondents are permitted to provide multiple responses.

Based on our survey, social media platforms, particularly Instagram, dominate the digital landscape among teenagers (Figure 6). Instagram is not only the most popular social media platform but also far outpaces others like TikTok and WhatsApp in terms of time spent by teens (Figure 7). However, through our interviews and focus group discussion, we also learned that each platform is used for different purposes. For example, while teens mostly browse Instagram, TikTok, and Facebook for online content and social messaging, Telegram and WhatsApp are primarily used for learning activities, as their teachers and schools have created groups to share class-related announcements and information on homework. Meanwhile, Discord is used for gaming, providing a platform for gamers to communicate and strategise during gameplay, particularly in multiplayer global games. The various purposes for which teens use social media underscore its central role in their everyday lives, as confirmed by our survey, with nearly half of teenagers reporting spending at least three hours or more daily on social media (Figure 8).

Xiaohongshu's Growing Influence among Malaysian Teenagers

Interviews with teenagers revealed that Xiaohongshu (Little Red Book), a Chinese social media and e-commerce platform often compared to Instagram, is rapidly gaining traction among Malaysian teens. As of February 2023, the platform has over 2.5 million users in Malaysia, predominantly within the Chinese Malaysian community, which constitutes around 36.7% of the country's ethnic Chinese population[7]. This platform is especially popular among Chinese-speaking teenagers attending schools where Chinese is the primary medium of instruction. Despite its rising popularity, Xiaohongshu's current user base falls below the 8 million-user threshold required for regulatory oversight under MCMC's new framework for social media platforms. As its user base continues to grow, regulators should consider the unique experiences of teenagers on Xiaohongshu and other rapidly expanding platforms and ensure appropriate safeguards are put in place.

7. See A look at Xiaohongshu, China's answer to Instagram that has Chinese Malaysians glued to their phones (VIDEO)Kenneth Tee, Malay Mail, September 24, 2024
8. Ibid.

Considering the substantial time teenagers spend on social media, it is understandable that these platforms influence both their social interactions and their emotional experiences. While the majority of teens in our survey feel more connected to their friends through social media, a notable proportion report that it has little to no impact on their emotional state (Figure 9). This finding could be due to some teens using social media in a more neutral, desensitised way, exercising positive self-regulation, or simply finding that social media is less emotionally charged or personal for them.

On the other hand, some respondents also expressed feeling anxious, the most negative emotional response associated with social media use. This suggests a complex relationship between social media and emotional well-being, where it serves as a tool for connection for many, but for others, it can trigger negative emotions such as anxiety, stress, and envy. The data highlights the varied emotional effects—whether positive, neutral or negative—that social media can have on teenagers.

Online Threats

Figure 10:
Less than half of teens feel safe online, with a similar proportion feeling unsafe or unsure.

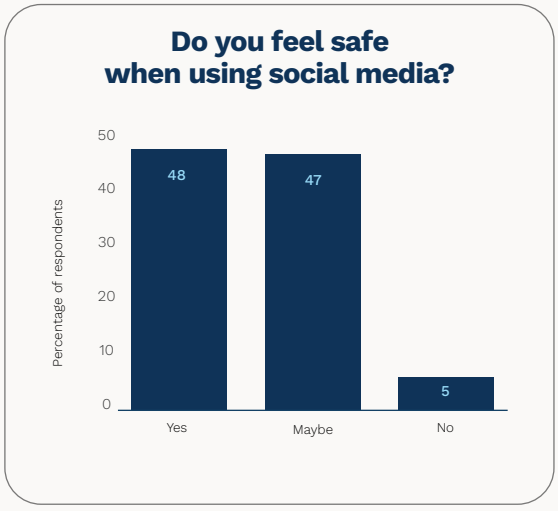
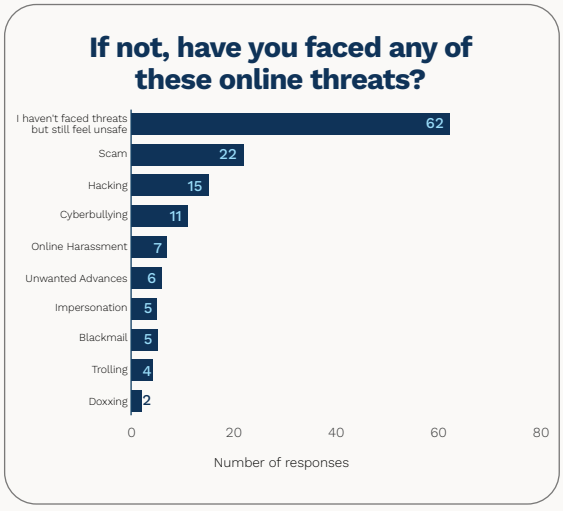


Figure 11:
Teens who feel unsafe or unsure of their online safety often do so without facing specific threats. The most common threats reported include scams, hacking, and cyberbullying.*



Source: SERI Malaysia (Author's Findings from Survey, 2024)
Note: * Indicates survey questions where respondents are permitted to provide multiple responses.

Less than half of teens report feeling safe online, with a similar proportion either unsure or feeling unsafe (Figure 10). Interestingly, many teens who feel unsafe or unsure of their online safety report these feelings despite not having encountered any specific threats (Figure 11). This trend was confirmed in our interviews, where almost all participants had not personally experienced negative online incidents but were aware of at least one friend who had.

This second-hand knowledge of cyberbullying[9] and scams[10] contribute to a general sense of unease and insecurity. Even though they have not faced these issues themselves, the awareness of these risks through their social networks may heighten their concerns, influencing overall perception of online safety. These findings highlight the nuanced nature of online safety concerns, where insecurity arises not only from real but perceived dangers.

Furthermore, the top three threats faced by teens on social media are scams, followed by hacking and cyberbullying. These findings are consistent with another survey, which found that Malaysian youth under the age of 20 face a significantly higher risk of falling victim to fraud and scams compared to other age groups.[11] [12] These trends highlight the vulnerability of younger internet users, who may lack the experience or awareness to identify fraudulent schemes. A deeper exploration of these threats, including their impact and how teens respond to them, will be discussed in the following sections of this white paper.

9. The act of deliberately posting inflammatory, upsetting, or provocative content online with the intention of provoking others into responding emotionally or disrupting discussions.
10. Deceptive schemes or fraudulent activities designed to trick people into giving away money, personal information, or access to systems, often through misleading offers or fake promotions.
11. See Internet User Survey 2022, MCMC, 2022
12. See Figure A9 in Appendix B for further details.

Cyberbullying, Online Harassment and Trolling

Figure 12:
About one in four teens feel unsafe due to cyberbullying, online harassment, and trolling on social media.

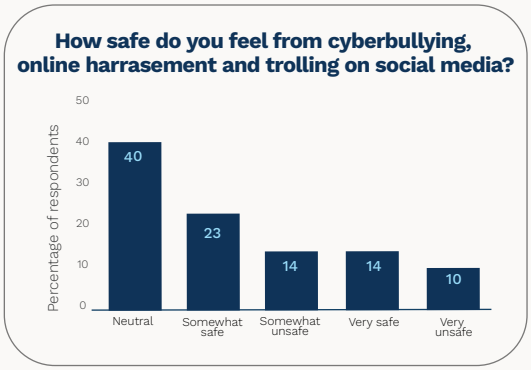


Figure 13:
One in five teens report being cyberbullied, harassed, or trolled online.

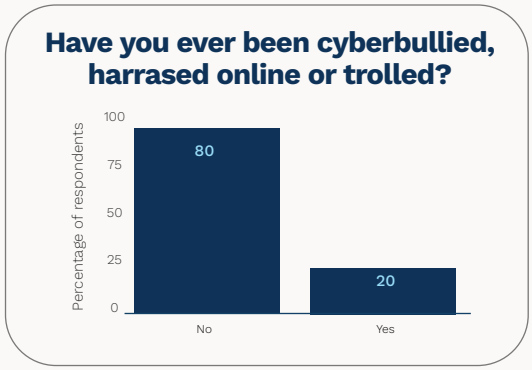


Figure 14:
However, most teens experience these threats rarely.

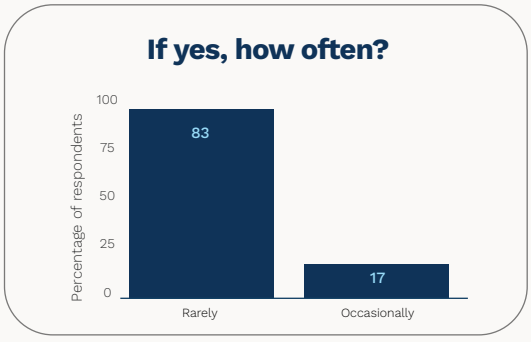


Figure 15:
More than two-thirds of teens do not know the perpetrators.

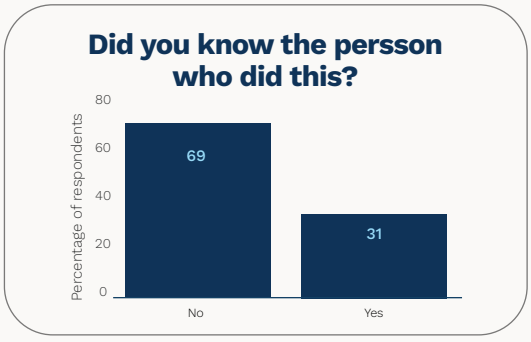


Figure 16:
Among those who know the perpetrators, most are friends or acquaintances.*

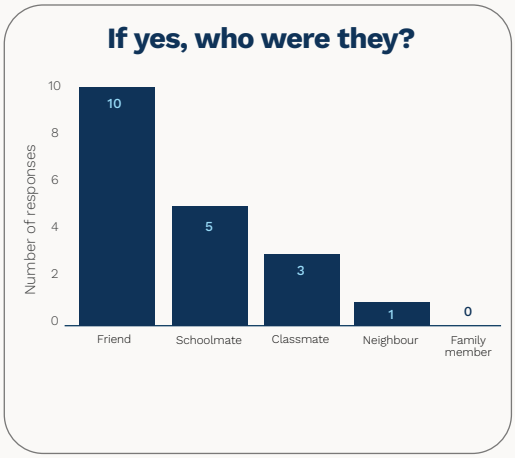
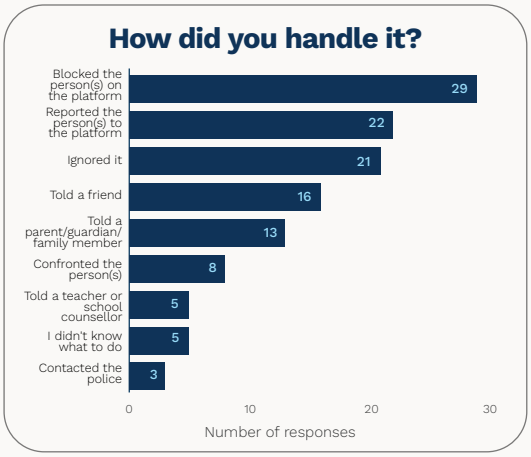


Figure 17:
Most teens who experience these threats either block or report the perpetrator to the platform.*



Source: SERI Malaysia (Author's Findings from Survey, 2024)
Note: * Indicates survey questions where respondents are permitted to provide multiple responses.

About one in four teens reported feeling unsafe on social media due to cyberbullying, online harassment[13], and trolling[14] (Figure 12), with one in five having experienced these threats themselves although rarely (Figures 13 and 14). These findings align with those from another survey, which found that Malaysian youth aged below 20 experience a disproportionately high incidence of cyberbullying.[15] [16] More worryingly, more than two-thirds did not know their bullies (Figure 15). This is significant because the anonymity of the online environment allows perpetrators to hide behind fake profiles, making it difficult for victims to identify or confront them. Meanwhile, for the minority of teens who did know their bullies, the vast majority reported that these perpetrators were their peers (Figure 16).

It is also worth noting that at least one in five Malaysian teenagers have themselves been involved in bullying activities through the internet, mobile phones, or other electronic devices[17]. Common forms of cyberbullying include making rude comments online, spreading rumours, sharing embarrassing photos, making threats, and soliciting sexual conversations or activities[18]. In one of the interviews conducted, an interviewee shared her own experience of bullying a classmate. She and her friends created a WhatsApp group to disparage another girl, but things took a turn when the victim discovered the group. The situation escalated further when the victim's older sister, an adult, shared screenshots of the cyberbullying on Facebook as well as publishing her private contact details, which led to the interviewee receiving hate comments from strangers. When the school found out about the incident, not only were the interviewee and her friends disciplined, but the victim was also reprimanded due to her sister's public disclosure of the incident on social media.

This case highlights not only the complexities surrounding vigilantism[19] in the digital age but also the unintended consequences of online actions and the shifting roles of victim and perpetrator. It underscores the pressing need for comprehensive online safety frameworks, particularly for minors, to address the risks posed by digital platforms. The victim's sister clearly felt it was necessary to expose the cyberbullying incident and share personal details of the perpetrator, raising critical questions about the appropriateness of such actions, especially when both the victim and the perpetrators were minors. The case exemplifies the challenges of balancing accountability with protection, emphasising the need for clear, enforceable guidelines to prevent further harm while fostering a better understanding of responsibility among both young people and adults navigating the digital landscape. At the same time, it is clear that platforms play a critical role as the first line of defence for victims of cyberbullying. Most teens who experience these threats take action by either blocking or reporting the perpetrator to the platform (Figure 17).

13. The act of using the internet to repeatedly and deliberately abuse, threaten, or annoy an individual, through actions such as offensive messages, stalking, or spreading malicious rumours.
14. The act of deliberately posting inflammatory, upsetting, or provocative content online with the intention of provoking others into responding emotionally or disrupting discussions.
15. See Internet User Survey 2022, MCMC, 2022
16. See Figure A10 in Appendix B for further details.
17. See Technical Report National Health and Morbidity Survey (NHMS)2022: Adolescent Health Survey, Institute for Public Health (IPH) Malaysia, 2022
18. Ibid.
19. The act of taking the law into one's own hands by engaging in actions intended to punish perceived wrongdoers, often without legal authority or due process. This can involve individuals or groups seeking justice outside of official legal channels.

Unwanted Advances, Blackmail and Doxxing

Figure 18:
More than half of teenagers reported feeling unsafe due to unwanted advances, blackmail, and doxxing on social media.

