Naif Arab University for Security Sciences

Journal of Information Security and Cybercrimes Research

مجلة بحوث أمن المعلومات والجرائم السيبرانية

https://journals.nauss.edu.sa/index.php/JISCR

JISCR

COVID-19 Pandemic Fuels Rise in Cybercrime: Egypt Case Study

Heba A. Yassa[*], Ramy N. Zakaria, Nora Z. Abdellah

Faculty of Medicine, Assiut University, Egypt.

Received 10 Feb. 2023; Accepted 30 May 2023; Available Online 22 Jun. 2023

Abstract

Since the declaration of COVID-19 as a pandemic by the World Health Organization, economies and daily life in many countries have been significantly affected. To mitigate the spread of the virus, various measures such as travel restrictions, lockdowns, and stay-at-home orders have been implemented worldwide. Consequently, there has been an increased reliance on internet-based methods to ensure public safety and continue essential activities. However, this increased online presence has also provided cybercriminals with opportunities to engage in malicious activities, exploiting the pandemic for financial gain. This study aims to provide a brief review of the cyber activities associated with the COVID-19 outbreak and investigate the extent of cybercrime during this period. A cross-sectional survey was conducted online, involving 400 internet users, to assess the occurrence of cybercrime during the pandemic. The findings indicate that victims of cybercrime encompass not only individuals who use online directories but also those engaging in routine internet searches and email communications. The study reveals that cybercrime has a detrimental impact on users' online experiences, potentially leading them to limit their online activities and resort to offline alternatives. The objective of this research is to comprehensively study cyber-attacks, analyzing the concept and variations of cyber-attacks before and during the COVID-19 pandemic era, in order to identify patterns, trends, and the overall impact of cybercrime on individuals.

I. Introduction

Before the end of 2019, COVID-19 virus was detected in China, and has been spread out massively and announced by the World Health Organization (WHO) as a pandemic. This pandemic has altered life globally by compelling organizations and individuals to embrace new practices such as social distancing and Teleworking [1]. Governments thought out ways to guarantee economic stability, this included expanded telework [2]. While the world is centered on the health and economic threats posed by COVID-19, cyber criminals around the world undoubtedly were profiting from this crisis prompting more cyber-crimes [3].

The UK's Crown Prosecution Service (CPS) categorize cyber-crime into two main general classes: cyber-enabled and cyber-dependent crimes. A cyber-dependent crime is a crime, “that can only be committed using a computer, computer networks or other form of information communications technology (ICT)”. Cyber-enabled crimes are, “traditional crimes, which can be expanded in their scale or reached by utilization of PCs, networks or different types of ICT” [4].

Keywords: COVID-19, Cybercrimes, Cyberspace Security, Financial fraud.

Production and hosting by NAUSS

[*] Corresponding Author: Heba A Yassa

Email: hebayassa@aun.edu.eg

doi: 10.26735/KUXW6317

UNODC reported the widely used threats that tormented the digital world during Covid19 pandemic. Several malicious websites promoted COVID-19 Phishing Email Kits utilizing an infected email attachment disguised as a map of the virus's flare-up [5]. To improve probability of success, the attacks targeted sale of high demand goods (e.g., Personal Protection Equipment (PPE) and Covid19 testing kits and medications), and impersonations of public authorities like WHO and CDC [6]. The US Federal Trade Commission estimated that 12 million dollars were lost from COVID-19-related fraudulent activities between January and April 14,2020 [7].

Since the beginning of the pandemic, the numbers of malwares attacks have fundamentally increased [8] with phishing being reported to have expanded by 600% in March 2020[8]. Phishing includes trials by illegitimate parties to persuade people to do an action (e.g., upload site, share private information or visit a site) under the affectation that they are involved in an authentic party [9]. Pharming is an advanced variant of phishing that aims to divert users into visiting malicious websites (e.g., utilizing DNS-based methods). This sort of attack is less common, as it requires utilizing more complex and well-designed techniques [10].

