A Framework for Protecting Teenagers from Cyber Crimes and Cyberbullying

Sultan Saud Alanazi[1], Adwan Alownie Alanazi[2]
College of Computer Science and Engineering
University of Ha'il, Ha'il
Saudi Arabia

Abstract—**Social applications consist of powerful tools that allow people to connect and interact with each other. However, its negative use cannot be ignored. Cyberbullying is a new and serious Internet problem. Cyberbullying is one of the most common risks for teenagers to go online. More than half of young people report that they do not tell their parents when this will occur, this can have significant physiological consequences. Cyberbullying involves the deliberate use of digital media on the Internet to convey false or embarrassing information about others. Therefore, this article provides a way to detect cyber-bullying in social media applications for parents. The purpose of our work is to develop an architectural model for identifying and measuring the state of Cyberbullying faced by children on social media applications. For parents, this will be a good tool for monitoring their children without invading their privacy. Finally, some interesting open-ended questions were raised, suggesting promising ideas for starting new research in this new field.**

Keywords—*Cyberbullying; cyber bullying; internet crimes; social media security; e-crimes*

I. INTRODUCTION

Due to increased use of social media and trending social applications, children are involving in different internet-based activities. The ratio of increase in the use of social media is shown in Fig. 1. On one side it is proving to be an informative and interactive medium for indolence's but on the other side it has a lot of emerging issues as well. One of the biggest concerns is towards the increasing cyberbullying cases day by day. As the technologies are increasing day by day and many of the parents are not well aware about it, more children are curious towards using internet-based facilities which led them to cyberbullying victimization [1][2]. Cyberbullying effects individual's life mentally and physically. Some cases of cyberbullying lead to death as well. So, the motivation of this article is to educate parents to monitor their children online activates, make them aware of such increasing cyberbullying crime and to provide their children an E- safe environment [1].

In recent years, the continuous development of technology has made it possible to keep in touch with friends and family around the world anytime, anywhere, making many conveniences and ease of life. With its increasing use we must focus on its uses to help us in our daily lives. As human is a social animal, we need to build a social network to survive [3][4]. In this modern era, social networking is most important. As a result, social networking sites are now widely used for a variety of purposes, including entertainment and networking. All social media platforms require the consent of all participants forming a network to communicate [4].

Benefits of this include the ability to acquire, deploy, maintain, and enhance the software used by consumers quickly and effectively. As a result, the number of new applications for platforms such as Mac, Android and iPhone have increased, and this model has been adopted to provide consumers with a variety of modern, low-cost applications. However, this paradigm shift has created a series of new security challenges [6].

As the market for new applications grows rapidly, so do the security threats with this software provisioning model. In the Android market, there are many reports of applications infected with malware and spyware [6].

As the use of cell phones increases, so does the misuse of information. Organized criminal groups may use services such as the WhatsApp mobile messaging application to engage in illegal activity, and the encryption technology used in these applications [7] is helping to cover the traces of this behaviour and make it undetectable to trace [8]. The growth of digital technology is mainly focused on the virtual life of individuals (mainly adolescents (11-19 years)) [9]. Internet users have a great opportunity to exchange ideas, interact and engage with people by developing a virtual community [1][2][10]. Often these interactions lead to passive use rather than active use. Cyberbullying is one of the most dangerous incidents in social media applications like WhatsApp and Facebook, and individuals (especially teens) are victims of cyberbullying [11]. Cyber security is a major concern of all security companies around the globe.
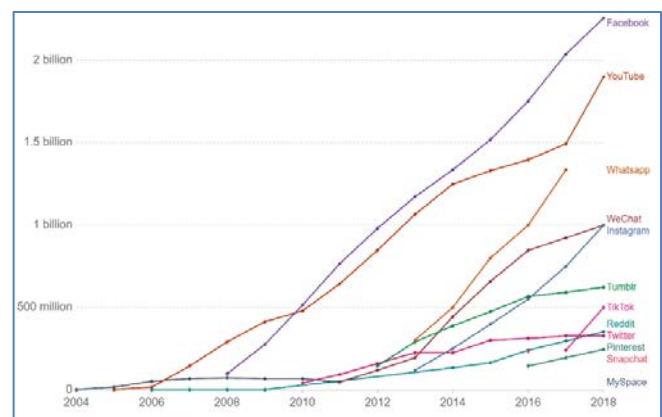

Fig. 1. Number of People using Social Media Platforms, 2004 to 2018 [5].