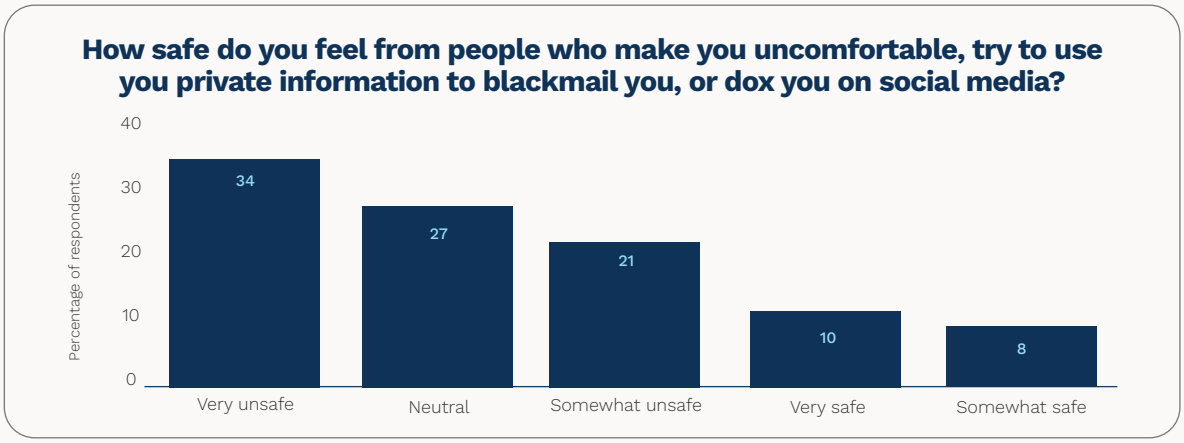


Figure 19:
More than one in four teenagers reported feeling uncomfortable due to the way someone interacted with them online.

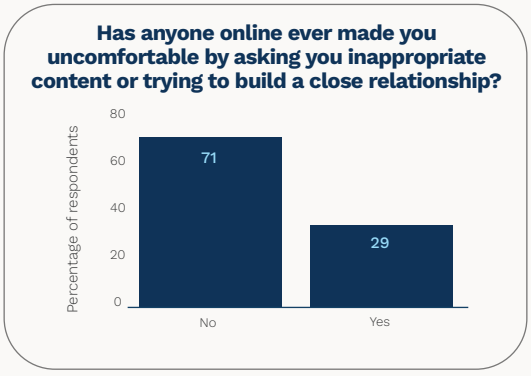


Figure 20:
Most teenagers took action by either blocking or reporting the person who made them feel uncomfortable on the platform.*

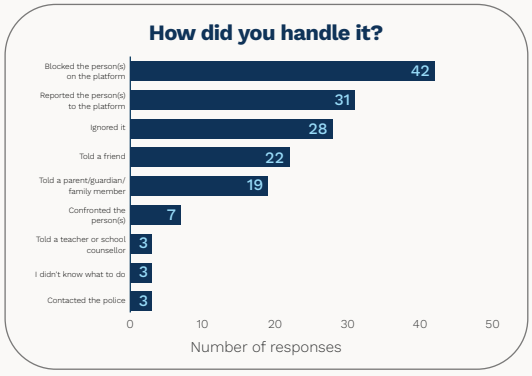


Figure 21:
The majority of teenagers reported never having been blackmailed with their private information.

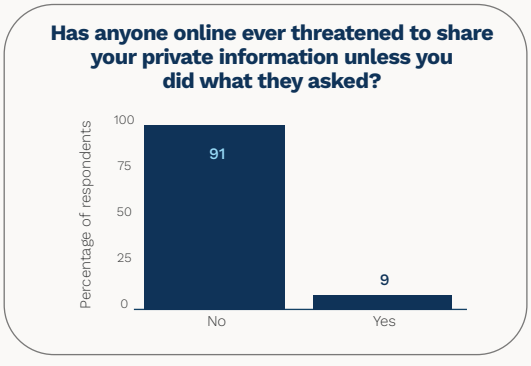


Figure 22:
Among teenagers who experienced blackmail, most responded by either reporting or blocking the perpetrator on the platform.*

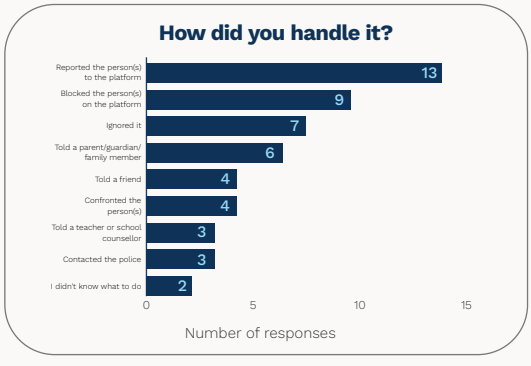


Figure 23:
Most teenagers have not faced any personal data leaks on social media.

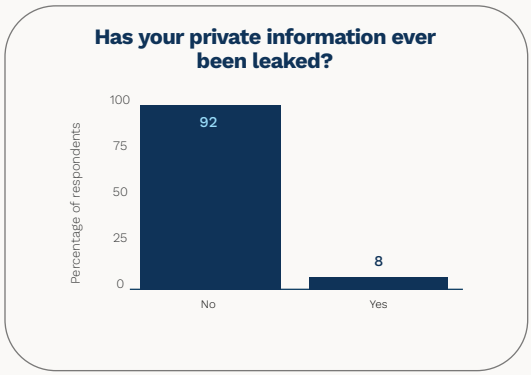
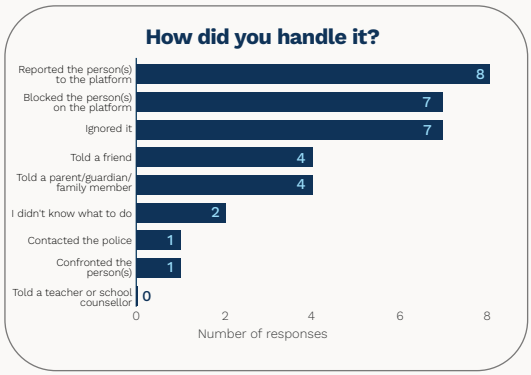


Figure 24:
For those who faced data leaks, they responded by either reporting or blocking the perpetrator on the platform, while an equal number chose to ignore the issue altogether.*



Source: SERI Malaysia (Author's Findings from Survey, 2024)
Note: * Indicates survey questions where respondents are permitted to provide multiple responses.

More than half of teenagers reported feeling unsafe due to unwanted advances, blackmail, and doxxing[20] on social media (Figure 18), which is consistent with a past study that found around one third of Malaysian children aged 12-17 come across explicit content via social media[21]. Furthermore, more than one in four teenagers reported feeling uncomfortable due to the way someone interacted with them online (Figure 19), taking action by either blocking or reporting the person who made them feel uncomfortable on the platform (Figure 20). This proactive approach to online safety is reflected in personal accounts as well. For example, one interviewee shared how her female friend received a highly disturbing direct message on Instagram from a stranger, which included an explicit photo. In addition to reporting the account to the platform, her friend also took the step of reporting the incident to the police to ensure further action was taken. These findings collectively suggest that many teenagers are able to recognise when they are in an unsafe situation online and take steps to protect themselves by using the tools available to them. However, this may not be the case for all, as awareness and action can vary depending on individual circumstances and knowledge.

Additionally, while the majority of teenagers reported never having been blackmailed with their private information (Figure 21) or having faced any personal data leaks on social media (Figure 23), those who did experience either of these incidents generally responded by either reporting or blocking the perpetrator on the platform (Figures 22 and 24). However, it is worth noting that a significant number of those who experienced data leaks chose to ignore the incident altogether (Figure 24). This could be due to factors such as fear of retaliation, uncertainty about how to respond, or a lack of trust in authorities or online platforms. While this may seem like a passive response, it is concerning because ignoring such incidents leaves individuals vulnerable to further exploitation and undermines efforts to improve online safety. Without reporting or addressing these issues, teens may not take the necessary steps to protect their privacy, increasing their risk of ongoing harm.

20. The malicious act of publicly revealing or publishing private information about an individual, such as their home address or contact details, without consent, often to harm or harass the person.
21. See Disrupting Harm in Malaysia: Evidence on Online Child Sexual Exploitation and Abuse, ECPAT, INTERPOL, and UNICEF, 2022

This vulnerability is further illustrated by a real-life example from one of our interviews. The interviewee described an incident involving a friend who trusted a stranger on Twitter with a transaction for a game top-up. The perpetrator convinced the friend to download an app requesting access to his photos. Once access was granted, the perpetrator gained entry to the victim's photo album, created explicit AI-generated[22] videos, and threatened to release them unless a ransom was paid. Although the friend contacted the police, he felt they were unable to offer any meaningful assistance. The incident concluded without further action, but it underscores how easily teens can be manipulated online and highlights the serious consequences of failing to address such threats comprehensively. This example further emphasises the broader concern that, without proper reporting mechanisms or a clear understanding of how to protect themselves, teens may remain vulnerable to exploitation.

Scams, Impersonation and Hacking

Figure 25:
Nearly half of teenagers reported feeling confident in spotting scams, impersonations, and hacks on social media.

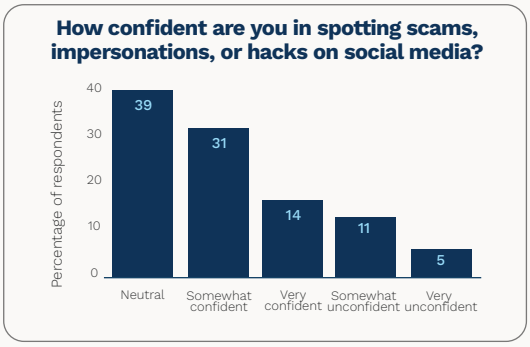


Figure 26:
More than half of respondents have seen, but not been victims of, scams.

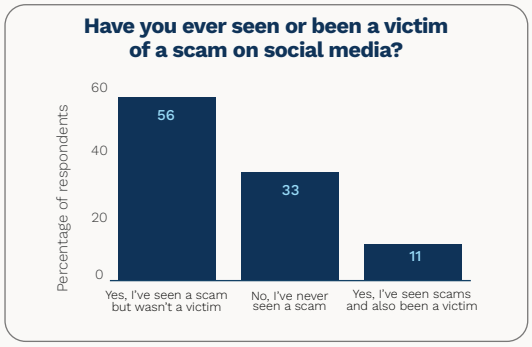


Figure 27:
The most common form of scams teenagers came across on social media was fake offers or deals.*

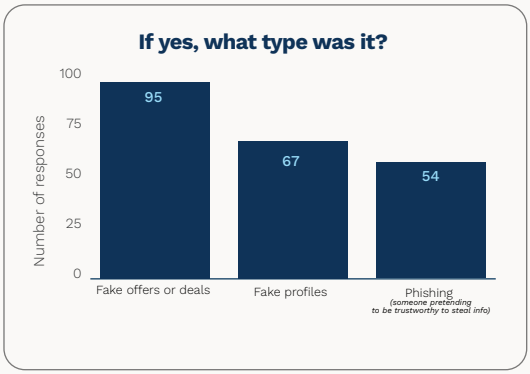
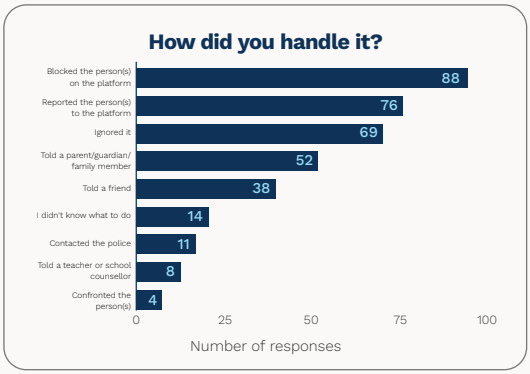


Figure 28:
For those who came across or fell victim to scams, they responded by either reporting or blocking them on the platform.*



Source: SERI Malaysia (Author's Findings from Survey, 2024)
Note: * Indicates survey questions where respondents are permitted to provide multiple responses.

22. Content, such as text, images, or videos, created by artificial intelligence (AI)systems using algorithms and machine learning to produce outputs that mimic human creativity or interaction.

Almost half of teenagers reported feeling confident in spotting scams, impersonations[23], or hacks[24] on social media (Figure 25). Despite encountering scams, more than half of teens indicated that they had not fallen victim to any (Figure 26), with fake offers and deals being the most common types of scams they experienced, followed by fake profiles and phishing[25] (Figure 27). For those who came across or fell victim to scams, the vast majority responded by either reporting or blocking the offenders on the platform (Figure 28).

In one of the interviews, we learned about the interviewee's female friend, who was targeted by a scammer on Instagram. The scammer offered her the opportunity to join a team and earn 'easy money'[26], promising that for every RM1 invested, RM2 would be returned, and for RM4, RM8 would follow. Initially hesitant to engage, she was gradually convinced by the scammer's persistent messages, which included small returns that appeared legitimate. As a result, she became further entangled in the scam and was eventually scammed out of a substantial amount, running into the thousands of ringgits. When attempting to report the incident to the police, she found that the law enforcement officers were unwilling to take action or offer assistance. This case highlights not only the manipulative tactics used by scammers to exploit vulnerable users, but also the challenges in holding perpetrators accountable and the lack of responsive support systems for victims.

Gaming-Related Scams Are on the Rise

Interviews with teenagers have revealed a growing trend of gaming-related scams, with many interviewees or their peers having experienced such schemes firsthand are often orchestrated through social media platforms such as Instagram, Discord, or Facebook, exploiting teenagers' lack of access to financial tools such as bank accounts and their reluctance to seek parental assistance, fearing disapproval of gaming-related spending. Scammers frequently pose as helpful strangers or experienced players, offering to purchase in-game currency in exchange or upfront payments. Using fake profiles and tactics such as impersonating high-level gamers or advertising exclusive deals, they build trust or create urgency before absconding with the funds. Addressing this issue requires coordinated efforts from parents, educators, and enforcement agencies. Beyond promoting digital literacy, policies should prioritise financial education for teenagers, equipping them to recognise secure payment methods, including the risks of transferring money without safeguards. Open, non-judgemental communication within families can further mitigate risks and foster safer online interactions.

23. The act of pretending to be someone else online, typically to deceive others or gain access to information, resources, or accounts by misrepresenting one's identity.
24. Unauthorised access to computer systems, networks, or devices, typically to steal, alter, or destroy data, or to disrupt normal operations, often for malicious purposes.
25. A fraudulent attempt to acquire sensitive information, such as passwords or credit card details, by pretending to be a trustworthy entity, often through deceptive emails or websites.
26. Money that is gained with little or no effort, often through shortcuts, schemes, or in ways that may be considered dishonest or unethical.

Online Safety Awareness and Practices

Figure 29:
Four in five teenagers reported having received some form of online safety education.

