Impact of Social Media-Related Cybercrimes and Preventive Precautions

AKSA Anudini#, HMSS Dissanayake and GAI Uwanthika

Department of Computer Science, General Sir John Kotelawala Defence University, Sri Lanka

#36-cs-0011@kdu.ac.lk

Abstract - The impact of social media on people's lives is enormous. Through social media, people can communicate and collaborate with anyone in the world and can entertain themselves. It is a good platform for entrepreneurs to promote their business too. As a result of the COVID-19 pandemic, people tend to work from home relying on computer systems, mobile devices and different social media platforms. The usage of social media platforms for communication, sharing information, business purposes and shopping increased to mitigate the impact of social distancing. Cybercrime will rapidly rise because of the widespread use of social media. The increase in volume, velocity, veracity and variety of data in social media networking are major concerns that may lead to privacy and security issues. Cybercrimes will create a massive impact on the security of people in future. To address this problem, the security of social media users should be improved using different techniques. This paper focuses on the usage of different social media platforms, types of social media-related cybercrimes, techniques, tips, recommendations and future precautions that can be used to prevent social media-related cybercrimes.

Keywords: ***cybercrime, social media, cybersecurity***

I. INTRODUCTION

Social media is a computer-based technology that enables people to interact with each other around the world and it helps to discover new things too. People can exchange data, pictures, videos through social media platforms. Among all the social media platforms Facebook, YouTube, WhatsApp, Messenger, Instagram, TikTok, Twitter, LinkedIn, Telegram, etc. are at the top. There are around 4.33 billion social media users worldwide in 2021, which's more than 55% of the global population. The growth of social media users increased by 13.7% from 2020 to April 2021, which means 16.5 new users per single second (Kemp & Kepios, 2021). Facebook is the biggest social media platform that is using today, it has nearly 2.85 active users in the first quarter of 2021 (Tankovska, 2021). With the rapid increase in social media users, social media platform security should be a key focus. These platforms should take appropriate steps to combat hackers and safeguard users' sensitive information. Social media data leakage makes a huge effect on data of people, intellectual property, business operations, etc.

Cybercrime is a criminal activity carried out against computers or devices to damage them or to harm sensitive data of individuals. Cybercrimes such as committing frauds, trafficking pornography of children, stealing identities, trafficking intellectual property, etc. can happen through social media. With the huge increase in social media usage cybercrimes raised day by day. Hackers try to get access to social media accounts of people and attack the financial and personal information of people suspiciously. As a result of the Covid-19 pandemic, people all around the world were compelled to work from home, reliant on the internet. As a result of this situation, cybercrime will become a bigger problem in 2020 and 2021 (Monteith, et al., 2021). To avoid cybercrimes people can enhance the security of their social media accounts themselves as well as all the authorized parties such as the government, social media companies, and cybersecurity authorities should take appropriate actions to reduce cybercrimes. This paper discusses the usage of different social media platforms, social media-related cybercrimes, a discussion on preventive measures against cybercrimes, and the conclusion.

II. BACKGROUND STUDY

Social media has been on the rise because of the Covid-19 pandemic (Monteith, et al., 2021). In 2021, social media networks such as Facebook, YouTube, WhatsApp, etc. are at their peak, with billions of active users.

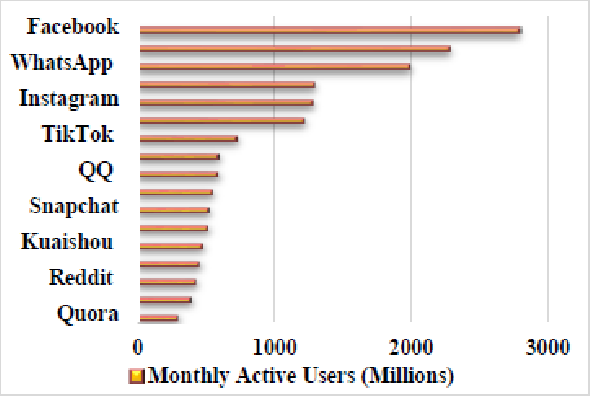

Figure 1. Different social media platform users of April 2021 Source: (Kemp & Kepios, 2021)

A study has revealed that a user visits more than 6 social media platforms each month and a user spends an average of 2.5 hours on social media per day. It also revealed that people spend about 15% of their lives on social media. In a typical day, people around the world spend over 10 billion hours on social media platforms, equating to 1.2 million years of human existence (Kemp & Kepios, 2021). Social media platform preferences are different from country to country. So, the main important thing is to concern about the privacy and security of people's data at a local level too by relevant authorities of the country.