During April 2020, Google allegedly hindered millions of malwares and phishing messages daily. Hundreds of domains related to COVID-19 have been registered daily. While some of them are genuine without ill-intentions, an enormous part of them is noxious in nature. By the end of March 2020, more than 9,000 domains were registered and enlisted with Covid19 theme. These vindictive websites have a wide variety of attacks at their disposal as creating domain names like the CDC's web address to request passwords and even bitcoin donations to support fake causes as funding Covid19 vaccine [5].

The vindictive websites can collect private data that may be used to make financial fraud, or it may install malware. Malware indicates that software that can be used for extracting data (e.g., credit card numbers, banking data, cryptocurrency wallets) and a range of other assaults like taking unapproved control of webcams, gathering sensitive data and installing a keylogger which will record everything all that is composed. Ransomware is a well-known type of malware today [11].

Hacking is a type of crime that includes compromising the confidentiality of a system and requires a reasonable technical skill that involves abusing system vulnerabilities to break into systems [11]. Denial of Service (DoS) attacks target system availability and work by flooding key services with illegitimate demands. The objective here is to devour the bandwidth utilized for authentic server demands, and ultimately disconnect the server. In cyberspace, availability of the assets is a vital component of cyber security alongside confidentiality and integrity [31].

II. Literature Review

Authors in [32] have conducted a comprehensive overview of the impact of the COVID-19 pandemic on cybercrime in Egypt. The authors conducted a systematic review of the literature and found that there has been a significant increase in cybercrime in Egypt during the pandemic. They also discuss the factors that have contributed to this increase, such as the increased use of online services and the increased vulnerability of businesses and individuals. In [33] a qualitative analysis of the impact of the COVID-19 pandemic on cybercrime in Egypt is provided. The authors interviewed 15 experts in the field of cybercrime and found that the pandemic has led to an increase in the number of cybercrime cases, the sophistication of cybercrime attacks, and the difficulty of investigating cybercrime cases. Authors in [34] have conducted a quantitative analysis of the impact of the COVID-19 pandemic on cybercrime in Egypt by analyzing data from the Egyptian Computer Emergency Response Team (CERT) and found that there was a 200% increase in cybercrime reports in the first six months of the pandemic. The most common types of cybercrime reported were phishing, malware, and ransomware. Authors in [8] stated that the increased anxiety caused by the pandemic heightened the likelihood of cyber-attacks succeeding corresponding with an increase in the number and range of cyber-attacks. Through their analysis, results showed how following what appeared to be large gaps between the initial outbreak of the pandemic in China and the first COVID-19 related cyber-attack, attacks steadily became much more prevalent to the point that on some days, three or four unique cyber-attacks were being reported. A recent publication by European Union Agency for law Enforcement Training (CEPOL) in [35] has highlighted that Coronavirus had made a clear path for cybercriminals, that through use of social media and messaging platforms gained easy access to potential victims with a significant increase in activity related to child sexual abuse and exploitation and medical related scams.

III. Methodology

In order to track the cybercrime problem in Egypt, A cross sectional survey was generated, to ask about sex, age, level of education, internet use hours before and after the pandemic, the most common sites used, the main cause to visit these sites, occurrence of crime through the internet. The data has been collected through an online survey. In order to comprehensively investigate the issue of cybercrime in Egypt, a cross-sectional survey methodology was employed to gather relevant data. This approach allows for a snapshot of the current situation by collecting data from a diverse range of individuals at a specific point in time. The survey included a set of questions designed to capture important demographic information such as sex, age, and level of education. These factors are crucial in understanding how different segments of the population may be affected by cybercrime and how their online behaviors may vary. Additionally, the survey inquired about the participants' internet usage patterns both before and after the pandemic. This information provides insights into the potential impact of the pandemic on online activities and whether there have been any notable changes in behavior during this period.

The survey also aimed to identify the most commonly used websites or online platforms among the respondents. Understanding the preferred online platforms helps identify areas that may be more susceptible to cybercrime and aids in developing targeted preventive measures.