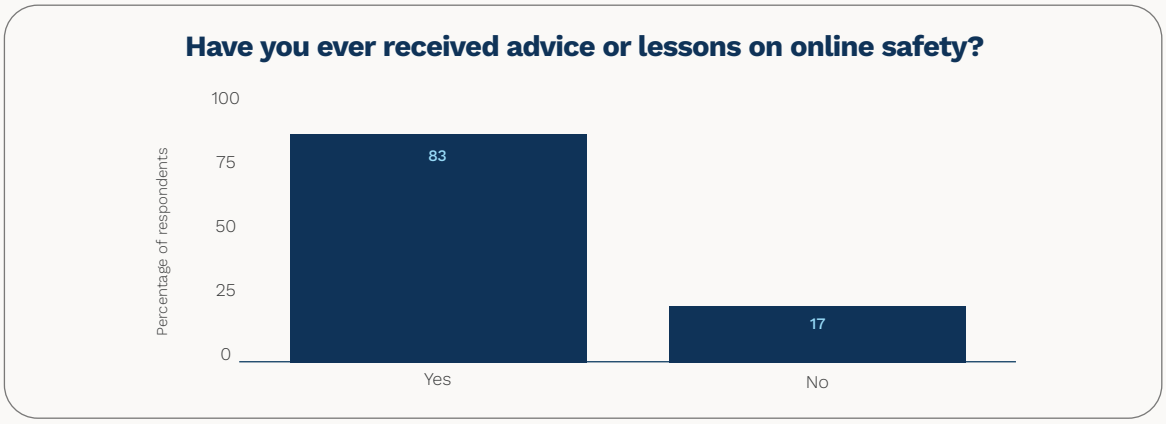


Figure 30:
The top three sources of the information they received were from schools, followed by their family and online resources.*

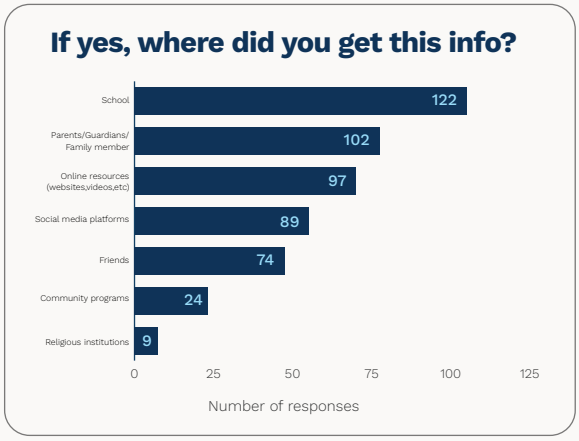
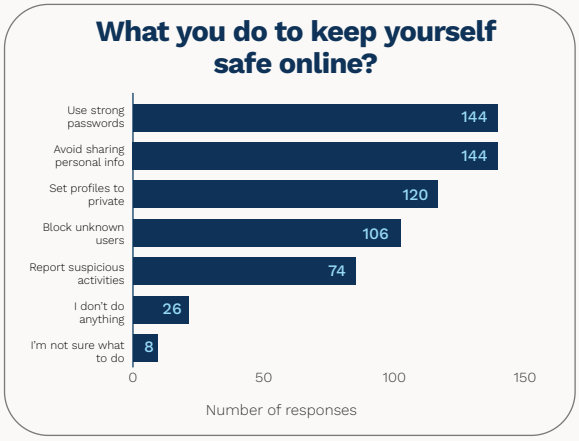


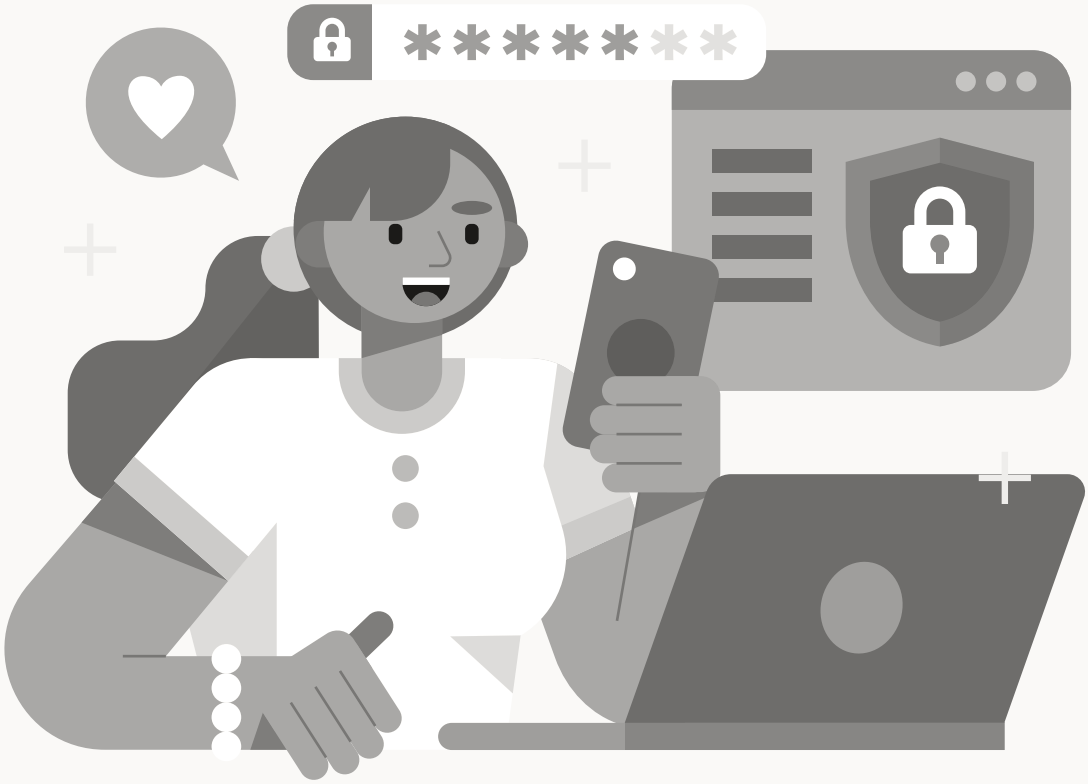
Figure 31:
Most teenagers employ various strategies to keep themselves safe online.*



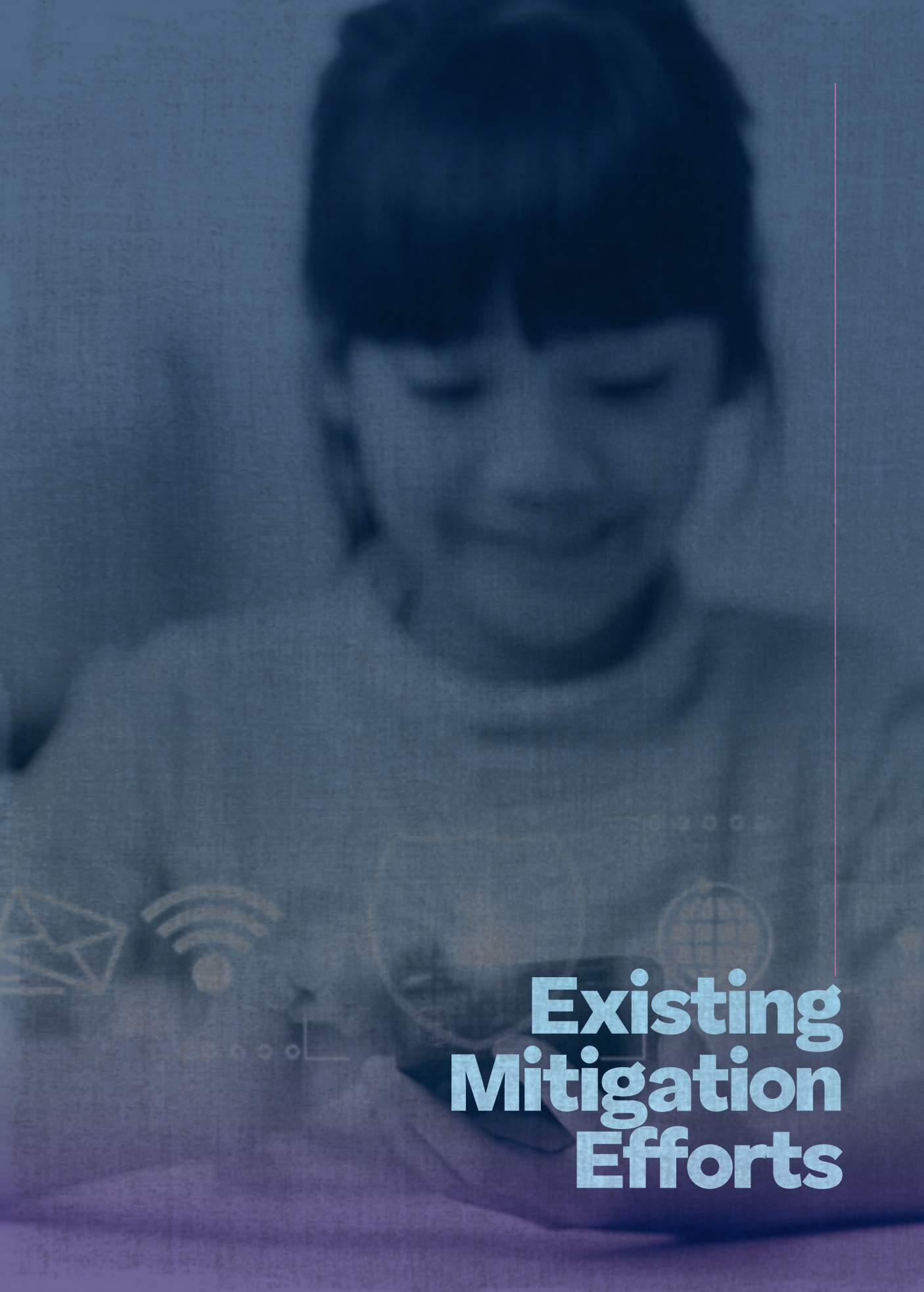
Source: SERI Malaysia (Author's Findings from Survey, 2024)
Note: * Indicates survey questions where respondents are permitted to provide multiple responses.

Four in five teenagers reported having received some form of online safety education (Figure 29), with school being the top source of the information, followed by their family and online resources (Figure 30). Most teenagers also take several steps to protect themselves online, including using strong passwords and avoiding sharing personal information as the most common strategies, followed by setting their profiles to private and blocking unknown users (Figure 31) which align

with the UNICEF study[27], showing that teenagers generally have a good understanding of online safety. However, they differ from the findings of another study[28][29], which found that digital safety literacy is lower among youths aged 19 and under, compared to adults. Additionally, in the FGD, one of the parents did express concern that teenagers lack the necessary education about privacy settings, the permanence of online content, and the risks of sharing personal information. These variations underscore the importance of considering socio-economic background, access to resources, and the urban-rural divide, since these factors can create gaps in digital literacy[30] education, highlighting the need for targeted interventions to ensure equal access to online safety education across different communities.



27. See Disrupting Harm in Malaysia: Evidence on Online Child Sexual Exploitation and Abuse, ECPAT, INTERPOL, and UNICEF, 2022
28. See ICT Use and Access by Individuals and Households Survey Report, Department of Statistics Malaysia, 2023
29. See Table A1 in Appendix B for further details.
30. The ability to effectively and responsibly use digital technologies, including understanding how to access, evaluate, and communicate information safely and ethically online.



Existing Mitigation Efforts

In response to the growing online risks faced by Malaysian teenagers, a range of mitigation strategies have been introduced by parents, educators, social media platforms, and regulators. This section explores these efforts, starting with the critical roles of parents, teachers, and schools in guiding teenagers' use of social media through parental mediation and digital literacy education. We also examine the safeguards implemented by social media platforms, such as Instagram's Teen Accounts and TikTok's Guardian's Guide, which aim to create safer digital environments for young people in Malaysia. Additionally, we review the Malaysian regulatory landscape that governs the online environment, including recent developments. Case studies from Japan and New Zealand showcase innovative approaches and emerging strategies that could inform and improve online safety for Malaysian teenagers. These efforts underscore the growing need for a more integrated, multi-stakeholder approach to enhancing online safety within the social media landscape, where collaboration across parents, educators, platforms, and regulators will be key.

Role of Parents, Teachers, and Schools: Guiding Teen Online Safety

Parents, teachers, and schools are key in shaping teenagers' digital experiences and protecting them from online risks. Parents are vital in guiding their children's online behaviour, setting boundaries, and encouraging open dialogue about internet safety. Teachers and schools, in turn, play a critical role in equipping students with the digital literacy skills needed to interact with online spaces safely and responsibly. Together, these two approaches—parental mediation at home and digital literacy education in schools—help ensure that teenagers are not only protected from immediate online threats but also empowered to make informed decisions in the digital world.

Parental Mediation

Figure 32:
A significant majority of teenagers reported that their parents/guardians knew about their social media use.

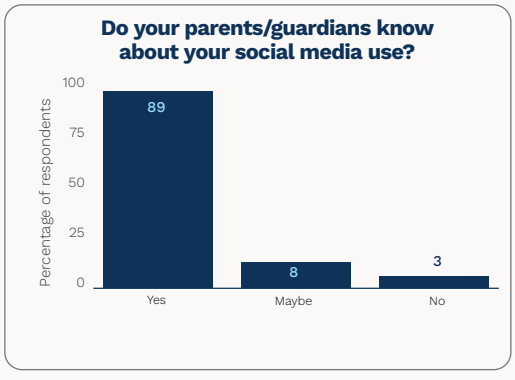


Figure 33:
More than half of the parents/guardians of the teenagers did not restrict their social media usage.

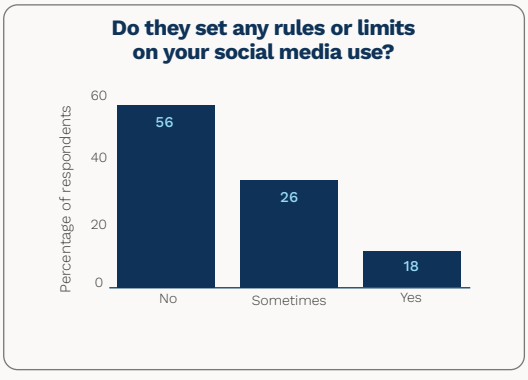


Figure 34:
The most common rule set by their parents was to limit screen time.*

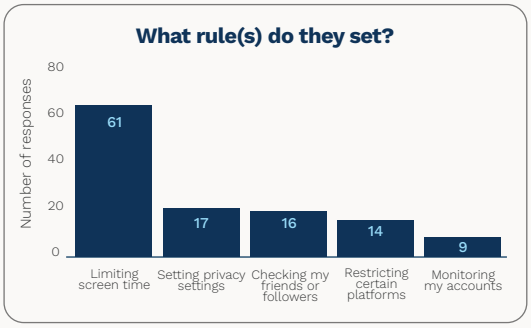
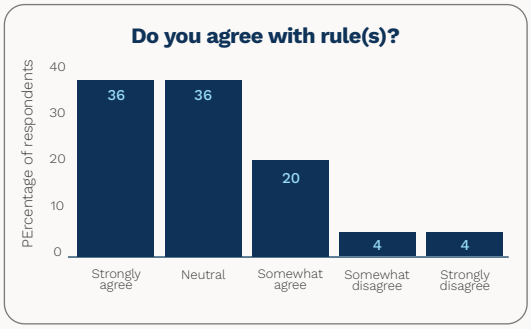


Figure 35:
Most teenagers either agreed with or were indifferent to the rules set by their parents.