Cybercrime has been identified as a major global threat (weforum.org, 2019). Cybercrime rate increases with the rapid use of social media platforms. Figure 2 shows how cybercrime complaints increased from 2016 to 2020 according to the data provided by the internet crime complaint center (Institute.org, 2020).

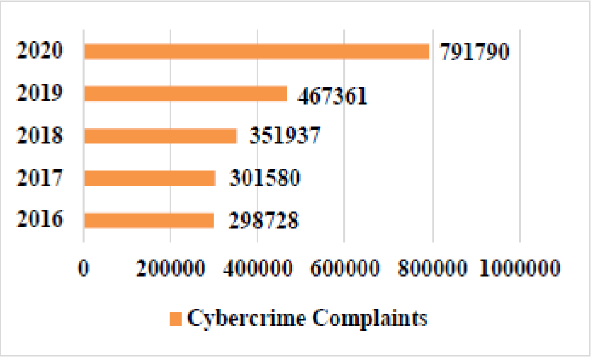

Figure 2. cybercrimes complaints (2016-2020) Source: (Institute.org, 2020)

As seen in Figure 2, cybercrimes increased considerably from 2019 to 2020. The main reason for this issue is the growing popularity of working from home because of the Covid-19 pandemic. Millions of people, including children, university students, employees, and others, were obliged to work from home because of this circumstance, and their use of social media platforms increased (Monteith, et al., 2021).

Main cybercrimes related to social media are Cyberstalking, Cyberbullying, Identity theft, Social engineering and phishing, Burglary using social networking, Malware (Malicious software), Cyber-casing, Cyber intrusion, and data breaches.

A. Cyberstalking, Cyberbullying

Cyberstalking and cyberbullying mean a crime where an attacker harasses a man/ woman using any social media platform or any other medium. Cyberstalking may include threats, cryptic messages, or sexual content. Mainly through cyberstalking attackers create major psychosocial impacts on victims. Victims reported many serious consequences such as depression, fear, stress because of cyberstalking and cyberbullying. January is the National Stalking Awareness Month since 2004 which raises to aware the impact of stalking and helps victims to get rid of depression, stress, and fear of cyberstalking. A survey revealed that 6 to 7.5 million people get stalked in the US each year and the 18-24 age limit is the highest risky age group being stalked. The survey found that 1 out of 5 people changes their daily routine, 1 out of 6 people change their contact details and social media accounts, 1 out of 8 employed people lose their jobs because of cyberstalking. According to the survey, 7% to 40% of students reported being stalked. (Telloian, 2019).

B. Identity theft

Identity theft means obtaining Personally Identifiable Information (PII) of people through social media platforms. Credit and Debit card frauds, online shopping frauds, driver license identity theft, child identity theft, mail identity theft, etc. are some identity thefts that occur mainly. Attackers use the information of victims to get access to their bank accounts and other sensitive information. This will be a huge problem for the security of victims' data. Identity theft is the category of cybercrimes that got the most complaints in 2020 (Institute.org, 2020).

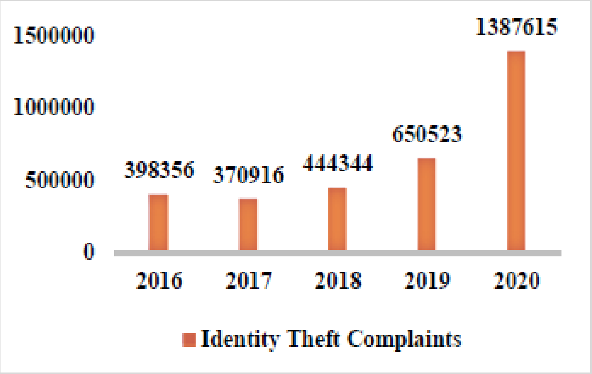

Figure 3. Identity theft complaints from 2016 to 2020. Source. (Institute.org, 2020)

C. Social engineering and phishing

Social engineering can be defined as tricking a user into giving up his or her private information. Phishing is a type of fraud that uses social engineering techniques. It is an attempt to acquire sensitive data of people such as passwords and credit card details by masquerading as a trustworthy person or business in an electronic communication. According to the Federal Bureau of Investigation (FBI), phishing is the most used cybercrime type in 2020. Phishing incidents doubled the frequency from 2019 to 2020. Federal Bureau of Investigation stated that phishing complaints raised 11 times in 2020 when compared with 2016.