Participants were asked about the main reasons for visiting these websites or platforms. This aspect provides valuable information about the motivations and intentions behind online activities and can help identify potential risk factors or areas of vulnerability. Furthermore, the survey included questions regarding the occurrence of cybercrime experiences. By collecting data on reported incidents, the research aims to assess the prevalence and nature of cybercrimes in Egypt. To ensure the feasibility and wide reach of data collection, an online survey platform was utilized. This allowed for efficient data collection from a larger and more geographically diverse sample of participants. The online format also ensures anonymity, which encourages participants to provide accurate and honest responses. Overall, the cross-sectional survey methodology utilized in this study provides a comprehensive and timely assessment of the cybercrime problem in Egypt. By collecting data on various factors related to online behavior and experiences, the research aims to shed light on the extent, patterns, and impact of cybercrime in the country.

- Statistical Analysis and limitations

All collected information of this survey has been shown in different charts and graphs. Using the SPSS program to analyze data by using percentage analysis. The work did not list all the attacks occurred in relation to the pandemic, as these are too much to be gathered, as well as the limited information and the fact that some attacks are hard to be traced,

IV. Results

This study aimed to clarify the effects of COVID 19 spread all over the world on cybercrime especially after increasing the work from home due to social distance. The volunteers who shared in the study was 400, 58.7% of them were females and 41.3% were male as shown in Fig. 1.

Fig. 2 shows the age distribution of those who shared in the study, highest number of the volunteers was among those in the age group (30-≤40 years) followed by age group (40-≤ 50-year-old).

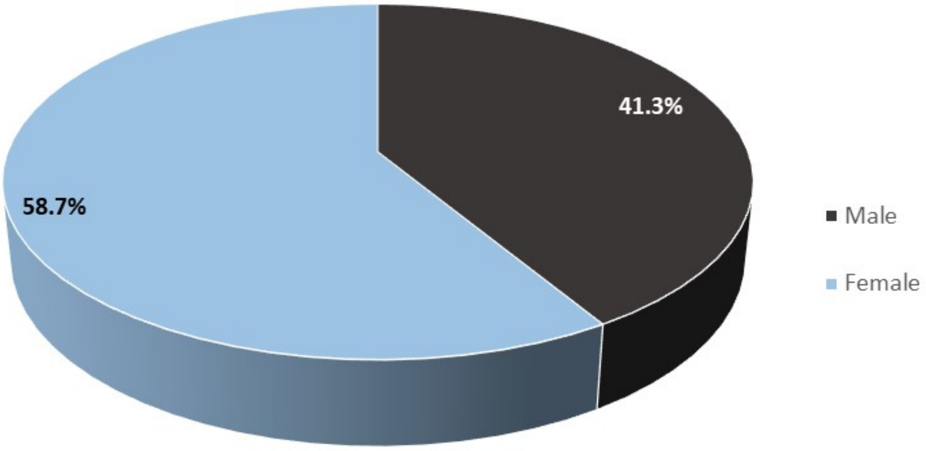

Fig. 1 Percent of male and female distribution among the study sample about the cybercrime during COVID 19

Table I shows the level of education in the participants. It reveals that 46% of them were educated with master degree, 23.25% high school, 17.25% less than high school education. Table II reveals the percent of hours that the internet users stay in front of the internet before and during spread of COVID 19 pandemic. There was highly significant difference between the two periods. During the pandemic most of the people stay at home and there was highly significant increase in the duration of the internet use, 65.7% of the users stay in front of the internet from 5 to 14 hours daily.