Source: SERI Malaysia (Author's Findings from Survey, 2024)
Note: * Indicates survey questions where respondents are permitted to provide multiple responses.

'Parental mediation' refers to the diverse strategies parents use to manage and regulate their children's social media experiences.[31] Our survey findings show that a significant majority of teens reported that their parents were aware of their social media usage (Figure 32). Almost half of the teens said their parents had set rules around their social media use (Figure 33), with the most common rule being limiting screen time[32] (Figure 34). Furthermore, most teens either agreed with or were indifferent towards the rules set by their parents (Figure 35). This could be partly explained by our FGD findings, where all participants agreed that teenagers can often find ways to bypass parental controls[33]. One parent shared an example of how one of her son's friends, whose parents had banned him from using a phone, would use her son's phone to access social media. To address this, the same parent explained that, rather than banning smartphones and social media, she regularly talks to her teenagers about how they use these platforms. This helps build trust, encourages open communication, and ensures a safer online experience.

However, another parent firmly believed that children should be banned from social media until they are 18. She has told her children this, as she believes that children benefit more from physical connections than virtual ones. She is also concerned about the strangers they meet online and the influence these strangers could have on them. Her concerns may reflect a broader sentiment shared by Malaysians, as a recent survey found that 71% of Malaysians believe social media should be banned for children under the age of 14.[34] These contrasting perspectives highlight the ongoing debate between strict regulation and open dialogue when it comes to managing children's online activity. Nevertheless, the common view remains that many parents still feel ill-equipped to discuss online safety with their children.

31. See How parents of young children manage digital devices at home: The role of income, education and parental style, Livingstone, Sonia, Giovanna Mascheroni, Michael Dreier, Stephane Chaudron, and Kaat Lagae, 2015
32. The amount of time spent using electronic devices such as smartphones, tablets, or computers, often with a focus on managing and limiting the amount of time spent on digital activities for health and well-being.
33. Software or tools that allow parents to monitor, limit, or block access to certain content or applications on digital devices, helping protect children from inappropriate material or excessive screen time.
34. See Education Monitor, Ipsos, 2024

Online Safety Concerns Differ by Gender

Insights from focus group discussions (FGDs) revealed that societal norms heavily influence how parents and educators address teen online safety, often prioritising girls' safety over boys'. A representative from an NGO observed that mothers in particular, are more vigilant about protecting daughters from risks such as scams, exploitation, and sexual violence. Meanwhile, boys' safety may receive less attention, even though they are more likely to engage in harmful behaviours like cyberbullying or exploitation, often due to limited oversight and a lack of accountability. The conversation also highlighted how gendered expectations influence how teens are monitored online, with boys often perceived as less vulnerable. To address these disparities, a more comprehensive, gender-sensitive approach to online safety must be adopted, ensuring that both girls and boys are equally guided and protected from online risks.

Digital Literacy Education

As teenagers spend much of their time in school, educators are uniquely positioned to guide and protect them in the digital world. This responsibility is widely recognised, with 56% of Malaysians believing that schools should take the lead in teaching digital literacy and online safety, a view echoed across Southeast Asia.[35] Moreover, our survey shows that schools are viewed as the primary source of guidance on online safety among teenagers (Figure 30), underscoring the critical role educators play in preparing students to navigate the digital world responsibly. However, despite this trust, it is also important to note that teachers and school counsellors are among the least approached by teens seeking help with issues such as cyberbullying (Figure 17), unwanted advances (Figures 20, 22 and 24), and scams (Figure 28). This discrepancy suggests a gap between the trust placed in schools as sources of online safety education and the actual engagement with school-based support when students face digital challenges.

Meanwhile, a growing challenge for schools is that many students are becoming disengaged from traditional lessons across all subjects, not just in online safety education. In our FGD, a teacher participant highlighted how the increasing dominance of social media platforms—where teens primarily connect, learn, and explore new ideas—has created a disconnect between students and the classroom.

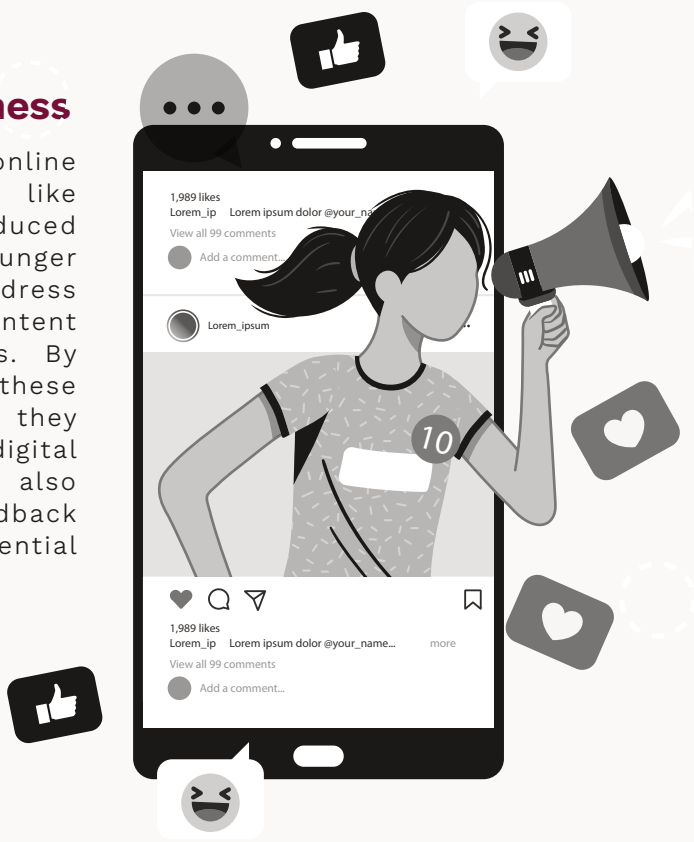
35. See Education Monitor, Ipsos, 2024

Students often find the information they access through social media and the internet more relevant than what is taught in school, making it harder for teachers to capture their attention in lessons. This disengagement affects not only online safety education but also other subjects, as students are more invested in platforms like YouTube and TikTok for learning and socialising. The teacher suggested that educators explore ways to integrate these digital platforms into lessons, using tools like Discord to connect with students in a space they already inhabit, and make lessons more engaging and relevant to their digital lives.

This challenge in engaging students is further compounded by gaps in the current methods of online safety education in schools, as highlighted by all interviewees. One participant noted that while teachers advise students to be cautious about what they post online and who they interact with during moral education lessons, often in a manner that can be perceived as preachy or fear-mongering, practical skills such as how to identify scams, assess others' intentions online, or communicate safely are not taught. Another interviewee raised concerns about the limited ability of teachers to assist students, given that they are often unaware of their students' social media activities. A third participant mentioned that online safety talks were organised not only in her secondary school but also in her primary school, introducing students to basic safety concepts. However, most interviewees agreed that digital literacy seminars and workshops in schools are often one-way, unengaging, and difficult to follow. These insights underscore the need for more comprehensive, interactive, and practical online safety education in schools, which can better address the complexities of real-world digital interactions.

Platform Safeguards: Awareness and Effectiveness

As concerns over teen safety online continue to grow, platforms like Instagram and TikTok have introduced various safeguards to protect younger users. These measures aim to address issues such as privacy, content exposure, and user interactions. By examining the features of these platforms, we can assess how they contribute to creating safer digital environments for teens, while also taking into account parental feedback on their effectiveness and potential limitations.



Instagram's Teen Accounts

Instagram is launching Teen Accounts which are accounts that come with built-in protections that are automatically applied to ensure safe and controlled experiences on the platform. For teens under 16, Instagram applies a set of default settings that limit who can contact them, what content they see, and how their time is managed on the platform.

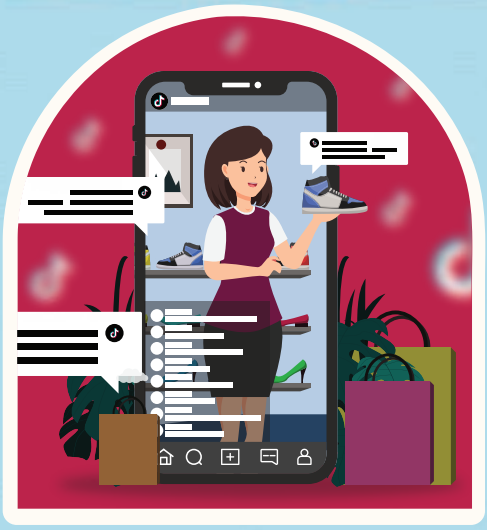
Key Protections for Teen Accounts:

- **Private Accounts:** Accounts for teens under 16 are automatically set to private. Teens must approve new followers before they can see or interact with their content. For users aged 16 and 17, the accounts will also be private by default, but they will have the option to switch to a public account or defer the decision by selecting "remind me later."
- **Messaging Restrictions:** Teens can only receive messages from people they follow or are already connected with, reducing the risk of unsolicited contact.
- **Sensitive Content Controls:** Teens are automatically placed in the strictest setting to limit exposure to sensitive content, such as violent material or posts promoting cosmetic procedures.
- **Limited Interactions:** Teens can only be tagged or mentioned by people they follow, helping to reduce unwanted attention. The **Hidden Words** anti-bullying feature is also enabled by default, filtering offensive language in comments and direct messages.
- **Time Limit Reminders:** Teens will receive reminders to take breaks after 60 minutes of app usage to promote healthier screen time habits.
- **Sleep Mode:** This feature will be activated between 10 PM and 7 AM, muting notifications and sending auto-replies to DMs to support good sleep hygiene.

Instagram is aware that some teens may attempt to bypass these protections by providing false age information. To address this, the platform is implementing additional age-verification measures. Teens will be required to verify their age if they attempt to create an account using an adult birthdate. Instagram is also developing new technology to identify accounts that may belong to teens, even if they list an adult birthday. This technology will automatically apply Teen Account protections to those accounts, ensuring that they are adequately protected.

Teen Accounts will be available within 60 days of the announcement made on 17th September 2024, first launching in the United States, United Kingdom, Canada, and Australia. The rollout will extend to the European Union later in the year, with global availability beginning in January 2025. Instagram also plans to extend Teen Accounts to other Meta platforms in the following year.

Source: Introducing Instagram Teen Accounts: Built-In Protections for Teens, Peace of Mind for Parents, Instagram, 2024



TikTok's Guardian's Guide

During our FGD, a representative from TikTok outlined several features aimed at protecting teenagers on the platform. These protections are designed to address concerns around privacy, content exposure, and overall safety for users under 18. The details of these features can be found at its Safety Centre.

Key Protections for Teen Users:

- **Private Accounts:** Accounts for teens under 16 are set to private by default, requiring approval for new followers to view or interact with their content.
- **Messaging Restrictions:** Teens under 16 do not have access to direct messaging or group chats (where available), limiting the possibility of unsolicited contact from strangers.
- **Content Exposure:** Content posted by accounts for teens under 16 is not recommended in the **For You** feed of users they don't follow, reducing exposure to potentially inappropriate content.
- **Live Streaming:** Only users aged 18 or older are allowed to broadcast live, ensuring that live interactions are more appropriate for adult users.
- **Screen Time Limits:** A default screen time limit of 60 minutes is set for all accounts under 18. This can be customised further through Family Pairing, which allows parents to manage screen time settings for their teens.
- **Family Pairing:** This tool enables parents or guardians to link their TikTok accounts with their teen's account. It provides several customisation options, including:
  - Setting a **daily screen time limit,** which teens can extend by requesting a passcode from a parent.
  - **Filtering the For You feed** by excluding videos containing specific keywords chosen by the parent.
  - **Customising comment controls** to allow or limit interactions on the teen's posts, including the option to
- **Community Guidelines:** These rules are designed to help safeguard users, especially those under 18, from harmful or inappropriate content.

TikTok acknowledges that some teenagers may attempt to bypass these protections by providing false age information. To address this, the platform is implementing **additional age verification** measures. Teens will now be prompted to verify their age if they try to create an account using an adult birthdate. Furthermore, TikTok is developing new technology to proactively identify accounts that likely belong to teens, even if an adult birthdate is listed. When such accounts are detected, they will automatically be placed under the same protective settings as other teen accounts.

Source: Guardian's Guide, TikTok, 2024

Effectiveness of Platform Safeguards

As highlighted earlier in the survey findings, a significant majority of teens respond to online threats—such as cyberbullying (Figure 17), unwanted advances and blackmail (Figures 20, 22, and 24), and scams (Figure 28)—by blocking the perpetrator or reporting the incident directly to the platform. This suggests a high level of awareness among teens about the platform's safeguards and their confidence in using these tools as their primary means of protection. However, it is also worth noting that teens are much less likely to involve adults, such as parents, teachers, or law enforcement, in responding to or addressing online harms. This contrast indicates that, while teens are proactive in using platform tools for self-protection, they tend to rely on these safeguards rather than seeking external support. This could stem from a desire for privacy and autonomy in managing online threats, though it may also reflect a belief that these tools are sufficient. The reluctance to involve adults suggests a potential gap in support, which could have implications for how teens engage with both platforms and offline support systems.

While teens recognise the value of platform safeguards, many believe these measures have inherent limitations. Most interviewees acknowledged that, while content moderation[36] systems like filters[37] and algorithms[38] can be improved, these tools cannot prevent all forms of online harm.

This view was shared by all interviewees, who emphasised the importance of self-regulation[39] and self-awareness[40] in managing their online presence. They argued that individuals must take greater responsibility for what they share and who they connect with online to reduce their vulnerability to threats. Some interviewees also noted that, while platforms can enhance safety measures, the responsibility to safeguard against risks ultimately lies with users.

36. The process of monitoring, reviewing, and managing user-generated content on digital platforms, such as social media or websites, to ensure it complies with community guidelines, legal regulations, and ethical standards, often to prevent harmful, offensive, or inappropriate material.
37. Tools or software settings that screen or limit access to certain types of content, typically used to block inappropriate or unwanted material on websites, social media, or search engines.
38. A set of rules or instructions followed by a computer to perform a specific task or solve a problem, often used in processing data or powering technologies such as search engines, social media feeds, or recommendations.
39. The ability of an individual or organisation to monitor and control their own actions, behaviours, or decisions without external influence, often in the context of managing online activities, content, or interactions responsibly.
40. The ability to recognise and understand one's own emotions, thoughts, and behaviours, and how they affect others. It is an essential aspect of emotional intelligence and personal development, particularly in managing online interactions and digital well-being.

Enhancing Age Assurance in Social Media

Platforms such as Instagram, TikTok, Facebook, and X (formerly Twitter) enforce age restrictions prohibiting children under 13 from creating accounts, yet the effectiveness of these measures warrants closer scrutiny. Interviews conducted during this study revealed that a significant proportion of teenagers had created accounts as early as 9 or 10 years old. While their initial use was largely passive—focused on observing rather than posting content—active engagement, including sharing personal photos and videos, typically began during secondary school. Nevertheless, this does not mitigate the concerns posed by their presence on social media platforms under the age of 13, as it highlights significant gaps in the enforcement of age restrictions and raises critical issues regarding children's exposure to inappropriate content, risks to their privacy, and early engagement with unregulated digital environments. These findings underscore the urgent need for robust age assurance[41] and age verification mechanisms that are both reliable and privacy-conscious. Policymakers and platforms must collaborate to strengthen these tools and enforcement strategies, ensuring a safer and more accountable digital ecosystem for younger users.