II. CYBERBULLYING

In recent years, many studies have been proposed to make the Internet a safer place to work. Security threats are on the rise, most notably cyber bullying and online grooming. Cyberbullying is a way to bully someone online. This can be done by maliciously posting or posting bad content online. This situation is disastrous for social media users, especially teenagers [11]. There have been many reported cases of cyberbullying as a cause of adolescent suicide. Online platforms like Facebook and WhatsApp are most commonly used by teens for all types of relationships as shown in Fig. 2. This social networking portal attracts more cybercriminals and engages in more illegal activities. As you know, billions of people around the world use it for many purposes [9][11].

On the other hand, online grooming presents you as dislike and uses victims to achieve their goals, usually through sexual activity [11]. As an open access platform, cyber-groomers also have access to the same internet platforms that are used by young people. Cyber bullying can take many forms, including posting harmful or threatening content on the Internet, spreading rumours, taking, and posting disgusting photos of someone without permission, posting pornographic images and information, and much more as shown in Fig. 3. Many teens suffer from cyber bullying and many of them engage in cyber bullying. More than a third of teens fell victim to cyberbullying, and they didn't even tell their parents about cyberbullying [11][12].
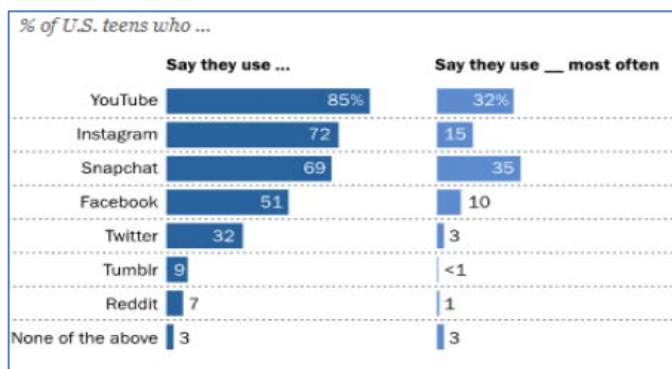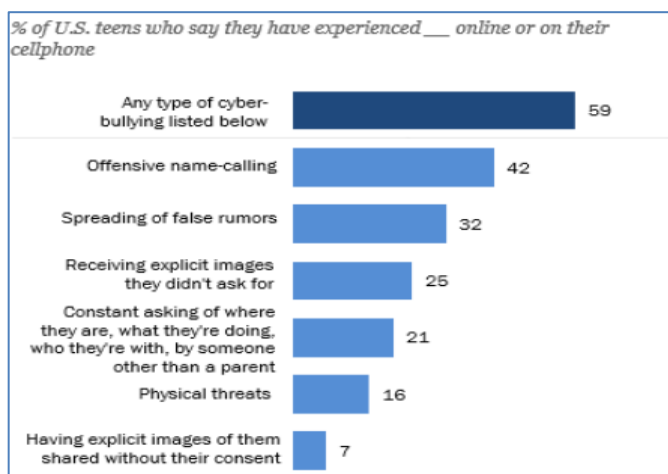

Fig. 2. Use of Social Media by Teens [9].

Fig. 3. Some Form of Cyberbullying [11].

The consequences of cyberbullying include anxiety, depression, and even suicide. Cyberbullying is primarily aimed at young people [11][13]. Cyberbullying begins when the victim begins to react to the harmful messages [13][14]. Internet use has been found to be a reliable predictor of victims experiencing cyberbullying. For men, Internet use is also an indicator of online cyberbullying [13][14].