D. Burglary using social networking

Social media burglars search for the personal information of people such as place of work, birthday, contact numbers, interests, etc. using their bio. Burglars keep attention to the posts shared by people about their trips, dinner outings, etc. to make their targets easy. According to a survey conducted in the US and UK with the prisoners convicted of burglary. The results of a survey were 30% of social media users mentioned their future holiday details in their accounts and 70% of users post Instagram photos when they are on trips (Verisure.CO.UK, 2017). It will be very easy for burglars to attack their empty homes. A survey was conducted with 500 burglars in New York and New Jersey in 2016. The result of the survey was 10% of burglars find their targets by checking current locations of people through social media (Verisure.CO.UK, 2017). It is recorded that a professional burglar attacked 33 women in California using GPS data of their Instagram and Facebook photos in 2015 (O'Reilly, 2021).

E. Malware (Malicious software)

Malware can be defined as a program file that will be harmful to computer users. It includes computer viruses, trojan horses, bots, worms, spyware, adware, etc. Through malware deleting sensitive data, monitoring user's activities, stealing data, encrypting sensitive data can happen. These malware attacks happen mainly through clicking un-secure links and opening un-secure attachments. If users click on these destructive links or documents, the virus will infect their accounts.

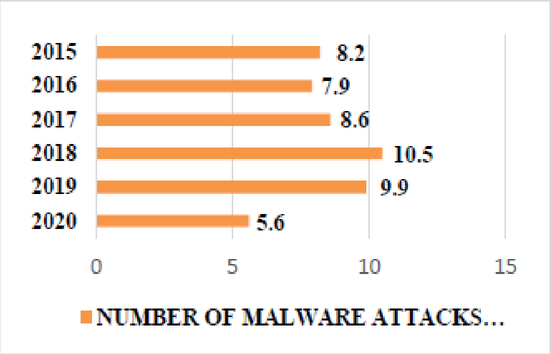

Figure 4. The number Of Malware Attacks Worldwide (2015- 2020). Source: (Johnson, 2021)

F. Cyber-casing

Cyber-casing uses geotagged text, photos, and videos to criminals. Geotagging refers to the process of adding geographical identification to the photographs, videos, etc. At present geo-tagging is a major trend in social media platforms. Geo-tagging is the root cause for the cyber- casing, which helps the attackers to plan their cybercriminals.

G. Cyber intrusion and data breaches

In Cyber intrusion, hackers use automated computer programs or files to access the computers or social media accounts of users. Data breaching means accessing the sensitive information of people without their permission. In data breaching also hackers use the personal information of people such as financial details, medical details, etc. Cyber intrusion and data breaches can be considered as a new emerging crime (Soomro & Hussain, 2019).

Table 1. The annual number of data breaches and the number of exposed records through data breaches from 2015 to 2020

Year	Number of Data Breaches	Number of exposed records through data breaches
2020	1001	155.8
2019	1473	164.68
2018	1257	471.23
2017	1632	197.61
2016	1106	36.6
2015	784	169.07

Source: (Johnson, 2021)

III. DISCUSSION

Social media plays an important role in the life of people. The main communication mode use now is social media. People use social media to stay in touch with their friends, stay updated with news and current events, get entertainment in their free time, network with people in the world, share photos or videos with friends, promote businesses, buy products from online stores in social media, etc. People can use preventive methods to enhance the security of their social media accounts such as using strong passwords, use different passwords for accounts on different social media platforms, etc. People should not click un-secure links, should not open un-secure attachments, should not access their social media accounts using un-secure Wi-Fi networks, and do not share passwords with friends. Relevant authorities such as companies and legal authorities should take appropriate actions to secure the social media accounts of users.