Meanwhile, insights from the FGD, with parents reveal that awareness of these features is more varied among parents. One parent mentioned being unaware of the safeguards, while another, although familiar with them, expressed concerns about their effectiveness. Both highlighted the challenge that teenagers may find ways to bypass restrictions, raising questions about the reliability of these safeguards in practice. Additionally, some parents pointed out that even with the available controls, there were gaps in understanding how to use them effectively, which could affect their implementation. It is also worth noting that for some parents, not having an account on these platforms exacerbates the challenge, as they lack direct experience with the digital spaces their children engage with.

41. The process of verifying the age of an individual to ensure they meet the minimum age requirements for accessing certain online services, platforms, or content, often to protect children and young people from age-inappropriate material or interactions.

Given these concerns, it is clear that raising awareness among parents about how these safety features work and how to use them effectively is crucial. Ensuring that parents are informed and equipped to navigate these tools is essential for their proper implementation, especially as teenagers continue to find ways to circumvent restrictions.

Regulatory Framework: Recent Developments and International Best Practices

The Communications and Multimedia Act 1998 (CMA 1998) is the primary legislation governing the communications and multimedia industry, which sets out a regulatory licensing framework. The Malaysian Communications and Multimedia Commission Act 1998 established the Malaysian Communications and Multimedia Commission (MCMC), a regulatory body for the industry.[42] As an agency under the Ministry of Communications, MCMC also advises the Minister on national policy matters and carries out any functions prescribed by the Minister through notifications published in the Gazette.[43]

Pursuant to Section 212 of the CMA 1998, the Communications and Multimedia Content Forum of Malaysia (Content Forum) serves as the industry forum tasked with overseeing and promoting self-regulation of content across electronic networks.[44] It is also responsible for implementing and enforcing the Malaysian Communications and Multimedia Content Code ("the Content Code").[45] The Content Forum houses a Complaints Bureau, which is empowered to address all complaints related to content disseminated over electronic networks.[46]

42. See History, MCMC
43. See Our Responsibility, MCMC
44. See Brief Overview of the Content Forum, Content Forum
45. Ibid.
46. Ibid.

Stakeholder Map for Social Media Safety

This stakeholder map outlines the key organisations and entities involved in promoting the safety of teenagers on social media platforms in Malaysia. It highlights the fragmented nature of current efforts to address online risks, with some roles and responsibilities potentially overlapping or being redundant. This lack of clarity in role allocation presents challenges in developing a cohesive strategy to ensure a secure online environment for teenagers. A more integrated, multi-stakeholder approach is necessary to streamline efforts, eliminate redundancy, and effectively mitigate the risks faced by young users online.

Tier 1: Key Ministries and Agencies

Roles: Develop policies, enforce regulations, and ensure social media platforms comply with online safety laws

Stakeholders:

- Ministry of Communications
- Malaysian Communications and Multimedia Commission (MCMC)

Tier 2: Enforcement Agencies

Roles: Investigate and prosecute cybercrimes and provide legal support for victims

Stakeholders:

- Royal Malaysia Police (PDRM)
- Bank Negara Malaysia (BNM)
- Content Forum

Tier 3: Social Media Platforms

Roles: Develop and deploy safety measures, including content moderation and scam detection technologies to protect users from online harms

Stakeholders:

- Facebook
- Instagram
- TikTok
- X (formerly Twitter)
- WhatsApp
- Telegram
- Discord

Tier 4: Other Relevant Ministries and Agencies

Roles: Coordinate efforts to protect teens online, provide education and resources for online safety, and offer mental and emotional support for victims of online harms

Stakeholders:

- Ministry of Digital
- Ministry of Education (KPM)
- Ministry of Women, Family, and Community Development (KPWKM)
- Ministry of Health (KKM)
- National Cyber Security Agency (NACSA)
- CyberSecurity Malaysia (CSM)

Tier 5: Educational and Social Support Networks

Roles: Educate and support teenagers in navigating social media safely

Stakeholders: Parents, Teachers and Schools, Civil Society and Media

Tier 6: Users

Roles: Make informed and responsible decisions to protect themselves online

Stakeholders: Teenagers

Latest legislative developments include the introduction of the regulatory framework for internet messaging services and social media services, which will come into effect on 1 January 2025[47]. This framework mandates that all internet messaging service providers and social media service providers with at least eight million users in Malaysia must apply for an Applications Service Provider Class Licence under the CMA 1998[48]. In addition, MCMC is developing a Code of Conduct (Best Practice) for internet messaging service providers and social media service providers which sets out best practices for adoption by service providers licensed under the CMA 1998 and addresses issues such as harmful content online and outlines other relevant conduct requirements that must be observed.[49]

Amendments to the CMA 1998 to address concerns about the misuse of digital platforms and enhance protections for vulnerable groups, particularly children, are currently being debated in Parliament. The proposed changes include higher penalties for offences involving children and a broader definition of offensive content, covering categories such as obscene, indecent, false, menacing, and grossly offensive material. Another significant piece of legislation tabled in Parliament is the Online Safety Bill 2024, which will require social media platform providers to meet three key responsibilities: ensuring platform safety, protecting children under the age of 13, and restricting access to harmful content.[50]

Despite the progress made through recent legislative developments in Malaysia, concerns remain regarding the practical enforcement of regulations, particularly for smaller platforms that may struggle with compliance. Additionally, there is a risk that overly broad regulations could limit freedom of expression or stifle innovation in a rapidly evolving digital landscape. To remain effective, the regulatory framework will need continuous review to address emerging threats and ensure a balance between security and digital freedoms. In this context, case studies from countries such as Japan and New Zealand—outlined in more detail on the following page—offer valuable insights into international best practices for promoting teen safety, digital wellbeing, and literacy. These examples highlight key considerations that could inform future policy development in Malaysia (see Appendix A for detailed information on the case study protocol).

47. See MCMC Introduces Regulatory Framework for Internet Messaging and Social Media Service Providers, MCMC, 2024
48. Ibid.
49. See MCMC Seeks Public Input on Draft Code of Conduct (Best Practice)for Safer Online Environment in Malaysia, MCMC, 2024
50. See Online Safety Bill to Mandate Three Key Responsibilities for Platform Providers, Bernama, October 16, 2024

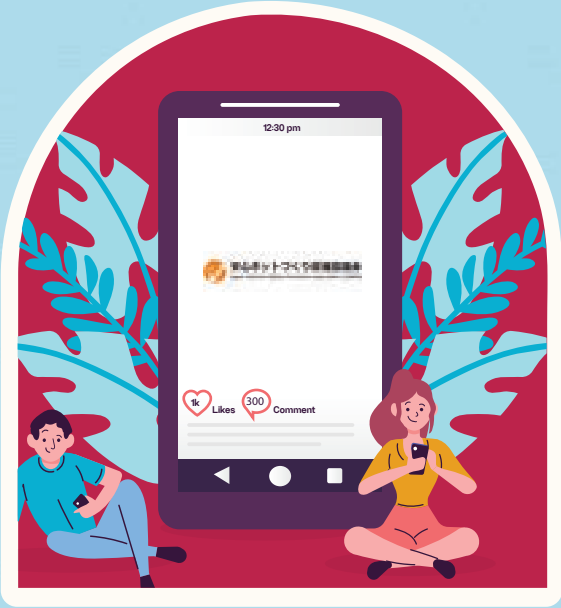
JISPA's Role in Shaping Japan's Youth Online Safety

With the growing reliance on digital platforms, young people in Japan are spending increasing amounts of time online. According to a fiscal survey by Japan's Children and Families Agency, high school students spend over six hours online, while junior high school students spend over four hours.[51]

Nevertheless, Japan has long recognised the need to address the risks associated with increased internet usage among young people, including cyberbullying, privacy violations,[52] and exposure to harmful content. The following case study outlines Japan's approach, offering valuable insights that can inform policy recommendations for Malaysia as it works to enhance digital safety and wellbeing for its youth.

Comprehensive Legislative and Policy Framework

Japan's **Act on Development of an Environment That Provides Safe and Secure Internet Use for Young People** (2008)[53] established a strong legal foundation for promoting safe internet use among youth. Alongside this, the **Basic Plan for Safe Internet Use for Young People**[54] was introduced, focusing on responsible internet use, digital literacy, and reducing exposure to harmful content through filtering technologies. The plan has been updated regularly, most recently in 2018[55], to address emerging issues such as cyberbullying, privacy protection, and online harassment.



This evolving policy framework ensures that Japan's approach remains adaptive to the changing digital landscape, effectively addressing new and growing risks.

Key Stakeholders and Cross-Sector Collaboration

Japan's approach to online safety emphasises collaboration among government bodies, the private sector, and civil society. **The Japan Internet Safety Promotion Association (JISPA),** founded in 2009, plays a pivotal role by bringing together diverse stakeholders to create a safer online environment for the Japanese public, including the youth[56]. JISPA promotes media literacy, encourages self-regulation in the private sector, and helps develop tools such as content moderation systems and safe browsing technologies.[57] This collaborative effort ensures a comprehensive response to online risks, pooling expertise from various sectors to safeguard young internet users.

51. See Japanese Youth Spend around 5 Hours a Day Online: Government Survey, Kyodo News, April 14, 2024
52. The breach or infringement of an individual's right to privacy, typically involving the unauthorised collection, use, or sharing of personal information, often through digital platforms or online activities.
53. See 青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律 (Act on Development of an Environment That Provides Safe and Secure Internet Use for Young People) The House of Representatives, Japan, 2008
54. See Basic Plan on Measures for Providing Safe and Secure Internet Use for Young People, Council for Promoting Measures Against Content Harmful to Young People on the Internet and Development of an Appropriate Environment, 2009
55. See The Fourth Basic Plan on Measures for Providing Safe and Secure Internet Use for Young People, Headquarters for the Promotion of Development and Support for Children and Young People, 2018
56. See わたしたちについて (About Us) JISPA
57. Ibid.

Digital Literacy and Education Initiatives

Education is a cornerstone of Japan's strategy to promote online safety. Initiatives like **e-Net Caravan**, supported by the **Ministry of Internal Affairs and Communications and the Ministry of Education**, provide resources for students, parents, and educators on topics such as cyberbullying, internet fraud, and privacy.[58] JISPA distributes workshops, brochures, and online courses co-developed by social media companies that raise awareness and enhance digital literacy.[59] These efforts have helped to equip both youth and adults with the skills needed to recognise online risks, fostering a more informed public capable of navigating the digital world safely.

Engagement and Empowerment of Teenagers

Japan actively engages teenagers in discussions about online safety through initiatives like the **High School Student ICT Conference**, which brings students together to explore internet ethics, safety, and privacy.[60] This event empowers young people to share their perspectives on online risks and propose solutions for safer internet use.[61] By involving youth directly in shaping the conversation around digital safety, Japan fosters a sense of responsibility among teenagers, encouraging them to take ownership of their online wellbeing and contribute to creating safer online spaces for their peers.

Monitoring and Evaluation: Measuring Impact and Progress

To assess the effectiveness of its online safety initiatives, Japan has implemented tools like the **Internet Literacy Assessment Indicator for Students (ILAS)**, which measures high school students' ability to identify and manage online risks.[62] Annual assessments have shown significant improvements in students' digital literacy, particularly in recognising threats like cyberbullying and privacy breaches.[63] These evaluations provide valuable data that helps policymakers refine educational strategies and interventions, ensuring that Japan's efforts to promote online safety remain relevant and responsive to new challenges.

Conclusion

Japan's integrated and evolving strategy for online safety has become a model for addressing the complex risks faced by teenagers in the digital age. By combining robust legislative frameworks, proactive teen engagement, and innovative cross-sector collaboration, Japan has created a dynamic approach that continually adapts to emerging threats. Notably, the country's commitment to digital literacy and its comprehensive monitoring systems have played a central role in safeguarding teens online. This approach serves as a prime example of how a sustained, multi-pronged effort can have a tangible and lasting impact on the online safety of teenagers.

For Malaysia, the opportunity exists to build upon Japan's successes and adapt these strategies to its own digital ecosystem. Drawing inspiration from Japan's emphasis on legislation and cross-sector partnerships, Malaysia could forge a similarly comprehensive approach that not only addresses immediate risks but anticipates future challenges. A tailored, coordinated framework will ensure that Malaysia's teenagers are equipped to navigate the complexities of the digital world with confidence and safety.

58. See e-ネットキャラバン (e-Net Caravan) JISPA
59. Ibid
60. See 2024年 高校生ICT Conference (2024 High School ICT Conference) JISPA
61. Ibid
62. See 青少年がインターネットを安全に安心して活用するためのリテラシー指標等に係る調査 (Survey on literacy indicators for young people to use the Internet safely and with peace of mind) Ministry of Internal Affairs and Communications, 2024
63. See FY2023 ILAS (Internet Literacy Assessment indicator for Students) Ministry of Internal Affairs and Communications, 2024

Netsafe's Leadership in Protecting New Zealanders Online

In New Zealand, teenagers are among the most frequent users of digital platforms, with nearly one-third of teens spending four or more hours online daily.[64] Despite the benefits of increased connectivity, this surge in internet use has also given rise to concerns about digital risks. In 2018, seven out of ten New Zealand teens reported experiencing at least one form of unwanted digital communication, including cyberbullying, harassment, and exposure to harmful content.[65]

New Zealand has taken a proactive stance in addressing these challenges through a combination of legislation, public education, stakeholder collaboration, and innovative research. This case study explores New Zealand's approach to promoting online safety and digital wellbeing for teenagers, offering insights that could inform similar efforts in other countries, including Malaysia.

Key Stakeholders and Role of Legislation

A central part of New Zealand's approach to online safety is **Netsafe**, an independent non-profit organisation founded in 1998.[66] Netsafe provides support to individuals facing online harm, develops educational resources, and collaborates with government agencies, schools, law enforcement, and the tech industry to promote a shared responsibility for online safety.[67] Following the introduction of the **Harmful Digital Communications Act (HDCA)** in 2015, which aimed to reduce harm caused by digital communications and provide victims with a legal avenue for redress, Netsafe—as the Approved Agency under the HDCA—plays a critical role by receiving complaints, investigating incidents, and offering advice and mediation services.[68] This legal framework complements Netsafe's broader efforts, ensuring that victims have access to both legal and community-based support.