III. DEADLY CHALLENGES

Now a day's cyberbullying is of great concern especially for teenagers. Parents need to check their children for such incidents which could reportedly took lives. Increasing social media use and growing apps have led to high level of curiosity among teenagers [13]. Due to this, teenagers try different games or interactive applications which led them to cyberbully victimization. One of these applications is the famous Blue Whale game. It is also known as Blue Whale Online Challenge, is a life-threatening online game that is believed to have killed hundreds of teenagers [15][16]. This online game is a great challenge for teenagers on various internet portals. Our dependence on technology is increasing. When curiosity leads teenage boys to online games, it can explain the Cyberbullying victimization very well. The boy faces a challenge online. He called the blue whale and agreed [15]. He gets a job, and he must do it. But is this task really important or problematic? These missions forced him to leak personal information used by criminals and began to threaten. The accident had a psychological impact on the victims, and sometimes even led to suicide. The game administrator has strict control over who can play or download. After research and analysis of the victims, they decide whom to grasp and who can be a very suitable and easy victim [15][16].

Social media cyberbullying can lead to suicides [17]. Another new WhatsApp group, MOMO CHALLENGE, was discovered by the popular YouTuber ReignBot in July 2018, and it has caught the attention of the public. After a few days, someone might accept the Peach Challenge. Momo information has been sent to countries such as Mexico, India, Argentina, the United States, France and Germany. In early August, WhatsApp Momo game reportedly killed two people, Manish Sarki (18) on August 20 and Aditi Goyal (age 26) in Kursong in Darjeeling the next day [18]. Police suspect they may have taken action because they are playing this suicide game.

After messaging a man named Momo on WhatsApp, a 12-year-old girl was found dead in a backyard near Buenos Aires, Argentina. "After searching for videos and chats on WhatsApp via a phone hack, they are now looking for a teenager who allegedly exchanged these messages with," police told the news portal [19]. Police believe the teenager's intention was to "upload the video to social media as part of a challenge, crediting the Momo game" for the suicide [19]. One of the challenges in this game is that people have to communicate with unknown numbers.

IV. MONITORING THE CHILD

With the growing technology parents are falling behind to cope up and understand the security threats of using internet. This is due to a lack of time and inadequate knowledge of

computers usage, social networking and rapid growing mobile apps they are unable to inspect what their children are doing when they are using internet. Parents are unaware or do not fully understand the evolution of bullying. Thus, it is necessary for parents of modern era to monitor their child.

Parents cannot control all of their children's behaviours, but there are steps they can take to prevent cyberbullying and protect their children from harm [20]:

- Track and monitor teenagers' social media, apps, and browsing history. Cyberbullying is usually occurring when parents notice negative changes in adolescent behaviour.

- View or reset the privacy settings and phone location (GPS) of your child.

- Follow your child on social media, and try to be in his friends list, or ask a trusted adult to do the same.

- Parents should pay attention and to be aware of the latest applications, social media platforms and digital languages used by teenagers.

- Know your child's social media email address, username, and password.

- Establish rules for good behaviour, digital content and applications.

- Limit internet use accordingly.

Following (Fig. 4) is a depiction of different stages to cyberbullying victimization.

Parents can use different available parental control tools and techniques that can help to build a non-invasive approach towards their teenage children and thus prevents them from cyberbullying, malicious behaviour on the internet, and inappropriate content. Free monitoring software and apps are available that can be used to help parents restrict inappropriate and unwanted content, block specific domains, and view children's online activities (including social media activities) without having to physically check their children's devices daily. In fact, it is also less invasive and sometimes invisible to children [21][22][23].
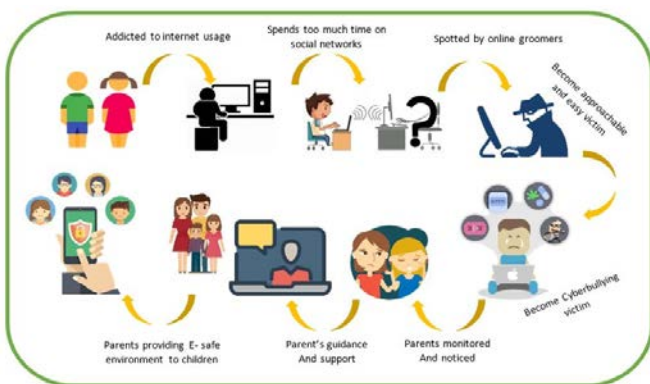