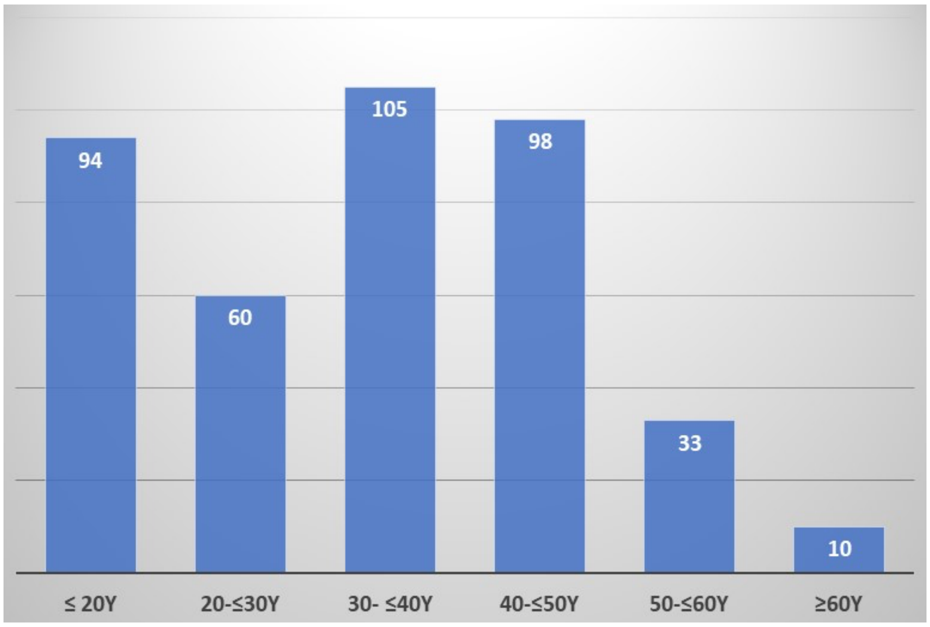

Fig. 2 Percent of age distribution of the participants in the study

Table III reveals the most common sites that used by the participants, most of them about 87% use social media every day mostly to chat or to know the new in spread of COVID 19, 78% use E mail every day,

TABLE I
Distribution of the Participants in the Study According to Their Learning

	No.	Percent
Illiterate	12	3
Less than High school	69	17.25
High school	93	23.25
Graduate	42	10.5
Master degree or more	184	46
Total	400	100

TABLE II
Distribution Percent According to Hours of Stay on Internet Before and During Covid 19

Hours	Before COVID 19	During COVID 19	P value
≤ 5 hours	11.4	0	0.01*
1 – 5 hours	80	20	0.001**
5-14 hours	5.7	65.7	0.001**
≥ 14 hours	2.9	14.3	0.01*

51% visits the educational sites especially students because of the beginning of the online education in this period of time, 48% visit the sport sites every now and then (2-3 times per week), religious sites can be visited once per week in 38% of the participants.

Fig.3 shows the percent of exposure of the participants to the cybercrime before and during the pandemic, it reveals that there is highly significant difference between the exposure to these crimes

TABLE III
Sites Most Commonly Used by the Participant

Sites	Every day (Usually)	Frequently (2 to 3 times per week)	Infrequent (Once per week)	Rare (once per month or less)
Social media	87%	12%	1%	0%
Sport sites	1%	48%	35%	16%
Religious sites	0%	9%	38%	53%
TV series and films	23%	38%	34%	5%
Research sites	49%	32%	8%	11%
Shopping sites	12%	32%	25%	31%
E mail	78%	12%	8%	2%
Educational sites	51%	37%	8%	4%

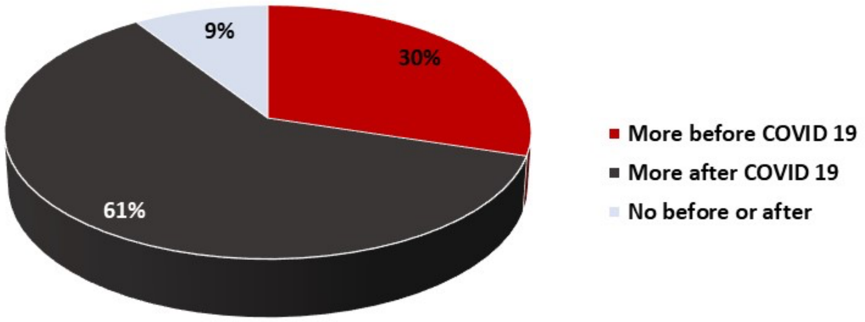

Fig. 3 Percent of exposure to cybercrime before and during COVID 19

before and during the pandemic.

Table IV reveals the different types of crime that the participants exposed to before and during the pandemic of COVID 19, most of these crimes were links to fake website 82%, received computer viruses and hackers 76% followed by claim to be another- persons with receiving messages from them 77%, and messages to request aid 70%. There was a highly significant increase in the crimes during the period of COVID 19 pandemic.

