*Research Article*

# Social Media and Cybercrimes

**[a]Lama Almadhoor, [b]Faiz Alserhani, [c]Mamoona Humayun***

College of Computer and Information Sciences, Jouf University, Al-Jouf, Saudi Arabia

**Article History:** Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

**Abstract**

Users can communicate with each other by posting multimedia materials such as audio, text, photographs, video, animation, and graphics via a forum known as social media networking through a website or application medium. Despite its benefits, Social media has posed a huge risk in various fields such as strategic interests and national security that leads to adverse impacts. Cybercriminals have turned to social media as an outlet for carrying out their criminal actions. Computers and the internet are used in carrying out cybercrimes by stealing other people's identities as well as tracking down personal information and victims. There are several types of cyber-crimes. It is necessary to incorporate security measures and methods to control cyber-crimes. In this paper, we provide an overview of cybercrimes on social media. We will discuss common cybercrimes, their mitigation techniques, and protection in social media.

**Keywords:** Social media; cybercrimes; types of cybercrimes; preventive procedures;

## 1. Introduction

These days, social media forums are becoming part of a human lifestyle where millions of persons are using internet-based social media forums. Social media be a combination of apps and websites designed to enhance information sharing and online networking [1]. YouTube, Snapchat, Twitter, WeChat, Facebook, WhatsApp, and Instagram are some of the popular social media applications which are commonly in use across the globe as shown in Fig.1[46].

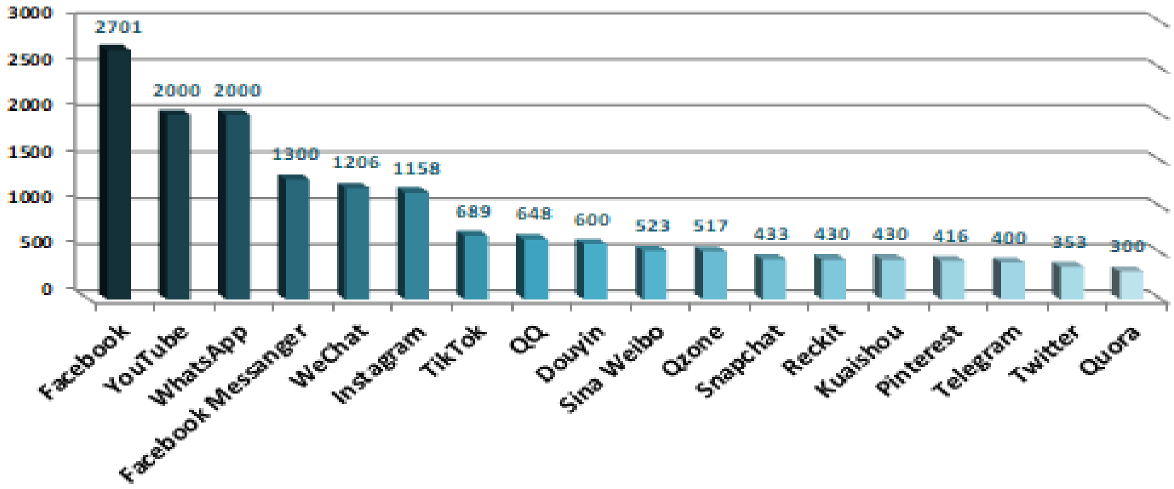

Fig.1. The world's most famous social networks as of July 2020

Users interact with each other and they also share multimedia materials such as graphics, pictures, video, texts, animations, and audio using social media. These large data content are presented in various forms of velocity, volume, veracity, variety, flexibility, discovery, accuracy, and dogmatism since they are big data hence cloud-based[2].

In March-2019, individuals using the internet arrive at 4,168,461,500 representing 50.08% of all the global populations [3]. In 2019, social media users were 2.77 billion across the world with 35.9 percent of worldwide social media platforms penetration. Overall, between 2019 and 2020, global social media audiences rose by 5.8%. These figures are expected to even go higher by 2021 with an estimation of 3.02 billion users [4] as shown in Fig.2.