Fig. 4. Stages to Cyberbullying Victimization [13].

When choosing the right internet application for a child, parents should consider their children's ages, device usage, and digital network behaviour, which may help. Parents should build trust relationships with their children by engaging in open and honest discussions. These conversations provide an opportunity to exchange values and expectations regarding digital family-friendly behaviours, such as viewing and sharing content, and available and unavailable applications. Ask your child about their online experiences to avoid potential risks of cyberbullying and abuse. Make it clear to them that your goal is to protect them and that you want to have an open conversation with them. Discuss their concerns, opinions and also manifest your opinion [21][22][23].

V. CYBERBULLYING DETECTION FRAMEWORK

In this section, the proposed cyberbullying detection architecture is presented. The proposed architecture includes five different modules, which not only detects the bulling content on the social application but also helps in the detection of mobile security level used by the child. As the use of mobile phones is growing tremendously, various mobile phone applications are also emerging. Different Social media applications are emerging through which youth can communicate in many different ways. Popular example of these type of social applications includes, WhatsApp, Facebook, Line and many more. The proposed architecture will help parents to monitor the child and detect the bulling content before time. This helps to save child from becoming victims to such crimes online. The details of the architecture are shown in Fig. 5 and also discuss in the following sections.

A. Registration Module

This module is used to ask the user (parent) to enter the Application login information of his or her minor. This login information is used to retrieve the relevant data from the desired logged-in App. It also provides information of the application used by his or her minor.
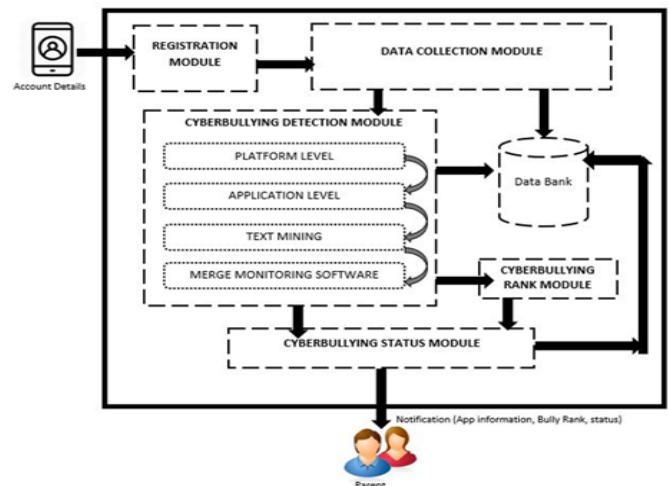

Fig. 5. Cyberbullying Detection Framework.

B. Data Collection Module

The Data Collection Module is the component that collects all the relevant information from the logged-in application for example:

- Contacts.
- Chat history.
- Backup of chat database.
- Avatars of contact.
- Received files.
- Sent files.
- Locations.

C. Data Bank

Stores all the relevant information regarding the particular topic and area of cyberbullying that is used by the application and helps to detect the bulling rank status further. It works as a repository of persistence information, keywords, chats, history, and any other relevant information based on the user requirements that can be used for reference for detection module.

D. Cyberbullying Detection Module

The Cyberbullying Detection Module uses the retrieved data to determine if a child or teenager is being bullied online. The main result of this component is the Bullying Rank (BR) calculated according to the state of art and specific vulnerability. Since we are focusing on Android apps, the following security settings will be checked accordingly.