TABLE IV
Comparison of Online Victimization Before and After Covid 19

Types of crimes		Every day (Usually)		Frequently (2 to 3 times per week)		Infrequent (Once per week)		Rare (once per month or more than month)		P value
		Before COVID19	During COVID19	Before COVID19	During COVID19	Before COVID19	During COVID19	Before COVID19	During COVID19	
Claim to be another person	No.	152	308	124	76	44	16	80	0	0.01*
	%	38%	77%	31%	19%	11%	4%	20%	0%	
Steal your online account	No.	44	144	40	112	32	108	284	36	0.05
	%	11%	36%	10%	28%	8%	27%	71%	9%	
Links to fake website	No.	100	328	40	44	60	20	200	8	0.001**
	%	25%	82%	10%	11%	15%	5%	50%	2%	
Messages to request aid	No.	124	280	84	60	40	40	152	20	0.001**
	%	31%	70%	21%	15%	10%	10%	38%	5%	
Messages to request your bank account	No.	40	196	60	100	112	48	188	56	0.000**
	%	10%	49%	15%	25%	28%	12%	47%	14%	
Messages to request money	No.	44	176	116	112	152	84	88	28	0.001**
	%	11%	44%	29%	28%	38%	21%	22%	7%	
Received notification about stolen your password	No.	32	284	60	88	128	20	180	8	0.000**
	%	8%	71%	15%	22%	32%	5%	45%	2%	
Experienced unwanted sexual comments	No.	20	68	44	112	84	128	252	92	0.07
	%	5%	17%	11%	28%	21%	32%	63%	23%	
Received computer virus or hacker affected your work	No.	4	304	8	56	84	8	304	32	0.000**
	%	1%	76%	2%	14%	21%	2%	76%	8%	

V. Discussion

The COVID-19 outbreak has been announced as a pandemic by WHO, causing tremendous effects on organizations and individuals' lives. This work aimed to clarify the effects of COVID 19 spread on the cybercrime subsequent to expanding the work from home due to social distancing. The volunteers who shared in the study was 400, 58.7% of them were females and 41.3% were males. The number of volunteers ranged from 20 to 60 years with highest number of the volunteers was among those in the age group (30-≤40 years) followed by age group (40-≤ 50-year-old). The educational level of nearly half (46%) of the participants was master's degree or higher.

The lockdown measures expanded Internet traffic of residential clients, specifically, for telework, entertainment, business, and education. A study found that the traffic volume increased by nearly 15-20% within a week. Communication-related applications showed strong growth during working hours, with Europe demonstrating a pervasiveness for messaging and the US showing a pervasiveness for email [12]. The present work showed significant difference in stay time on the internet after the pandemic. Most of participants used social media (87%) and E mail (78%) on a daily basis. While nearly half of them visited research and education sites on daily basis.

With nearly all public gatherings canceled, individuals sought out entertainment and looked to connect with each other on web via streaming services and social media. The present work showed significant changes of time of stay on internet before and after COVID 19 with 87% of participants visited social media daily. People relied on social media to stay connected remotely with friends, and families to reduce effects of isolation. And, to consume the news, and to be entertained [13, 14].

Nearly half (48%) of participants in the current study visited sport sites frequently (2 to 3 times per week). To safeguard the health of athletes and others, most sporting events worldwide have been cancelled or postponed preventing the spread of Covid19. The Olympics and Paralympics, for the first time in the history of the modern games, have been postponed, to be held in 2021 [15]. There have been minimal live games to watch since March 2020. Some sport events were resumed behind closed [16].

One aspect of the lockdown is that places of worship have been temporarily shut. The pandemic has affected religious practice in a significant manner, including the cancellation of religious gatherings, including pilgrimages, festivals and celebrations [17]. This might result in a marked shift from public to private prayer. A few mosques and churches have offered online services through live streaming, radio and TV [18]. In the current results, 53% of the participants visited religious sites rarely (once per month or less).

The present data demonstrated that the largest percentage of participants (38%) watched online TV series and films frequently. With shutting of the cinema halls and suspension of film release amid the Covid19 pandemic, there was shift towards a new sort of watching experience through internet streaming services [17].

Regarding shopping sites, 32% of participants of the current survey visited online shopping sites from 2 to 3 times per week. Due to the COVID-19 pandemic, the international commerce and other activities have been interrupted. 52% of customers were reported to abstain from going physical shopping and crowded malls and shops. The global supply chain has been broken down due to the nearly worldwide lockdown. With the start of COVID-19, the e-commerce industry showed an exceptional expansion internationally. However, E-commerce in developing countries faces an absence of confidence and transparency, and people have a negative standpoint towards online shopping. In addition, the users of credit and debit card are few [19, 20].