Digital Literacy and Education Initiatives

Education is a critical component of New Zealand's strategy to reduce digital risks and promote online safety among youth. Netsafe has developed a comprehensive range of digital literacy resources aimed at helping individuals and families navigate the digital world safely.[69] The organisation's website hosts a wealth of

64. See New Zealand teens' digital profile: A factsheet, Dr. Edgar Pacheco and Neil Melhuish, Netsafe, 2018
65. See New Zealand teens and digital harm: Statistical insights into experiences, impact and response, Netsafe, 2018
66. See About Netsafe, Netsafe
67. Ibid.
68. See About the Harmful Digital Communications Acts (2015) Netsafe
69. See Online safety at home, Netsafe

of educational materials tailored to different age groups.[70] These include **Netsafe's age-appropriate conversation starters**, which are designed to help parents initiate discussions with their children of various ages and also online learning modules co-developed with social media platforms that cover a wide range of topics relevant to young people, including cyberbullying, scams, online abuse, and digital privacy.[71] These interactive resources help young people identify potential risks and provide practical advice on how to stay safe while navigating the online world.

Support for Schools and Teachers

Recognising the importance of schools in shaping young people's digital habits, Netsafe offers a dedicated set of resources for educators through its **Netsafe Kete portal**.[72] This portal is designed to provide teachers with easy access to a variety of online safety tools and teaching materials, ranging from lesson plans and worksheets to online modules and interactive activities.[73] In addition, Netsafe provides schools with an interactive capability review tool based on its **Netsafe Educator Framework.**[74] This tool helps schools assess their approach to online safety across seven key areas, providing valuable insights into how they can improve their digital safety programs.[75] By regularly reviewing and updating their strategies, schools can ensure that they are creating a safe and supportive digital environment for their students.

Youth Empowerment and Engagement

In line with its commitment to youth engagement, Netsafe runs the **Youth Action Squad (YAS)**, a programme supported by funding from the **Ministry of Education**, that empowers young people to become leaders in the online safety space.[76] Through YAS, teens are encouraged to take ownership of online safety issues that directly affect them and to develop projects and resources that address these challenges.[77] In 2023, for example, members of YAS collaborated to create a toolkit for young leaders in schools across New Zealand to lead online safety initiatives in their own schools.[78] By involving youth in the creation of resources and projects, Netsafe fosters a sense of responsibility among young people and encourages them to contribute positively to the digital wellbeing of their peers.

Research, Innovation, and Data-Driven Initiatives

Netsafe is also at the forefront of research and innovation in the field of online safety. The organisation's **Netsafe Lab** uses advanced technologies such as machine learning, artificial intelligence, and data analytics to track trends and identify emerging risks in the digital landscape.[79] The lab's work focuses on developing new tools and resources to combat online harms like cyberbullying, misinformation, and scams.[80] The lab's findings are used to inform policy development and improve existing strategies for online safety in New Zealand.[81]

70. Ibid.
71. See Online safety conversation starters, Netsafe
72. See The Kete: a self-service portal for schools, Netsafe
73. Ibid.
74. Ibid.
75. Ibid.
76. See Youth Action Squad (YAS) Netsafe
77. Ibid.
78. Ibid.
79. See Netsafe Lab, Netsafe
80. Ibid.
81. Ibid.

Conclusion

New Zealand's approach to online safety is characterised by a strong emphasis on collaboration and teen empowerment, underpinned by a comprehensive framework that combines legislation, digital literacy, and cutting-edge research. The role of Netsafe, a leading organisation dedicated to online safety, exemplifies the power of dedicated non-governmental actors in driving meaningful change. New Zealand's unique focus on teen-led initiatives and community-based efforts has fostered an environment where teenagers are not just protected but actively engaged in shaping their own digital wellbeing. This holistic model highlights the importance of education, innovation, and proactive collaboration across all sectors to safeguard teenagers in the digital landscape.

For Malaysia, New Zealand's emphasis on teen-centred approaches offers valuable lessons. By prioritising digital literacy, teen participation, and multi-sector partnerships, Malaysia can build a framework that is not only effective in mitigating risks but also empowering teenagers to take ownership of their own online safety. A forward-thinking, adaptive strategy that balances education with empowerment will equip Malaysia's teenagers to thrive in an increasingly digital world.

Policy Recommendations

Ensuring the safety and wellbeing of teenagers in Malaysia on social media requires a coordinated, whole-of-society approach. As digital platforms become increasingly integral to the lives of Malaysian teens, it is essential to involve a diverse range of stakeholders in creating a safe and supportive online environment. This includes government regulators, social media platforms, parents, teachers, and teens themselves. A collaborative approach is necessary to effectively address the aggressive, sexual and commercial threats associated with social media use.

The responsibility for ensuring the safety and wellbeing of teens online is shared among several key actors:

- **Regulators:** The Malaysian government should establish and enforce clear legislation and regulations that hold social media platforms accountable for protecting teen users. These policies and rules must address issues such as data privacy, harmful content, and online harassment, and should be flexible enough to respond to the evolving digital landscape.
- **Platforms:** Social media companies operating in Malaysia must implement robust content moderation mechanisms and offer tools to support the mental health and wellbeing of teen users. Platforms should take proactive measures to prevent online harms, such as cyberbullying and exploitation, that disproportionately affect teens.
- **Users:**
    - **Teens:** It is critical to equip Malaysian teens with the necessary digital literacy skills to recognise risks, make informed decisions, and use social media responsibly. Comprehensive digital education programmes should be introduced to help teens manage their online presence and navigate potential dangers.
    - **Parents and Teachers:** Parents and teachers play a vital role in guiding teens' online activities. In Malaysia, this includes setting clear boundaries for social media use, fostering open dialogue about online experiences, and educating teens on safe internet practices. By providing support and guidance, parents and teachers can help teens engage with digital platforms in a responsible and balanced manner.
- **Civil Society:** Civil society organisations (CSOs) play a critical role in advocating for balanced social media regulations that protect online safety without undermining freedom of expression. They can monitor platform compliance with content moderation policies, ensuring they target harmful content without stifling free speech.

Thus, this section will discuss three policy recommendations—the **3Rs**—that engage all key stakeholders:

1. **Redesigning Reporting and Support Mechanisms**
2. **Reimagining Digital Literacy Education**
3. **Reapproaching Multi-Stakeholder Partnerships**

Recommendation 1: Redesigning Reporting and Support Mechanisms

To ensure that teenagers are adequately supported in online environments, it is essential for platforms, regulators, and enforcement agencies to collaborate in developing clear, accessible reporting mechanisms tailored specifically for young users. While organisations such as the MCMC, the Royal Malaysia Police (PDRM), and Bank Negara Malaysia (BNM) currently provide complaint channels,[82] these systems may not always be customised to meet the unique needs of teenagers.

Key Actions:

- **Intuitive and Accessible Reporting Interfaces**
  - Reporting mechanisms should be intuitive and non-intimidating, enabling teenagers to easily identify content that can be reported. They must also be sensitive to the emotional and developmental challenges teenagers face when encountering online harms, such as cyberbullying and scams. Additionally, platforms and regulators should offer support for content that may not meet the criteria for reporting but still causes distress, ensuring teenagers have access to guidance whenever necessary.

- **Inclusive 24/7 Helplines**
  - Given the significant amount of time teenagers spend online, platforms and regulators should provide round-the-clock support, combining both AI-driven tools and human assistance, to ensure immediate help is always available when needed. Support should be accessible in multiple languages to cater to teenagers from diverse backgrounds, ensuring that language is never a barrier to receiving help. Additionally, support tools must be designed with accessibility in mind, incorporating features such as text-to-speech functionality, screen reader compatibility, and other options suited for users with visual or hearing impairments.

- **Robust Teen Mental Health Support Systems**
  - Platforms must ensure that support teams are trained in teen mental health and trauma response, so they can provide immediate and compassionate assistance to teenagers who experience online harms. After incidents such as cyberbullying, harassment, exploitation, or falling victims to scams, teenagers should have access to crisis counselling from trained professionals, emotional support, and resources to help build resilience. These resources may include videos and interactive tools on coping strategies, mindfulness, and self-care, all tailored to teenagers.

Malaysia could benefit from adopting best practices from New Zealand's Netsafe, which provides multiple accessible reporting and support options, designed for all citizens, with particular relevance to teenagers in the context of this study. Netsafe offers a range of services,[83] including email support, a helpline, an online harm report submission system, and a text service. This approach is user-friendly and accessible, and could serve as an effective reference for Malaysia in developing reporting and support systems that are more inclusive and tailored for young users. By adopting these targeted reporting and support systems, Malaysia can provide teenagers with the necessary tools and resources to feel safe, heard, and supported online.

82. See FAQs, MCMC
83. See Helpline services, Netsafe

Recommendation 2: Reimagining Digital Literacy Education

To address the growing gap in teens' ability to navigate social media risks, digital literacy education must extend beyond schools and be integrated into the home environment as well. While initiatives like MCMC's Klik Dengan Bijak (Click Wisely)[84] have made valuable progress in raising public awareness about internet safety, it is crucial that families, educators, and teens themselves all take an active role in fostering digital literacy.

Key Actions:

- **Strengthening and Monitoring Digital Literacy in Schools**
  - Digital literacy education in schools should focus on depth rather than breadth. Instead of attempting to cover a wide range of topics superficially, programmes should delve deeper into key areas such as recognising online risks, understanding digital footprints,[85] and navigating online privacy settings. To ensure the effectiveness of these programmes, schools should regularly assess students' digital literacy through surveys or evaluations, helping to identify knowledge gaps and enabling educators to tailor the curriculum to address specific areas of concern.

- **Tailored Parent and Caregiver Resources**
  - Adults should be provided with resources on online risks, healthy online behaviour, and communication strategies to create a supportive home environment where teenagers feel encouraged to share any harmful online experiences. These resources could include tips on how to have open, non-judgemental conversations about online activities, ensuring that parents feel equipped to discuss sensitive issues. The resources should be age-appropriate, easily accessible to all, regardless of socioeconomic background, and available in multiple languages to meet the diverse needs of families.

- **Engaging and Empowering Teens**
  - Schools could facilitate student-led activities focused on online harms and digital wellbeing, allowing teenagers to share their experiences and concerns in a peer-driven setting. Peer-led support networks could also be established, providing a safe space for students to discuss challenges and offer advice to one another. Additionally, selecting online safety ambassadors from the student body could further promote responsible digital behaviour, as peers are often more likely to listen to and learn from one another, thereby fostering a culture of safety and awareness within the school.

Learning from Japan, Malaysia could explore various resources specifically curated for parents, educators, schools, and children of different age groups to ensure everyone is aware of their role in protecting young users online, such as こどもとネットのトリセツ (Kids and the Internet Manual)[86], developed by JISPA, which offers tips for parental control in a creative and engaging way. This approach could foster a more collaborative and comprehensive effort towards digital literacy, helping to create a safer and more supportive online environment for teens both at home and in schools.

84. See Malaysia's online safety initiative, Klik Dengan Bijak (Click Wisely)
85. The trail of data an individual leaves behind while using the internet, including information shared on social media, websites visited, and online activities, which can be traced and potentially used to track or identify them.
86. See こどもとネットのトリセツ (Kids and the Internet Manual) JISPA

Recommendation 3: Reapproaching Multi-Stakeholder Partnerships

Recognising the complex and evolving nature of online harms, a unified, multi-stakeholder approach is essential for effective mitigation. Establishing a dedicated autonomous non-profit organisation, with the authority to convene diverse stakeholders, to lead initiatives on online safety and digital wellbeing for Malaysians of all ages could help consolidate efforts currently dispersed across multiple ministries and agencies. This would enhance coherence, resource allocation, and improved coordination.

Key Actions:

- **Establish Multi-Stakeholder Collaboration Networks:**
  - The organisation will establish formal networks for collaboration among key stakeholders—including regulators, platforms, users, and civil society— to share knowledge, resources, and best practices on online safety. It will bring together CSOs (including human rights advocates and digital rights groups) to ensure that safety measures respect freedom of expression. Regular forums, working groups, and consultations will foster open dialogue on balancing content moderation with individual rights, helping to guide future policy design and implementation.

- **Lead Public Awareness Campaigns and Digital Literacy Campaigns:**
  - The organisation will lead nationwide campaigns to raise awareness about online safety, digital wellbeing, and responsible online behaviour, with tailored content for children, parents, educators, and older adults. It will also provide training and resources for schools, teachers, and parents to equip them with the tools needed to support online safety among students and children. Partnerships with technology companies and platforms will further promote the development of toolkits and modules that are practical and applicable to real-life scenarios.

- **Conduct Research and Gather Community Feedback:**
  - The organisation will establish a research function to collect data on the prevalence and impact of online harms in Malaysia. A system for gathering public feedback on online safety issues will enable the organisation to stay responsive to emerging threats and adapt initiatives based on real-world experiences. Surveys, online forums, and consultations will help assess whether the various initiatives and activities remain relevant to the needs of the community.

Both New Zealand and Japan offer relevant examples for establishing this new organisation. New Zealand's Netsafe operates independently alongside government agencies and law enforcement, focusing on online safety by providing free support, guidance, and educational resources.[87] Similarly, the Japan Internet Safety Promotion Association (JISPA) serves as a platform for dialogue among users, industry stakeholders, and educators, fostering the exchange of information, the adoption of best practices, and the creation of collaborative initiatives to promote a safer online environment.[88] Adopting these approaches in Malaysia will enhance cross-sector collaboration and streamline efforts to safeguard the online wellbeing of all Malaysians.

87. See About Netsafe, Netsafe
88. See わたしたちについて (About Us) JISPA

Conclusion

This study highlights the significant online presence of teenagers in Malaysia, with social media playing an important role in their daily lives. However, this widespread usage exposes teens to various risks, such as cyberbullying and scams, with many reporting feelings of insecurity. While there is some basic awareness of essential safety practices, such as managing privacy settings and understanding the permanence of online content, many teenagers remain inadequately equipped to navigate these risks. Additionally, parents and teachers lack the necessary tools and knowledge to support safe online behaviour, and the collaboration between platforms and the government remains insufficient.

The findings suggest that ensuring the online safety and well-being of teenagers requires a collaborative approach. Parents, teachers, social media platforms, and the government must all play active roles. Social media platforms have introduced safety features and content moderation tools, but these must be continuously monitored and updated to address emerging risks. In addition, ongoing collaboration between platforms, parents, and teachers is crucial to ensure that teenagers are fully equipped to navigate online spaces safely. The government can further support these efforts by promoting policies that foster safe online practices and accountability for platforms.

To address these challenges, immediate action is needed based on the study's recommendations structured around the 3Rs: 1) Redesigning Reporting and Support Mechanisms, 2) Reimagining Digital Literacy Education and 3) Reapproaching Multi-Stakeholder Partnerships. By taking these steps, Malaysia can ensure that teenagers not only connect, learn, and thrive, but are also empowered to face any dangers with confidence and courage.