A. Preventing Cyberstalking, Cyberbullying

To prevent cyberstalking and cyberbullying people can keep a low personal profile while utilizing privacy settings, without sharing personal details such as an address, phone numbers, and other real-time information such as where you are and who you are with. You can use separate email addresses for office work and social networks to ensure your security. And if possible, you can use a nickname on social media platforms like Instagram, Twitter, etc. And mainly you should not add friend requests from fake profiles. Fake profile holders mostly use a name of a famous person or any other commonly used names (These names may vary from country to country). They don't share their pictures in profile pictures, sometimes they use photos of people in military uniforms. Fake profiles mostly don't contain any shared contents or sometimes have fake content and those accounts have no mutual friends or few mutual friends. And another important thing to prevent stalking and bullying is updating the software because software updates are developed to patch security threats, hiding IP addresses, maintain good digital hygiene and avoid disclosing sensitive information. According to the studies conducted women get affected by cyberbullying and cyberstalking than men (Zsila, et al., 2019). When anyone is being cyberstalked by someone, they should block the person, report that person, inform the police and other relevant authorities, and take illegal actions to ensure security. Most of the time it is difficult to track professional attackers because they know how to anonymize themselves. When discussing the legal aspects of cyberstalking most countries don't have laws to regulate cyberstalking. Cyberstalking in the United States is discussed under harassment and anti-stalking laws. A fine or imprisonment is given depending on the severity of the case (Tripwire, 2018). Techniques that can use to prevent cyberstalking and cyberbullying are rule mining, text mining, signature-based data mining, and cyberstalking detection framework.

B. Preventing Identity theft

People can freeze their credit cards to prevent prospective creditors from accessing their credit files. Freezing helps to prevent opening accounts to your name by others. And people can safeguard their social security number, can be alert about phishing and spoofing, can use strong passwords, can add an extra authentication step to access their social media accounts, users can check their mails credit reports regularly, and monitor financial and medical statements. It is important to destroy expired driving licenses and other identity documents and shouldn't share identity documents on social media platforms. People should keep their credit cards, debit cards, and other personal identity documents securely with themselves. People can report identity theft problems to the Federal Trade Commission, postal service and credit bureaus, and police departments. Then they can follow the recommended steps to make a recovery plan. Preventive techniques for identity thefts are using three-factor authentication, biometrics, anti-virus software, genetic algorithm, logistic regression, hidden Markov model, and outlier detection. Credit card fraud is also widely occurring in identity theft. To prevent credit card fraud can use the techniques such as Address Verification Service (AVS), Card Verification Value (CVV), hidden Markov model, decision tree, and genetic algorithm.

C. Preventing Social engineering and phishing

To prevent social engineering and phishing people should be suspicious about e-mails and messages which asked for their personal information. Most user-friendly anti-phishing techniques are one-time password (OTP), CAPTCHA, digital certificates, genetic and attribute-based anti-phishing algorithms. People shouldn't provide their details unless verifying the identity of websites, emails, and messages and should refrain from sharing any personal or financial information on social media. If anyone doubts these messages, you can directly contact the relevant organization to verify the problem. And people should mainly concern about the Uniform Resource Locator (URL) of a website is secure or not. Installing anti-virus software, firewalls, and email filters help to reduce social engineering and phishing attacks. If anyone is a victim of these types of attacks, they can inform the administrators of the relevant company about the suspicious activity. Then take relevant legal actions by informing the police and Federal Trade Commission. If financial accounts get attacked people can inform the financial institute and close your accounts. Another key step is to change passwords. If people use the same password for multiple accounts, they are more likely to be hacked. The use of neural networks is a good technique to prevent social engineering and phishing.

D. Preventing Burglary using social networking

People can take appropriate decisions to prevent burglary. People can share their posts only with their friends and followers because if they share their posts publicly anyone in the world can see their posts, it will be very risky for their security. Also, through the settings and privacy of social media accounts, people can avoid being tagged in other people's posts. Limiting connections to known people is also a good way to get rid of burglary. Sharing personal information like address, phone number, birthday, workplace, day to day outings is a good target for burglars. Don't give a chance to burglars to target your home or workplace. If you are a victim of burglary, you can inform the police station as quickly as possible, then they will get appropriate steps to find the burglars. People can use security cameras, door locks, motion-activated lights, etc. to ensure the physical security of their places. Preventive techniques for burglary are genetic algorithms and case base reasoning, time-series approach, multi-layer perception, rule-based induction, and random forest-based model can be mentioned.

E. Preventing Malware (Malicious software)

The most suitable way to prevent malware is by installing anti-virus software. It can scan your computer and protect against malware. A regular software update is also a good solution to prevent malware. Mainly users shouldn't click suspicious links and avoid downloading un-secure documents. Always should be aware of the fake websites which asked for your personal information through them anyone can get a direct attack to the computer. Installing a firewall is another solution to prevent malware. A firewall can provide an extra barrier to malware when compared with anti-virus software. Regular backup is important to protect your valuable data from malware and should always be aware that the Uniform Resource Locator (URL) of a website is secure or not. Signature-based malware detection, anomaly-based malware detection, hybrid features, assembly instructions, N-gram models in Natural Language Processing (NLP) are some techniques to prevent malware.