With the spread of the pandemic and knowing more about the virus spread, a growing number of educational institutions have closed in regard to eye-to-eye classes [21]. This brought about a move from the ordinary learning process to electronic learning with an expanded number of online classes, conferences, meetings, and so on. Nearly half of the participants of the current survey visited research and education sites on a daily basis. Various countries have introduced several arrangements to carry forward the education system through introducing TV broadcast, Online libraries, assets, online channels, and video lectures [22].

The present data revealed significant change in the rate of online victimization before and after COVID 19. However, an American study demonstrated that the stay-at-home did not fundamentally modify cyber schedules, and cybervictimization did not increment either. Instead, worldwide levels of cybervictimization were nearly indistinguishable pre- and post-pandemic, and just one kind of victimization (stealing private data) changed. Moreover, this victimization decreased in the post-COVID-19 sample [2].

Of the cyber threats and violations that showed highly significant change after Covid19 in the present work; links to fake website, messages to request aid, messages to request bank account, messages to request money, stealing password, receiving computer virus or hacking. Social networking sites (SNSs), with their enormous number of users and huge database, appear to be ideal favorable place for abusing the weakness of individuals, who are considered the most fragile connection in security. Deceiving, convincing, or influencing individuals to provide data or to perform an activity that will profit the attacker [23]. In many cases, the fraudsters impersonate legitimate organizations, using similar names, websites and email addresses in their attempt to deceive unsuspecting individuals, even connecting through emails and social media messages [24]. For example, a fake corona virus medicalkit.com website alleged that the web site provides WHO-approved vaccine kits for COVID-19, users have been requested to enter their credit card details [25].

Sexual violence was facilitated by technology and online aggression against women has been reported since the early phases of internet development [26]. The relatively term of sexting can be interpreted as a practice of visually inappropriate behavior that includes the experience of sharing photographs, videos, pornography, texts through technological devices [27]. The present work did not show significant changes of the online sexual harassment after Covid19. There have been several speculations on the increase in cyberbullying incidents during COVID-19. An analysis indicated an increase in the cyberbullying conversation trend by Twitter users during COVID-19, which could conceivably be because of the pandemic's immediate effect [28]. In an Indonesian study and dependent on the experience of victims, social media in the form of Twitter was the primary means of providing a place for online sexual violence [29, 30].

VI. Conclusions

As mentioned before, the stay-at-home has radically altered the daily routines of millions globally with increasing teleworking. In addition, the use of social media sites such as Facebook, and Instagram are also spiking. The likelihood and impact of cyber-attacks increases as we become more technology dependent than ever, and the nature of the cyber threat changes with the current situation. Based on the results of the analysis, there was significant change of cyber habits and cyber security threats after the Covid-19 pandemic. Countermeasures must be undertaken to ensure improved security.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Authors declare that they have no conflict of interest.

References

[1] World Health Organization, "WHO Director-General's opening remarks at the media briefing on COVID-19," Mar. 11, 2020. [Online]. Available: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

[2] J. Hawdon, K. Parti, and T. Dearden, "Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment," *Am. J. Crim. Justice*, vol. 45, pp.

546-562, 2020, doi: 10.1007/s12103-020-09534-4.

[3] M. Baz, H. Alhakami, A. Agrawal, A. Baz, and A. Khan, "Impact of COVID-19 pandemic: a cybersecurity perspective," *Intell. Autom. Soft Comput.*, vol. 27, no. 3, pp. 641-652, 2021, doi: 10.32604/iasc.2021.015845.

[4] M. McGuire and S. Dowling, "Cyber dependent crimes," Home Office, United Kingdom, Research Report 75, Oct. 2013. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf

[5] UK's National Cyber Security Centre (NCSC) and the US' Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), "Advisory: COVID-19 Exploited by Malicious Cyber Actors," 2020. [Online]. Available: https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory. [Accessed: Oct. 15, 2020].