E. Application Platform Level Security Check

A mobile application platform is a set of software tools used in the development, creation and maintenance of mobile applications. In part, it is an enterprise mobile application platform that provides organizations with mobile application tools. It is also vulnerable to many security threats. The continued emergence of mobile malware not only provides knowledge and copyright for developers, but also leads to information leakage and even financial loss. The security requirements of mobile applications have become a serious issue in the development of the entire application market. A tabularized Platform Level Security Comparison is shown in the Table I below.

TABLE I.   PLATFORM LEVEL SECURITY COMPARISON

Feature	Android	iOS
App Download	Crowdsourcing	iOS App store only
Signing Technology	Self-Signing	Code signing
Inter-process Communication	Yes	No
Open/ Close Source	Open source	Close
Memory Randomization	Yes	Yes
Storage	Internal & External	Internal only
Shared User ID	Yes	No

F. Application-Level Security Check

Application-level security refers to the security services that are invoked on the interface between the application and the queue manager connected to it. A tabularized Comparison is shown in Table II.

TABLE II.   APPLICATION-LEVEL SECURITY CHECK

Feature	Found (✓)/ Not Found (x)
Shared User ID	✓
No. of permissions	✓
Application Verification	✓
Encrypted Messages	✓
Decrypted Messages	✓
Contacts	✓
Media	✓
Location	✓

G. Text Mining Check

Here, we're going to use two sets of data. It uses the Bad Words Dataset and Sensitive Word Dataset to categorize the user's message and record the bad history in the database. If a user exceeds the limit for inappropriate posts or adult photos, they will be automatically blocked. Some abusive words are given in the Table III.

TABLE III.   ABUSIVE WORDS

ABUSIVE WORDS
BAD WORDS (Retarded, Dumb)
SWEAR WORDS (Bit**)
SECOND PERSON (You, Yours)

H. Merge Monitoring Software

Implementing monitoring software will help to understand the big picture. There are different types of monitoring software available (paid or free), including Spyzie and net nanny. Spyzie is a professional monitoring solutions provider that provides tracking and surveillance tools for smartphone users [24]. It is used to protect children from online threats and to ensure that they are always in a safe place. Parents will be able to track and store call logs, messages, social activities, etc.

I. Cyberbullying Rank Module

Rank the cyberbullying according to the following scale:

No.	RANK	RANGE
1	Low	0-3
2	Medium	4-6
3	High	7-10

The ranking will be based on the severity of the words which affects the mentality and behaviour of the teenagers and attract other teenagers and public opinion of the circle. Keywords will low affect will have less effect and thus will be

ranked low accordingly. For example, sexting and related keywords will be considered as high severity, posting embarrassing photos, stealing identity of a person will be considered high ranking but keywords related to beauty, body, may be considered as low rank or medium rank.

VI. ADVICE FOR PARENTS

To reduce the harms of cyberbullying and online behaviour, parents can:

- Set clear expectations about their child online reputation and behaviour.

- Make their children aware about the negative consequences of cyberbullying, make annoying and inappropriate comments and messages, share nude photos of you and other people, sexting etc. and the legal issues associated with all this.

- Be clear and strict about what can be viewed and what can be shared.

- Determine which apps are right and allowed to use for your child and which are not.

- Set rules for how your child spends time online or on the device.

- Simulate positive and respectful online behaviour to him through your devices and online and social media accounts.

- Talk to your child about the bad effects of being a bystander of cyberbullying.

Talking to your children about cyberbullying and digital behaviour is not a one-off activity, but a continuous conversation. Before your child switches to text messaging, social media, online games, and chatting, discuss these topics with them. It can help them better understand the reality and potential bad effects of cyberbullying and provide them with ongoing opportunities to practice the coping skills. In this way, you can support the transition from a bystander to ally. SAMHSA provides a free 'Learn about Bullying' app for parents, teachers and educators with dialogue options, tips and other tools to help prevent bullying [25].