F. Preventing Cyber-casing

Switching off Global Positioning System (GPS) is a solution to prevent cyber-casing. It is important not to share your vacation photos publicly on social media before returning home. People should avoid sharing their daily outing times on social media.

Techniques that can be used to prevent cyber-casing are Support Vector Machines (SVM) classifiers, use online tools such as geoimgr.com to remove the geolocation of images.

G. Preventing Cyber intrusion and data breaches

Cyber intrusion and data breaches can be minimized by upgrading devices, enforcing Bring Your Device (BYOD) policies, and enforcing multi-factor authentication. Deploying an intrusion detection and prevention system is the best solution to prevent cyber intrusion and data breaches. Techniques that can be used are verification and validation, Personal Identification Number (PIN), Card Verification Method (CVM), National Vulnerability Database (NVD), and Common Vulnerability Exposure Database (CVE)

Table 2. Preventive precautions and recommendations that can be taken by users and preventive techniques.

Cybercrime	**Preventive tips and recommendations to enhance the security of social media platforms**	**Preventive Techniques to enhance the security of social media platforms**
Cyberstalking, Cyberbullying	•keep a low personal profile while utilizing privacy settings. •Use a nickname on social media platforms. •Updating and upgrading the software on time. • Use different email addresses for personal accounts and work.	Rule mining, text mining, signature-based data mining, and cyberstalking detection framework.
Identity theft	• safeguard all identity documents • Be alert about phishing and spoofing, can use strong passwords, • Add an extra authentication step to social media accounts • Check mails credit reports regularly • Monitor financial and medical statements regularly • Destroy expired driving licenses and other identity documents	Three-factor authentication, biometrics, anti-virus software, genetic algorithm, logistic regression, hidden Markov model, and outlier detection. To prevent credit card fraud can use the techniques such as Address Verification Service (AVS), Card Verification Value (CVV), hidden Markov model, decision tree, and genetic algorithm
Social Engineering and Phishing	• Shouldn't provide details unless verifying the identity of websites, emails, and other messages. • Should refrain from sharing any	One-time password (OTP), CAPTCHA, digital certificates, genetic and

	personal or financial information on social media. • Can directly contact the relevant organization to verify the doubts about emails or messages. • Installing anti-virus software, firewalls, and email filters help to reduce social engineering and phishing attacks.	attribute-based anti-phishing algorithms, and neural networks
Burglary using social networking	• Don't share locations when sharing photos • People can share their posts only with their friends and followers. • Through the settings and privacy of social media accounts, people can avoid being tagged in other people's posts. • Limiting connections on social media. • Don't share personal information like address, phone number, birthday, workplace, day to day outings on social media • Use security cameras, door locks, motion-activated lights, etc. at homes and workplaces to get extra security.	Genetic algorithms and case base reasoning, time-series approach, multi-layer perception, rule-based induction, random forest-based model
Malware	• Installing anti-virus software • Updating and upgrading software on time • Shouldn't click suspicious links and avoid downloading un-secure documents. • Aware of the URL of websites are secure or not • Installing a firewall • Regular backup	Signature-based malware detection, anomaly-based malware detection, hybrid features, assembly instructions, N-gram models in Natural Language Processing (NLP).
Cyber-casing	• Switching off Global Positioning System (GPS) • Don't share vacation photos publicly on social media before returning home. • Avoid sharing the daily routine of life on social media. • Use online tools such as geoimgr.com to remove the geolocation of images	Support Vector Machines (SVM) classifiers
Cyber intrusion and data breaches	• Upgrading devices • Enforcing Bring Your Device (BYOD) policies • Enforcing multi-factor authentication. • Deploying an intrusion detection and prevention system	Verification and validation, Personal Identification Number (PIN), Card Verification Method (CVM), National Vulnerability Database (NVD), and Common Vulnerability Exposure

		Database (CVE)