References

Bernama. (2024, October 16). Online Safety Bill to mandate three key responsibilities for platform providers. NST Online. *https://www.nst.com.my/news/nation/2024/10/1120502/online-safety-bill-mandate-three-key-responsibilities-platform-providers#:~:text=KUALA%20LUMPUR%3A%20The%20Online%20Safety,restricting%20access%20to%20harmful%20content.*

Content Forum. (n.d.). Brief Overview of the Content Forum. *https://contentforum.my/about-us/*

Council for Promoting Measures Against Content Harmful to Young People on the Internet and Development of an Appropriate Environment. (2009). Basic Plan on Measures for Providing Safe and Secure Internet Use for Young People. *https://www.cfa.go.jp/assets/contents/node/basic_page/field_ref_resources/04628de7-d704-4ed2-ae11-7dfa859ded0e/3f592722/20230401_policies_youth_kankyou_internet_torikumi_guideline_p1_detail_en.pdf*

Department of Statistics Malaysia. (2023). ICT Use and Access by Individuals and Households Survey Report. *https://newss.statistics.gov.my/newss-portalx/ep/epDownloadContentSearch.seam?contentId=190841&actionMethod=ep%2FepDownloadContentSearch.xhtml%3AcontentAction.doDisplayContent&cid=46445*

ECPAT, INTERPOL, & UNICEF. (2022). Disrupting Harm in Malaysia: Evidence on Online Child Sexual Exploitation and Abuse. *https://www.unicef.org/malaysia/media/3291/file/Disrupting%20Harm%20Malaysia%20Full%20Report%20(English).pdf*

Headquarters for the Promotion of Development and Support for Children and Young People. (2018). The Fourth Basic Plan on Measures for Providing Safe and Secure Internet Use for Young People. *https://www.cfa.go.jp/assets/contents/node/basic_page/field_ref_resources/04628de7-d704-4ed2-ae11-7dfa859ded0e/207659d9/20230401_policies_youth_kankyou_internet_torikumi_guideline_p4_detail_en.pdf*

Institute for Public Health (IPH). (2022). Technical Report National Health and Morbidity Survey (NHMS) 2022: Adolescent Health Survey. *https://iku.gov.my/images/nhms-2022/Report_Malaysia_nhms_ahs_2022.pdf*

Ipsos. (2024). Education Monitor. *https://www.ipsos.com/sites/default/files/ct/news/documents/2024-09/Education_Monitor_2024_0.pdf*

Japan Internet Safety Promotion Association. (n.d.-a). 2024年 高校生ICT Conference (2024 High School ICT Conference). *https://www.good-net.jp/ict-conference/2024/*

Japan Internet Safety Promotion Association. (n.d.-b). e-ネットキャラバン (e-Net Caravan). *https://www.good-net.jp/lectures/demae_contents/content9_category_201/2013_275-1100_999*

Japan Internet Safety Promotion Association. (n.d.-c). こどもとネットのトリセツ (Kids and the Internet Manual). *https://www.kodomo-safety.org/*

Japan Internet Safety Promotion Association. (n.d.-d). わたしたちについて (About Us). *https://www.good-net.jp/anshinkyo/*

Klik Dengan Bijak (Click Wisely). (n.d.). Malaysia's online safety initiative. *https://klikdenganbijak.my/en/about.php*

KYODO NEWS. (2024, April 14). Japanese youth spend around 5 hours a day online: government survey. Kyodo News+. *https://english.kyodonews.net/news/2024/04/1d6b44221a69-japanese-youth-spend-around-5-hrs-a-day-online-govt-survey.html#:~:text=Japanese%20youth%20spend%20around%205%20hours%20a%20day%20online%3A%20government%20survey,-KYODO%20NEWS%20%2D%20Apr&text=Japanese%20youth%20spend%20on%20average,to%20a%20recent%20government%20survey.*

Livingstone, S., Mascheroni, G., Dreier, M., Chaudron, S., & Lagae, K. (2015). How parents of young children manage digital devices at home: the role of income, education and parental style (pp. 1–25). EU Kids Online, LSE. *https://eprints.lse.ac.uk/63378/1/__lse.ac.uk_storage_LIBRARY_Secondary_libfile_shared_repository_Content_EU%20Kids%20Online_EU_Kids_Online_How%20parents%20manage%20digital%20devices_2016.pdf*

Malaysian Communications and Multimedia Commission. (n.d.-a). FAQs. *https://mcmc.gov.my/en/faqs/online-content-problems/what-are-the-steps-required-for-me-to-lodge-compla*

Malaysian Communications and Multimedia Commission. (n.d.-b). History. *https://www.mcmc.gov.my/en/about-us/history*

Malaysian Communications and Multimedia Commission. (n.d.-c). Our Responsibility. *https://www.mcmc.gov.my/en/about-us/our-responsibility*

Malaysian Communications and Multimedia Commission. (2021). Hand Phone Users Survey 2021. *https://mcmc.gov.my/skmmgovmy/media/General/pdf2/FULL-REPORT-HPUS-2021.pdf*

Malaysian Communications and Multimedia Commission. (2022). Internet Users Survey 2022. *https://mcmc.gov.my/skmmgovmy/media/General/IUS-2022.pdf*

Malaysian Communications and Multimedia Commission. (2024a, August). MCMC Introduces Regulatory Framework for Internet Messaging and Social Media Service Providers [Press release]. *https://mcmc.gov.my/skmmgovmy/media/General/pdf2/MS_REGULATORY-FRAMEWORK-FOR-SOCIAL-MEDIA-AND-INTERNET-MESSAGING-SERVICE-PROVIDERS-IN-MALAYSIA.pdf*

Malaysian Communications and Multimedia Commission. (2024b, October). MCMC Seeks Public Input on Draft Code of Conduct (Best Practice) for Safer Online Environment in Malaysia [Press release]. *https://mcmc.gov.my/skmmgovmy/media/General/PressRelease/MS_-Public_Consultation_on_the_draft_Code_of_Conduct_-Best-Practice-MCMC.pdf*

Malaysian Communications and Multimedia Commission & UNICEF Malaysia. (n.d.). Child *safety online: global strategies and challenges [Slide show].*

Ministry of Internal Affairs and Communications. (n.d.-b). 青少年がインターネットを安全に安心して活用するためのリテラシー指標等に係る調査 (Survey on literacy indicators for young people to use the Internet safely and with peace of mind). *https://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000408.html*

Netsafe. (2018). New Zealand teens and digital harm: Statistical insights into experiences, impact and response. *https://www.women.govt.nz/sites/default/files/2021-08/NZ-teens-and-digital-harm_statistical-insights_2018%20%281%29.pdf*

Netsafe. (2024a). About Netsafe. *https://netsafe.org.nz/netsafe*

Netsafe. (2024b). About the Harmful Digital Communications Act (2015). *https://netsafe.org.nz/our-work/helpline-services/the-harmful-digital-communications-act*

Netsafe. (2024c). Helpline Services. *https://netsafe.org.nz/our-work/helpline-services*

Netsafe. (2024d). Netsafe Lab. *https://netsafe.org.nz/our-work/netsafe-lab*

Netsafe. (2024e). Online safety at home. *https://netsafe.org.nz/online-safety-at-home*

Netsafe. (2024f). Online safety conversation starters. *https://netsafe.org.nz/parents-and-caregivers/conversation-starters*

Netsafe. (2024g). The Kete: a self-service portal for schools. *https://netsafe.org.nz/our-work/education#explore-the-kete*

Netsafe. (2024h). Youth Action Squad (YAS). *https://netsafe.org.nz/our-work/youth-action-squad*

Pacheco, E., & Melhuish, N. (2018). New Zealand teens' digital profile: A factsheet. *https://ndhadeliver.natlib.govt.nz/delivery/DeliveryManagerServlet?dps_pid=IE32634724*

Ramendran, C., & Tong, G. (2024, July 7). New rules mulled after activist's death. The Star *https://www.thestar.com.my/news/nation/2024/07/07/new-rules-mulled-after-activists-death*

Tan, B. (2024, September 6). TikToker 'Abang Bas' arrested for filming schoolgirls, even calling some of them his "crush." Malay Mail. *https://www.malaymail.com/news/malaysia/2024/09/06/tiktok-abang-bas-arrested-for-filming-schoolgirls-even-calling-some-of-them-his-crush/149455*

Tee, K. (2024, September 23). A look at Xiaohongshu, China's answer to Instagram that has Chinese Malaysians glued to their phones (VIDEO). Malay Mail. *https://www.malaymail.com/news/malaysia/2024/09/24/a-look-at-xiaohongshu-chinas-answer-to-instagram-that-has-chinese-malaysians-glued-to-their-phones-video/151238*

The House of Representatives, Japan. (2008). 青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律 (Act on Development of an Environment That Provides Safe and Secure Internet Use for Young People). *https://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/kaiji169_l.htm*

Appendices

Appendix A - Research Methodology

Overview of Research Design:

This study employed a mixed-methods approach, combining both quantitative and qualitative research methods to gain comprehensive insights into the online safety and digital well-being of Malaysian teenagers.

Quantitative Data:

- Survey Instrument: A structured bilingual (English and Malay) small-scale survey was developed, with a total of 185 responses collected through platforms such as schools and social media. Please note that the findings are not representative of the broader population due to the limited sample size.
- Purpose: To gather data on teenagers' online behaviours, experiences, and attitudes towards online safety and digital wellbeing.
- Sampling Method: Convenience sampling, with participants from the age group 13-17.
- Data Analysis: Descriptive statistics were used to identify key trends and patterns in the responses.

Demographics of Survey Respondents:

Figure A1:
Age Distribution

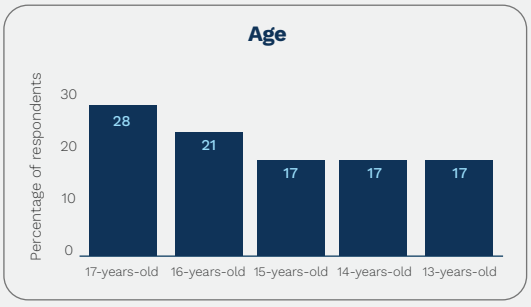


Figure A2:
Gender Distribution

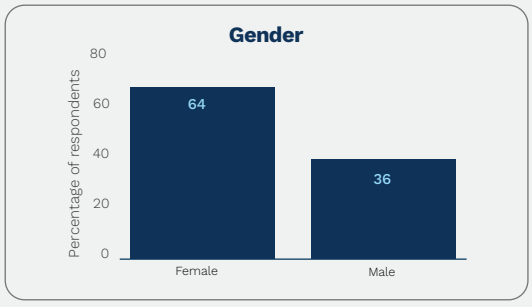


Figure A3:
Highest Education Level of Parents/Guardians

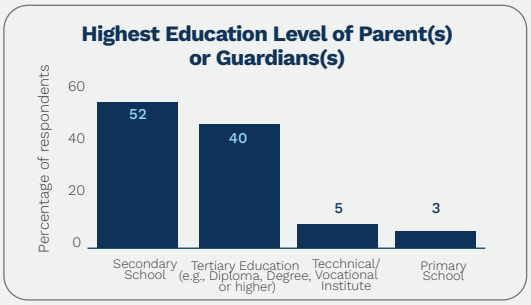


Figure A4:
Family Income Distribution

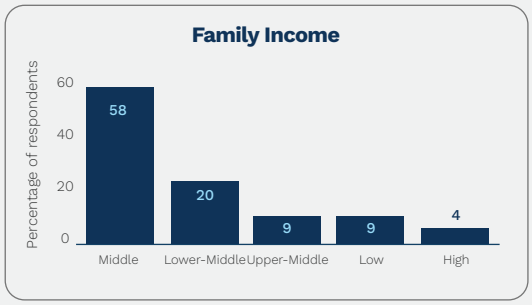


Figure A5:
Availability of Personal Devices at Home

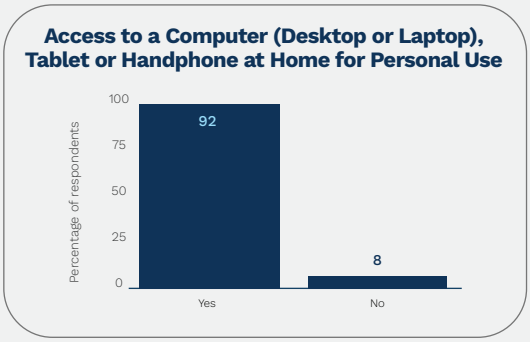
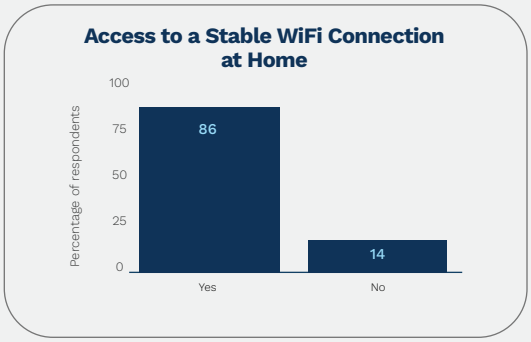


Figure A6:
Access to Stable WiFi Connection at Home



Source: SERI Malaysia (Author's Findings from Survey, 2024)

Qualitative Data:

- **One Focus Group Discussion (FGD):**
  - Sampling Method: Purposive sampling was used to select key stakeholders, including two parents, one secondary school teacher, a representative from an educational NGO, and a representative from a social media platform. This approach aimed to gather insights into teenagers' social media usage, digital mediation practices, and the awareness and effectiveness of current platform safety measures and regulations.
  - Data Analysis: Thematic analysis was used, with discussions transcribed and coded to identify recurring themes and perspectives.
- **Five Semi-Structured Interviews:**
  - Sampling Method: Voluntary sampling was used to select teens who expressed interest in follow-up interviews after completing the survey.
  - Data Analysis: Narrative analysis was used, focusing on the personal anecdotes shared by the teens.

Two Case Studies:

Sampling Method: Convenience sampling was used to select relevant case study subjects based on their relevance to Malaysia and the availability of information.

Data Analysis: Comparative analysis was used, highlighting international best practices and how they could inform Malaysia's current digital safety and well-being measures for teens.

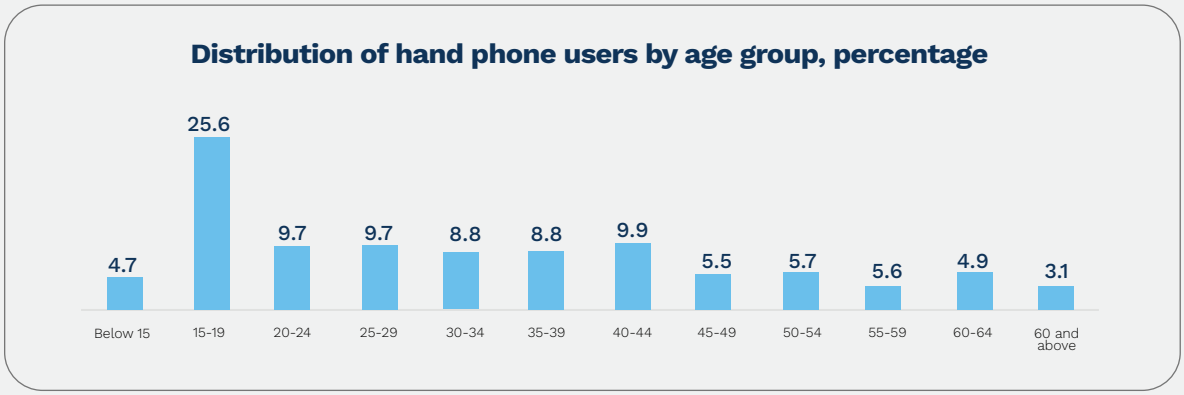
- **Ethical Considerations:**
  - Verbal Consent: All participants, including teenagers, parents, and professionals, were given an explanation of the study's purpose, nature of participation, and their rights before agreeing to take part.
  - Confidentiality: Participants were assured that all personal data collected, including survey responses, interview and discussion transcripts, would be kept confidential and used solely for research purposes.
  - Right to Withdraw: Participants were informed that they had the right to withdraw from the study at any stage without any consequence. They were also given the option to skip any questions they felt uncomfortable with.
  - Participant Welfare: Every effort was made to ensure the welfare and safety of participants during the study. Sensitive topics were approached with care to avoid distress.