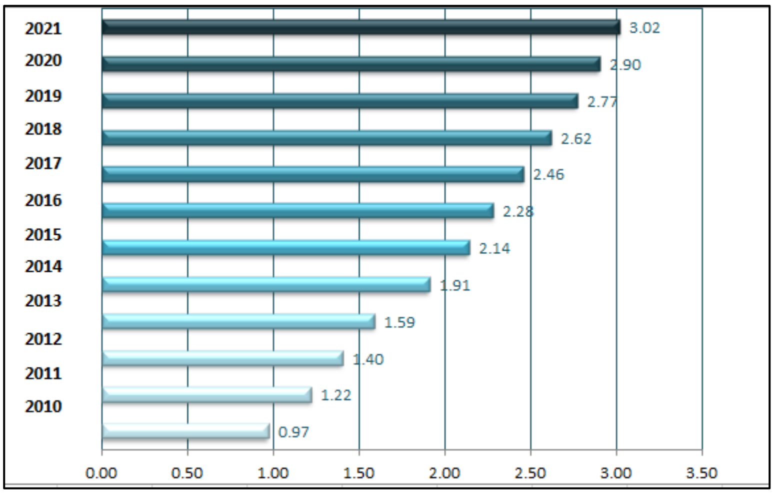

Fig.2. Amount of users of social media global from 2010 to 2021 (in billions)

Computers can either be used as a target or as a weapon in carrying out unlawful actions in cyber-crimes. generally, cybercrimes can be described as crimes involving credit card fraud, phishing, ban theft, industrial espionage, illegal downloading, scams, children trafficking, child pornography among others[5]. The enormous social media usage, strategic interests, and national security can have adverse effects[6]. Regrettably, Social Media has been the preferred outlet for cybercriminals to carry out their dirty actions. Cybercriminals permit social networking forum users to access their data, such as an address, gender, age, and telephone number. Social media offers a medium for cybercriminals to access other individual's personal information and use it to commit crimes[7, 8]. The numbers of cybercrimes are significantly on the rise due to the increased number of social media users which continue to grow tremendously each day. The hackers are targeting personal information that is misused by sending unauthorized messages termed as spam as well as stealing money from banks for victims' bank accounts [9].

In this paper, we provide an overview of cybercrimes on social media by providing various types of cybercrimes, then we highlight and focus on the most common types of cyber-crimes.

The paper is structured in the following sections: an introduction is explained in Section 1. Segment 2 provides a summary of the literature related to cybercrimes on social media. Segment 3 provides an overview of the subject. Section 4 provides different types of cybercrimes. Section 5 discuss and explains the most common types of cyber-crimes. Section 6 deals with the best preventive procedures and protection mechanisms for cybercrimes in social media, in section 7, we conclude the paper with the finding and discussion.

## 2. Literature Review

Social networking extends to online tools and websites that "facilitate user experiences to exchange information, opinions and interests" [10,11]. On the other hand, it has also indicated great potential as an innovative tool in monitoring events and functions[12].

The most popular applications for social networking forums are WhatsApp, WeChat, Facebook, Snapchat, Twitter, YouTube, Instagram, etc. When it comes to sharing images and videos (Instagram, YouTube), social networking (Facebook), or social networking platforms and micro-blogging (Twitter) have changed media systems, transforming production, consumption, and distribution patterns irrevocably[13].

Given the various literature related to Social media and cybercrimes that Social media forums have resulted in the most popular user's tools of communication which enable the sharing of data, personal information, personal images, messages, video calls, share thoughts. The prevalence of using social media for interaction between individuals, organizations, and governments raises new challenges involving privacy on social media, accessibility, protection, and other personal related issues[14].

In [42] Weulen and others saw that Cybercrimes affect life situations in both professional and private life. According to the opinions of some researchers in[43,44], Individuals who use social media are victims of harmful technologies, then as a solution, they put an approach for tracing social information that can result in cyber-attacks. In[45] the authors said that the Internet has seen cybercrime using techniques and conventional crime, all of which lead to 'safe-havens' for a criminal. Also, a criminal tries new types of crime because there exists little electronic communication by the community. Furthermore, techniques and recommendations are discussed and outlined by the authors for deterring cybercrime.

Despite the many benefits that social media offers internationally, The threats associated with social media need to be made aware of by individuals. cybercrimes is one of the most difficult challenges facing Social Media. This paper aims to provide maximum types of cybercrimes and the best protection mechanisms for these crimes.

## 3. Cyber Crimes Overview

A broad term that is used to define illegal activities carried out through computer networks or computer in which they are either used as a weapon, a target, or a location for criminal activity and include anything from electronic cracking to (DDOS) distributed denial of service attacks is called cybercrime. Additionally, cybercrimes involve the traditional crimes in which computer networks or computers are applied to enable facilitate activity[5]. These activities can range from pirated movie streaming to destabilization national economies. From phishing to highest crimes like cyber terrorism, this is the range of nonfinancial crimes [15]. In general, cybercrime is often characterized by the use of a computer and the Internet in a crime to steal an individual's identity, track victims, and data. As technology plays a critical part step by step in the life of an individual, cybercrime will increase with technological benefits [16].