If you think your child has witnessed cyberbullying, you can encourage them to do something they should and shouldn't. For example, encourage children to dislike or not like, share, or comment on someone's racial, or hurtful text or posted information, or send hurtful text to others. Without sharing and participating on the malicious or cyberbullying content, you can limit the harm the message can do to others or to yourself.

When the children feel they should react, encourage them to respond calmly, clearly, and constructively. Anger and violent reactions to a situation can make the situation worse. Encourage children (and adults!) To stay away from the device and not accuse, insult, or retaliate against others. It helps you stay calm and focused and shows that the digital behaviour of others is harmful and unacceptable.

Please reply directly to the person who sent the offending message or comment. If you feel safe, you can contact each other online, by phone, or directly with people creating or transmitting malicious messages. This way you can clearly show that they can't stand the negative behaviour. This is also an opportunity to honestly share concerns about the behaviour and its causes.

VII. CONCLUSION

This section concludes this article by identifying a complex set of open-ended research questions and compelling solutions. Cyber bulling is an emerging concern with growing technology. Main victims of cyberbullying are teenagers who are bullied online. Teenagers are emotionally weak and fall an easy prey. In this era to provide an e safe environment to children we proposed an architecture to detect cyberbully, rank it and provide information to the concerned parent.

In future, we will develop a prototype of this framework for general purpose use for both Android and iOS.

VIII. NOTES ON CONTRIBUTORS

Sultan Saud Alanazi completed his bachelor's in Information Technology from Deakin University in 2019. He is currently working for Al-Shamli General Hospital, Saudi Arabia as an IT admin. He is also doing his Master's in Cybersecurity at University of Ha'il. His area of interests includes Application security and Network security.

Dr. Adwan Alownie Alanazi received the PhD degree in Computer Science and engineering from the University of Bridgeport, USA. He is currently holding an assistant professor position with the University of Hail, Saudi Arabia. His research interests include Internet of things (IoT) and security in wireless Sensor networks.

REFERENCES

[1] Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: its nature and impact in secondary school pupils. Journal of Child Psychology and Psychiatry, and Allied Disciplines, 49(4), 376–385. https://doi.org/10.1111/j.1469-7610.2007.01846.x.

[2] Langos, C. (2012). Cyberbullying: The Challenge to Define. Cyberpsychology, Behavior, and Social Networking, 15(6), 285–289. https://doi.org/10.1089/cyber.2011.0588.

[3] O'Keeffe, G. S., & Clarke-Pearson, K. (2011). The Impact of social media on Children, Adolescents, and Families. Pediatrics, 127(4), 800–804. https://doi.org/10.1542/peds.2011-0054.

[4] Khan, G. F., Swar, B., & Lee, S. K. (2014). Social Media Risks and Benefits. Social Science Computer Review, 32(5), 606–627. https://doi.org/10.1177/08944393145247011.

[5] Ortiz-Ospina, E. (2019, September 18). The rise of social media. Retrieved from Our World in Data website: https://ourworldindata.org/rise-of-social-media.

[6] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005.

[7] Madden, D., & Deb, A. (2019, December 16). WhatsApp is a Threat to Society. Here's How to Fix It. Retrieved August 16, 2020, from Techonomy website: https://techonomy.com/2019/12/whatsapp-is-a-threat-to-society-heres-how-to-fix-it/.

[8] Bernal, N. (2018, July 4). WhatsApp admits encryption has helped criminals as it plans crackdown on illegal behaviour. The Telegraph. Retrieved from https://www.telegraph.co.uk/technology/2018/07/04/whatsapp-admits-encryption-has-helped-criminals-plans-crackdown/.

[9] Anderson, M., & Jiang, J. (2018, May 31). Teens, Social Media & Technology 2018. Retrieved from Pew Research Center: Internet, Science & Tech website: https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/.