Note:

The following materials are available upon request:
- Survey Instrument
- Interview Protocol and FGD Guide
- Case Study Protocol

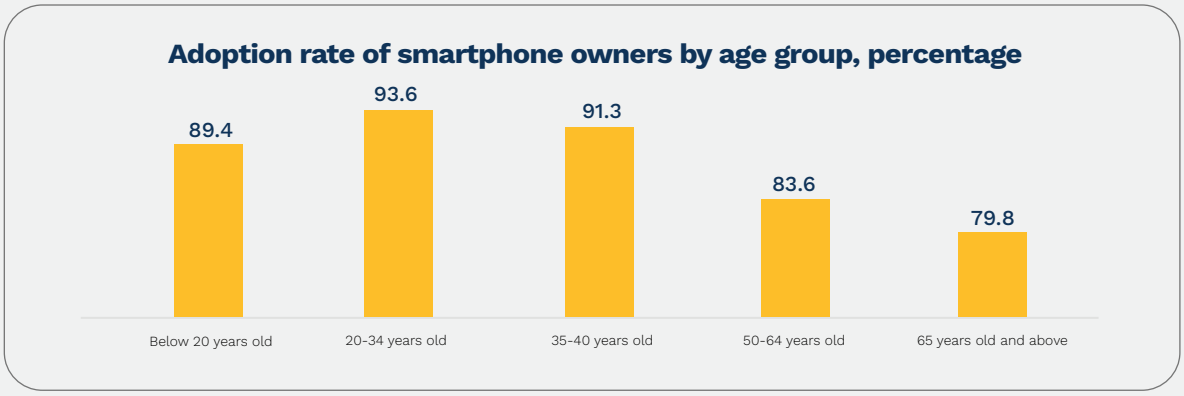
Appendix B - Additional Figures and Tables

Figure A7:
Late Malaysian teenagers are the highest number of hand phone users.



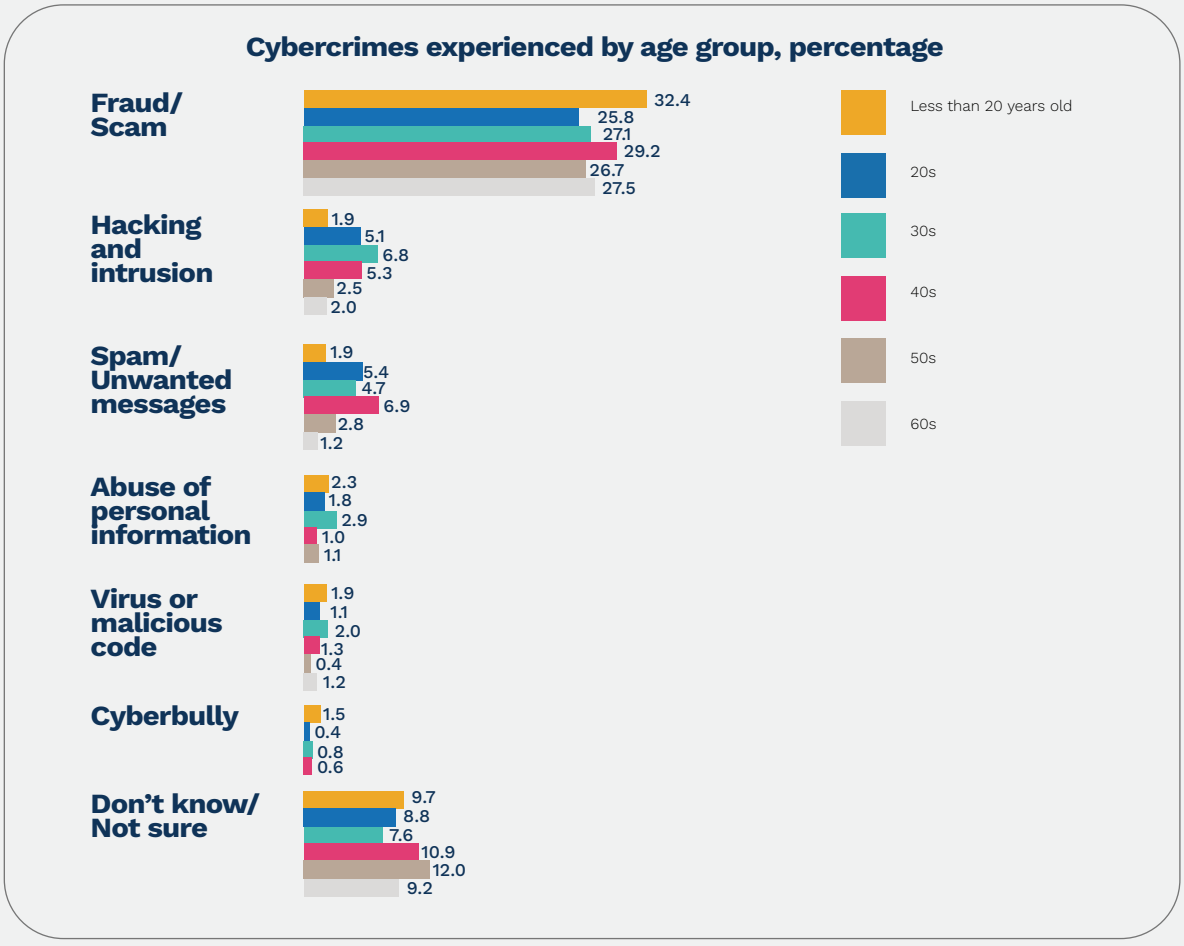
Source: Hand Phone Users Survey 2021, Malaysian Communications and Multimedia Commission (MCMC)

Figure A8:
Smartphone ownership is highest among young Malaysians.



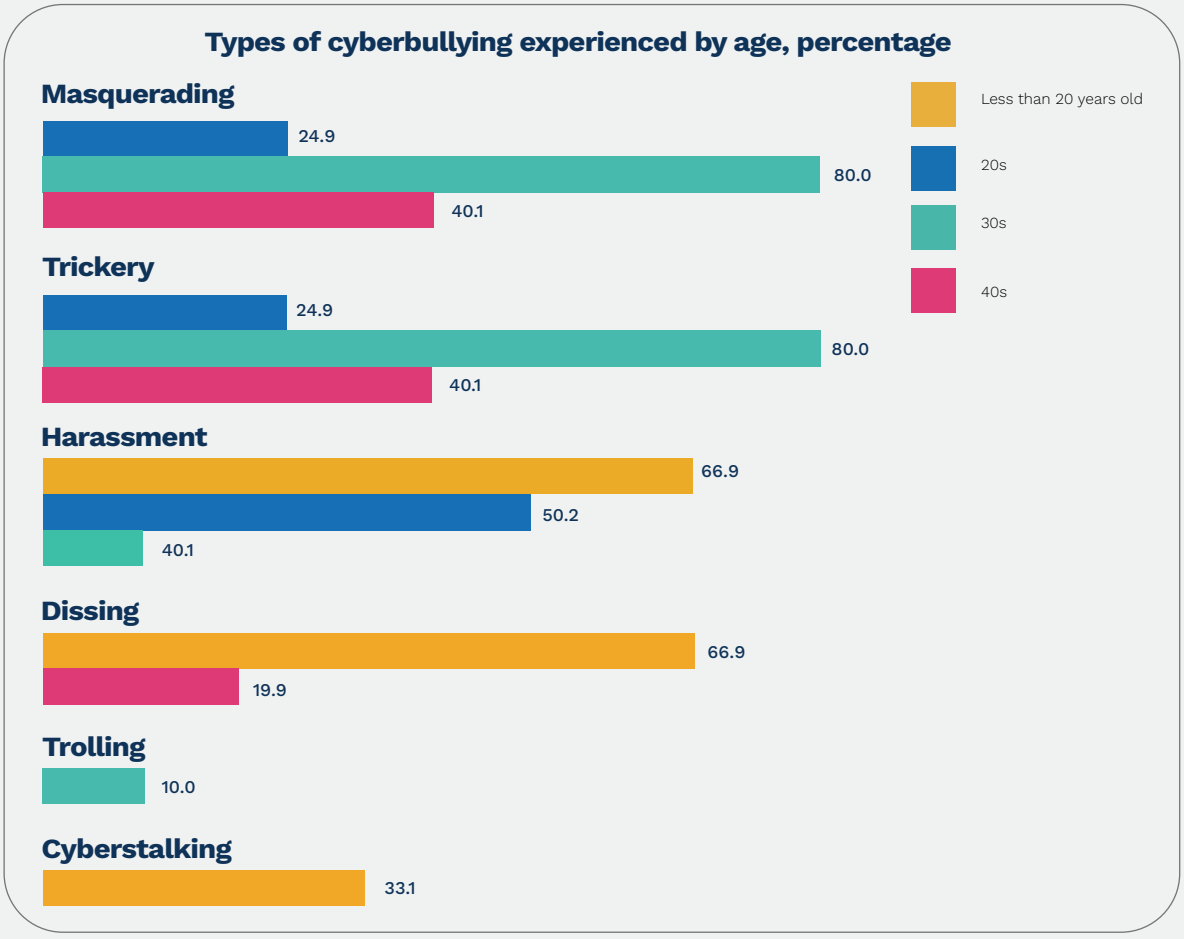
Source: Hand Phone Users Survey 2021, Malaysian Communications and Multimedia Commission (MCMC)

Figure A9:
Malaysians under the age of 20 experienced the highest occurrence of fraud/scams.



Source: Internet User Survey 2022, Malaysian Communications and Multimedia Commission (MCMC)

Figure A10:
Malaysian youth are more prone to experience cyberbullying.



Source: Internet User Survey 2022, Malaysian Communications and Multimedia Commission (MCMC)

Figure A11:
Cyber crime awareness is lowest among Malaysian teenagers compared to other age groups.

Individuals using the Internet by age group and type of activity, percentage

Safety, Online Protection and Awareness

Age Group	Verifying the reliability of information found online	Setting up effective measure to protect devices and online accounts	Changing privacy settings on your devices, accounts or app	Cyber crime awareness
Total	**29.0**	**79.6**	**78.3**	**65.7**
15-19	24.9	64.5	76.7	50.6
20-24	32.6	91.2	85.7	67.0
25-29	40.8	90.3	89.5	65.2
30-34	44.1	87.1	87.5	69.0
35-39	30.5	88.1	88.3	69.9
40-44	27.4	87.1	86.8	75.4
45-49	25.3	85.7	82.5	75.3
50-54	25.8	80.3	77.2	70.5
55-59	23.1	70.3	68.9	63.5
60+	9.6	49.8	37.5	55.2

Source: ICT Use and Access by Individuals and Households Survey Report, Malaysia, 2023, Departmentof Statistics Malaysia (DOSM)

Appendix C - Limitations of the Study

01. **Sampling Limitations:** The study focused on teenagers aged 13 to 17, but the sample may not fully represent the broader demographic of Malaysian teens, especially in terms of socio-economic background, geographic location, and digital access. Notably, Orang Asli, Orang Asal, refugees, and other non-Malaysian teenagers living in Malaysia were not included. These groups are likely to be more vulnerable to online threats due to their minority status and marginalisation, potentially exposing them to higher risks. Future studies should prioritise these populations to ensure that policies are inclusive and effective across all demographic groups.

02. **Self-Reporting Bias:** Reliance on self-reported data—through surveys, interviews, and focus groups—could introduce bias. Participants may have underreported or overstated their experiences due to fear of judgement or social desirability. Teenagers, in particular, may hesitate to disclose sensitive information about online threats, such as cyberbullying or grooming. This limitation highlights the need for more robust, anonymised data collection methods to improve the accuracy and reliability of future research, especially when informing policy decisions.

03. **Limitations of Case Study Selection:** The international case studies included in this study may not fully reflect Malaysia's unique cultural, legal, or social context. While these cases offer valuable insights, their direct applicability to Malaysia is limited. Policymakers should recognise that best practices from other countries may need adaptation to fit local regulatory and societal conditions.

04. **Scope of Platforms Studied:** The study focused on several widely-used platforms, including WhatsApp, Telegram, Instagram, Facebook, TikTok, X (formerly Twitter), and Discord. However, many participants reported using platforms not initially included in the study, such as Xiaohongshu (Little Red Book), a popular platform among some teens. This highlights the need for policy frameworks that can accommodate emerging platforms and evolving digital trends, ensuring that all platforms are considered in digital safety measures.

05. **Generalisation of Online Threat Types:** While the study concentrated on three main categories of online threats—aggressive, sexual, and commercial—other threat types, such as value threats (e.g., ideological extremism or political manipulation), were not included. These threats are difficult to measure and quantify but are becoming increasingly significant. Future research should explore these emerging threats to provide a more comprehensive understanding of online risks for teenagers, allowing policymakers to address a broader range of safety concerns.

06. **Time Constraints and Changing Digital Landscape:** Given the rapid evolution of digital threats and online platforms, the findings of this study may quickly become outdated. The study was conducted within a specific timeframe and does not account for future changes in the digital landscape. Policymakers should consider the dynamic nature of online threats and ensure that policies are adaptable to emerging risks and trends.

07. **Absence of Longitudinal Data:** The study did not include longitudinal data, which limits the ability to track changes over time in teenagers' experiences with online threats or the effectiveness of interventions. Long-term studies would offer valuable insights into how online safety challenges evolve and provide evidence of the lasting impact of policy measures. Policymakers should consider the importance of ongoing research to assess the effectiveness of interventions and refine policies accordingly.

SERI SOCIAL & ECONOMIC RESEARCH INITIATIVE

Social and Economic Research Initiative (SERI) is a non-partisan think-tank dedicated to the promotion of evidence-based policies that address issues of inequality. Visit **www.seri.my** or email **hello@seri.my** for more information.

ooooo

: Social & Economic Research Initiative : Social & Economic Research Initiative (SERI)

: seri.my : hello@seri.my : @SERI_Malaysia