IV. CONCLUSION

The above statistics prove that cybercrimes via social media are gradually expanding with each passing year. If people give priority to personal security, most of the cybercrimes through social media can be reduced. Most people are victims of cybercrime because of their negligence. This paper discussed seven major cybercrimes that can occur through social media, as well as the tips and techniques that users can undertake to minimize cybercrimes. As discussed in this paper, most social media-related cybercrimes can be avoided by sharing photos and other personal information only with friends, using separate email addresses for personal and professional accounts, adding an extra authentication step to social media accounts, strengthening passwords while using unique passwords for different social media platforms, and limiting connections on social media platforms. People shouldn't provide their details unless verifying the identity of websites, emails, or messages, and shouldn't share locations when sharing photos. And people can enhance their security by installing anti-virus software, firewalls and updating and upgrading software on time. Apart from that, this paper discussed the preventive techniques that can use by social media companies and other cybersecurity authorities to enhance the security of social media platforms and these techniques include Natural Language Processing techniques, Neural Networks, Genetic Algorithms, Biometrics, Digital Signature, etc. It can be concluded that most social media-related cybercrimes can be minimized if people use the above-discussed cybercrime preventive tips for their social media accounts. In addition, cybersecurity authorities and social media companies should use preventive techniques discussed in this paper to enhance the security of social media platforms.

REFERENCES

Institute.org, I. I., 2020. Insurance Information Institute. [Online] Available at: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime

Johnson, J., 2021. Statista. [Online] Available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records exposed/#:~:text=In%202020%2C%20the%20number%20of,%2Dthan%2Dadequate%20information%20security.

Johnson, J., 2021. Statista. [Online] Available at: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/

Kemp, S. & Kepios, 2021. DATAREPORTAL. [Online] Available at: https://datareportal.com/social-media-users#:~:text=Our%20latest%20data%20show%20that,of%20the%20total%20global%20population.

Kemp, S. & Kepios, 2021. DATAREPORTAL. [Online] Available at: https://datareportal.com/social-media-users#:~:text=Our%20latest%20data%20show%20that,of%20the%20total%20global%20population.

Monteith, S., Bauer, . M. & Alda, . M., 2021. Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. Current Psychiatry Reports, 23(4), pp. 1-9.

O'Reilly, L., 2021. Security Boulevard. [Online] Available at: https://securityboulevard.com/2021/02/the-state-of-phishing-in-2021/

Rosenthal, M., 2021. Tessian. [Online] Available at: https://www.tessian.com/blog/phishing-statistics-2020/#:~:text=According%20to%20the%20FBI%2C%20phishing,in%202020%20compared%20to%202016.

Soomro, T. R. & Hussain, M., 2019. Social Media-Related Cybercrimes and Techniques for Their Prevention. Applied Computer Systems, 24(1), pp. 9-17.

Tankovska, H., 2021. Statista. [Online] Available at: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/#:~:text=With%20roughly%202.85%20billion%20monthly,the%20biggest%20social%20network%20worldwide.

Telloian, C., 2019. *GoodTherapy.* [Online] Available at: https://www.goodtherapy.org/blog/facts-and-statistics-that-emphasize-how-stalking-impacts-mental-health-0131198

Tripwire, 2018. *Tripwire.* [Online] Available at: https://www.tripwire.com/state-of-security/security-awareness/what-cyberstalking-prevent/

Verisure.CO.UK, 2017. *Verisure Smart Alarms.* [Online] Available at: https://blog.verisure.co.uk/how-burglars-use-social-media/

weforum.org, 2019. *World Economic Forum.* [Online] Available at: https://www.weforum.org/reports/the-global-risks-report-2019

Zsila, A., Urban, R. & Demetrovics, Z., 2019. Gender Differences in the Association Between Cyberbullying Victimization and Perpetration: The Role of Anger Rumination and Traditional Bullying Experiences. *International Journal of Mental Health and Addiction,* 17(5), pp. 1252-1267.

ACKNOWLEDGMENT

This research was supported by General Sir John Kotelawala Defence University; we would like to pay our gratitude to all the lecturers at the Faculty of Computing for the guidance provided throughout this research.

AUTHOR BIOGRAPHIES

AKSA Anudini is a third-year undergraduate of General Sir John Kotelawala Defence University. Following the BSc (Hons) Computer Science Degree Programme. Studied at Sanghamitta Balika Vidyalaya, Galle.

HMSS Dissanayake is a third-year undergraduate of General Sir John Kotelawala Defence University. Following the BSc (Hons) Computer Science Degree Programme. Studied at Kingswood College, Kandy.

GAI Uwanthika Received BSc(sp) in Computer Science and Technology degree from Uva Wellassa University. Currently pursuing her master's degree at the University of Peradeniya. The main research interests include Bioinformatics, Deep Learning, and Digital Image Processing.