Generally, more than half of worldwide internet users have ever undergone cybercrime. Based on the results of surveys in [47] a huge number of the user has fallen victim to cybercrime as shown in Fig.3

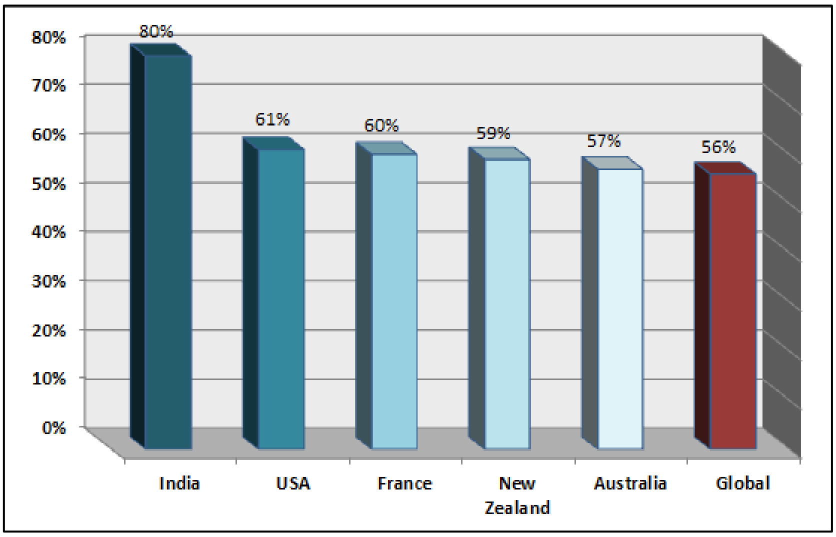

Fig.3. Percentage of internet users who have witnessed some cybercrime in 2019 in some countries

## 4. Type Of Cyber Crimes

There are several types of cyber-crimes. It can be divided into two groups as follows:

*4.1.* Traditional computer criminal activities that are made possible through computer systems usage[17] include:

- Spamming [5,15,17,20] .
- Hacking(Unauthorized access) [5,15,20] .
- Malware[5,15,17,20].
- Distributed Denial Of Service (DDOS) [15,16,17].
- Social engineering and phishing [15,45].
- Online Identity theft [5,15,20].
- Cyber-stalking [5,45,15,20].
- Cyber bulling [45,22] .
- Copyright infringement [17].
- File sharing through peer-to-peer networks [17].
- Email scams [17].
- Online gambling [17].
- Child soliciting and abuse [17,15,5].
- Frauds involving credit cards[45].
- Data breaches and cyber intrusion[45].
- Frauds involving Disaster[45,16].
- Botnets [15].

- Ransomware [15].
- Publication of Derogatory Materials[15].
- Laundering and Taxation trough E-money[15].
- Cyber Harassment[16].
- Cyber Terrorism [40].
- Industrial espionage [20].

*4.2.* National security cyber-crime perspective, include:

National security-critical areas include illegitimate interception of communications and industrial control systems, telecommunication networks, and hacktivism (a combination of activism and hacking)[17].

## 5. Most Common Types Of Cyber Crimes

The most popular online practice is social media networking. Social networking users now spend an average of 2 hours and 24 minutes per day on different networks [49]. Social networks have become the center of concern for offenders with this evolving nature of communication and they use it for their harmful purposes. Below we explain commonly occurring cyber threats

### *5.1.* Spamming

The cybercriminals may use social media forums to distribute illegal messages through the passage of wrong information normally via writing a message to individuals using social media[18]. Initially, spam was more common with emails but it has recently been common through social media forums. It occurred through the distribution of illegal messages that possess malicious links. By unwanted posting lots of links in the form of ads or personal messages via false identification, a spammer may direct unwanted bulk messages [19]. Targeted victims can receive harmful links from the attackers which upon clicking on the links the users are directed to other pages which leads to harmful consequences.

In January 2020, spam messages registered for 53.95 percent of e-mail flow. In reality, the global e-mail spam rate has dropped as seen in Fig.4 [48].