[10] Rivera-Vargas, P., & Miño-Puigcercós, R. (2018). Young people and virtual communities. New ways of learning and of social participation in the digital society. Páginas de Educación, 11(1), 67. https://doi.org/10.22235/pe.v11i1.1554.

[11] Anderson, M. (2018, September 27). A Majority of Teens Have Experienced Some Form of Cyberbullying. Retrieved from Pew Research Center: Internet, Science & Tech website: https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/.

[12] Whittaker, E., & Kowalski, R. M. (2014). Cyberbullying Via Social Media. Journal of School Violence, 14(1), 11–29. https://doi.org/10.1080/15388220.2014.949377.

[13] Chan, T. K. H., Cheung, C. M. K., & Lee, Z. W. Y. (2021). Cyberbullying on social networking sites: A literature review and future research directions. Information & Management, 58(2), 103411. https://doi.org/10.1016/j.im.2020.103411.

[14] Patchin, J. W. (2015, February). Our latest research on cyberbullying among school students. Retrieved April 8, 2021, from Cyberbullying Research Center website: http://cyberbullying.org/2015-data/.

[15] Mahadevaiah, M., & Nayak, R. B. (2018). Blue Whale Challenge: Perceptions of First Responders in Medical Profession. Indian Journal of Psychological Medicine, 40(2), 178–182. https://doi.org/10.4103/ijpsym.ijpsym_399_177.

[16] Narayan, R., Das, B., Das, S., & Bhandari, S. S. (2019). The depressed boy who accepted "Blue Whale Challenge." Indian Journal of Psychiatry, 61(1), 105–106. https://doi.org/10.4103/psychiatry.IndianJPsychiatry_234_18.

[17] Luxton, D. D., June, J. D., & Fairall, J. M. (2012). Social Media and Suicide: A Public Health Perspective. American Journal of Public Health, 102(S2), S195–S200. https://doi.org/10.2105/ajph.2011.300608.

[18] NDTV. (2018, August 26). After Two Deaths, Bengal Grapples with Suicide Game "Momo Challenge." Retrieved April 8, 2021, from NDTV.com website: https://www.ndtv.com/india-news/after-two-deaths-bengal-grapples-with-suicide-game-momo-challenge-1906357.

[19] Chiu, A. (2018, September 5). The "Momo Challenge": A sinister threat to young people or an urban myth?. Washington Post. Retrieved from https://www.washingtonpost.com/news/morning-mix/wp/2018/09/05/the-momo-challenge-a-sinister-threat-to-young-people-or-an-urban-myth/.

[20] Ybarra, M. L., & Mitchell, K. J. (2004). Online aggressor/targets, aggressors, and targets: a comparison of associated youth characteristics. Journal of Child Psychology and Psychiatry, 45(7), 1308–1316. https://doi.org/10.1111/j.1469-7610.2004.00328.x.

[21] Elsaesser, C., Russell, B., Ohannessian, C. M., & Patton, D. (2017). Parenting in a digital age: A review of parents' role in preventing adolescent cyberbullying. Aggression and Violent Behavior, 35, 62–72. https://doi.org/10.1016/j.avb.2017.06.004.

[22] Mehari, K. R., Moore, W., Waasdorp, T. E., Varney, O., Berg, K., & Leff, S. S. (2018). Cyberbullying prevention: Insight and recommendations from youths, parents, and paediatricians. Child: Care, Health and Development, 44(4), 616–622. https://doi.org/10.1111/cch.12569.

[23] UNICEF. (2020). Cyberbullying: What is it and how to stop it. Retrieved from www.unicef.org website: https://www.unicef.org/end-violence/how-to-stop-cyberbullying.

[24] Spyzie. (2020). Spyzie. Retrieved from Spyzie.com website: https://www.spyzie.com/.

[25] SAMHSA. (n.d.). KnowBullying Mobile App | Publications and Digital Products. Retrieved from store.samhsa.gov website: https://store.samhsa.gov/product/knowbullying.