[6] H. He and L. Harris, "The impact of Covid-19 pandemic on corporate social responsibility and marketing philosophy," *Journal Bus. Res.*, vol. 116, pp. 176-182, 2020, doi: 10.1016/j.jbusres.2020.05.030.

[7] S. Hakak, W. Z. Khan, M. Imran, K. R. Choo, and M. Shoaib, "Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies," *IEEE Access*, vol. 8, pp. 124134-124144, 2020, doi: 10.1109/ACCESS.2020.3006172.

[8] H. S. Lallie, et al. "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic," *Comput. Secur.*, vol. 105, p. 102248, 2021, doi: 10.1016/j.cose.2021.102248.

[9] J. M. Alghazo and Z. kazimi, “Social Engineering in Phishing Attacks in the Eastern Province of Saudi Arabia,” *Asian J. Inf. Technol.*, vol. 12, no. 3, pp. 91-98, 2013, doi: 10.36478/ajit.2013.91.98.

[10] S. Gastellier-Prevost, G. Gonzalez Granadillo, and M. Laurent, "A Dual Approach to Detect Pharming Attacks at the Client-Side," in *2011 4th IFIP Int. Conf. New Technol. Mobil. Secur.,* Paris, 2011, pp. 1-5, doi: 10.1109/NTMS.2011.5721063.

[11] S. Schmeelk, K. Thakur, M. L. Ali, D. M. Dragos, A. Al-Hayajneh and B. R. Pramana, "Top Reported Data Security Risks in the Age of COVID-19," in *2021 IEEE 12th Annual Ubiquitous Comput. Electron. Mob. Commun. Conf. (UEMCON),* New York, USA, 2021, pp. 0204-0208, doi: 10.1109/UEMCON53757.2021.9666573.

[12] A. Feldmann, et al., "The Lockdown Effect: Implications of the COVID-19 Pandemic on Internet Traffic," in *Proc. Internet Meas. Conf. (IMC '20),* New York, NY, USA, Oct. 2020, pp. 1-18, doi: 10.1145/3419394.3423658.

[13] World Health Organization, "Mental health and psychosocial considerations during the COVID-19 outbreak," Mar. 18, 2020. [Online]. Available: https://www.who.int/docs/default-source/coronaviruse/mental-health-considerations.pdf [Accessed: Oct. 13, 2020].

[14] O. Király, et al., "Preventing problematic internet use during the COVID-19 pandemic: Consensus guidance," *Compr. Psychiatry,* vol. 100, p. 152180, 2020, doi: 10.1016/j.comppsych.2020.152180.

[15] A. Corsini, G. N. Bisciotti, C. Eirale, and P. Volpi, "Football Cannot Restart Soon during the COVID-19 Emergency! A Critical Perspective from the Italian Experience and a Call for Action," *Br. J. Sports Med.,* vol. 54, no. 20, pp. 1186-1187, 2020, doi: 10.1136/bjsports-2020-102306.

[16] M. Halle, *et al.*, "Exercise and sports after COVID-19—Guidance from a clinical perspective," *Transl. Sports Med.,* vol. 4, no. 3, pp. 310-318, 2021, doi: 10.1002/tsm2.247.

[17] M. Kumar, R. Khadia, and G. Awasya, "A Study: OTT Viewership in 'Lockdown' and Viewer's Dynamic Watching Experience," *Int. J. Transform. Media Journal. Mass Commun.,* vol. 5, no. 2, pp. 10-22, 2020.

[18] P. Rookes. (2020). Spirituality & the Covid-19 Pandemic [PowerPoint slides]. Available: https://www.spiritualitymentalhealth.org.uk/post/the-spiritual-adgenda-in-responding-to-covid-

[19] M. Neger and U. Burhan, "Factors Affecting Consumers' Internet Shopping Behavior During the COVID-19 Pandemic: Evidence from Bangladesh," *Chin. Bus. Rev.,* vol. 19, no. 3, pp. 91-104, 2020, doi: 10.17265/1537-1506/2020.03.003.

[20] A. Bhatti, H. Akram, H. Basit, A. Khan, S. Naqvi, and M. Bilal, "E-commerce trends during COVID-19 Pandemic," *Int. J. Future Gener. Commun. Netw.,* vol. 13, no. 2, pp. 1449-1452, 2020.

[21] W. Ali, "Online and Remote Learning in Higher Education Institutes: A Necessity in light of COVID-19 Pandemic," *High. Educ. Stud.,* vol. 10, no. 3, pp. 16-25, 2020.

[22] V. D. Soni, "Global Impact of E-learning during COVID 19," 2020. [Online]. Available: https://ssrn.com/abstract=3630073

[23] A. Algarni, Y. Xu and T. Chan, "Social Engineering in Social Networking Sites: The Art of Impersonation," in *2014 IEEE Int. Conf. Serv. Comput.,* Anchorage, AK, USA, 2014, pp. 797-804, doi: 10.1109/SCC.2014.108.

[24] C. Weerth, "INTERPOL on COVID-19: Urgent warning about COVID-19 fraud schemes & models," 2020. [Online]. Available: https://www.researchgate.net/publication/340363521

[25] N. A. Khan, S. N. Brohi, and N. Zaman, "Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic," *TechRxiv,* 12-May-2020 [Online]. Available: https://www.techrxiv.org/articles/preprint/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792/1

[26] N. Henry, A. Flynn, and A. Powell, "The Promise and Paradox of Justice," in *Rape Justice Beyond the Criminal Law,* in A. Powell, N. Henry, and A. Flynn, Eds., Hampshire, UK: Palgrave Macmillan, 2015, ch. 1, doi: 10.1057/9781137476159_1.

[27] D. M. Crimmins and K. C. Seigfried-Spellar, "Peer attachment, sexual experiences, and risky online behaviors as predictors of sexting behaviors among undergraduate students," *Comput. Hum. Behav.,* vol. 32, pp. 268-275, 2014, doi: 10.1016/j.chb.2013.12.012.

[28] S. Karmakar and S. Das, "Evaluating the Impact of COVID-19 on Cyberbullying through Bayesian Trend Analysis," in *Proc. Eur. Interdiscip. Cybersecur.* Conf. (EICC), France, Nov. 2020, doi: 10.1145/3424954.3424960.

[29] M. Jatmiko, M. Syukron, and Y. Mekarsari, "Covid-19, Harassment and Social Media: A Study of Gender-Based Violence Facilitated by Technology During the Pandemic," *J. Soc. Media,* vol. 4, no. 2, pp. 319-347, doi: 10.26740/jsm.v4n2.p319-347.

[30] "Cybercrime - prosecution guidance," 2019. [Online]. Available: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance [Accessed: Sep. 17, 2020].

[31] K. Zeb, O. Baig and M. K. Asif, "DDoS attacks and countermeasures in cyberspace," in *2015 2nd World Symp. Web Appl. Netw.* (WSWAN), Sousse, Tunisia, 2015, pp. 1-6, doi: 10.1109/WSWAN.2015.7210322.

[32] C. Breisinger, M. Raouf, M. Wiebelt, A. Kamaly, and M. Karara, "Impact of COVID-19 on the Egyptian economy: Economic sectors, jobs, and households," Int. Food Policy Res. Inst. (IFPRI), Washington, DC, USA, MENA Policy Note 6, 2020. [Online]. Available: https://www.ifpri.org/publication/impact-covid-19-egyptian-economy-economic-sectors-jobs-and-households#:~:text=The%20COVID%2D19%20crisis%20may,have%20declined%20by%208.7%20percent.

[33] T. Ahmad, "Coronavirus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity," in Proc. Available at SSRN 3568830, 2020.

[34] M. Alawida, A. E. Omolara, O. I. Abiodun, and M. Al-Rajab, "A Deeper Look into Cybersecurity Issues in the Wake of COVID-19: A Survey," J. King Saud Univ. Comput. Inf. Sci., vol. 34, no. 10, Part A, pp. 8176-8206, Nov. 2022, doi: 10.1016/j.jksuci.2022.08.003.

[35] I. Coman and I. C. Mihai, "The Impact of COVID-19. Cybercrime and Cyberthreats," Eur. Law Enforc. Res. Bull., SEC 5, pp. 61-67, 2021, doi: 10.7725/eulerb.v0iSCE%205.489