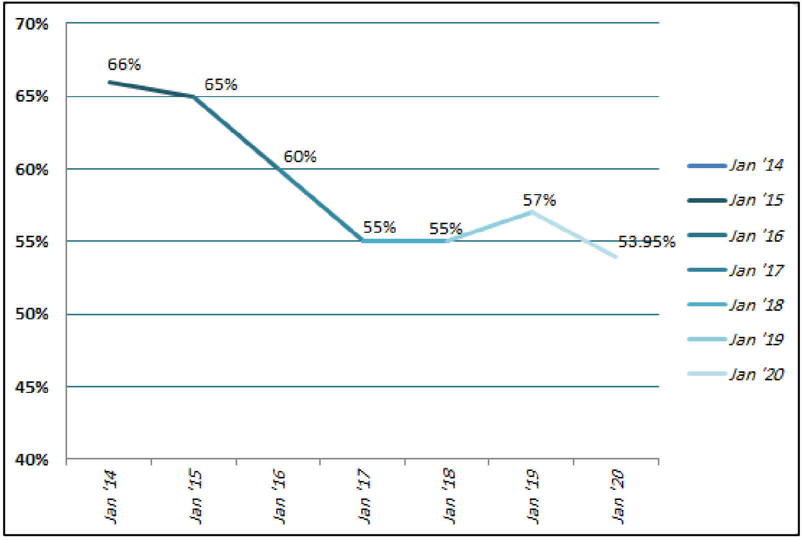

Fig.4. A percentage of total e-mail flow worldwide spam volume from January 2014 to January 2020

### *5.2.* Hacking

Illegal access to any digital devices or a computer done through various social media forums is called hacking. The hackers who normally are part of cybercriminals distribute messages to the individuals using social media. This occurs when the user clicks on those invalid links get hacked by criminals[20]. There are various methods that Cybercriminals can apply to gain access to the digital device of the targeted user.

The most common kind of attacks used by cyber-criminals is (1) opportunistic attack and (2) Targeted attack. In targeted attacks, specific tools are used by the criminals. On the other hand, in opportunistic attacks, the attackers use worms and viruses[20]. Generally, hackers, spammers, cyber-criminals carry out the targeted attacks through cybercrimes[21].

### *5.3.* Malware

Social networking forums media offers an excellent platform where malware and viruses are spread. Malware can be either malicious software or a threat developed to access social media users' information by prohibited access to social networking forums[22]. Sophos antivirus developer indicates that 40 percent of its members are victims of malicious software via social media sites[23]. In 2019, based on the Symantec ISTR, a substantial reduction can be seen in newly developed malware variants during the 2018 period, but Emotet a form of banking Trojan malware aggressively showed a great increase in its market share from 4 percent in 2017 to 16 percent in 2018 [24].

Malware attacks can harm the protection of organizational data security. In 2013, more than $1.6 billion was lost worldwide due to malware attacks[25].

For social networking sites, there are three forms of malware: Trojan, click-jacking, and cross-site scripting (XSS). In cross-site scripting, It can be used by criminals to distribute on social media sites malicious code to gather user data [22]. XSS is used against web applications, the attackers or cyber-criminals use this threat to hijack the account of a social network, steal cookies, attract users to download malware[18]. A Trojan is a worm containing secret code, used for stealing an individual's confidential information. On social media platforms, it is a very common malware threat. It is used as a fraud method for criminals to gather confidential SNS data and steal cash from bank accounts[26]. Another kind of social media malware is the Click-jacking worm. In click-jacking, the cyber-criminal creates a website aimed at luring social media users. Users who click on that link will have secret links that will redirect them to another page. Upon clicking on the links by the users, it appears on the wall of their friend's, and they often press on that page and become infected [27].

### *5.4.* Distributed Denial of Service attacks(DDOS)

Today, these attacks are very common. The growing speed of such threats has made network devices and internet servers more at risk than ever before. It is specifically used to disregard certain resources, such as an Internet server for users [28, 29]. The attacker has a massive effect on the target user in the (DDOS) attack by multiplying the attack power gained from a huge number of computer agents. For an attacker, it becomes feasible because before applying an attack, he takes numerous computer machines under his hold over the Internet [29].

To launch a DDOS attack using Facebook, the hacker creates malicious apps that incorporate URLs that relate to the webserver of the target, which points to documents that he hosts [30]. In such a case, Facebook™ is being used to execute the attack as an intermediary. Although Facebook users monitor their profile content by setting up the right privacy settings, criminals can still search for their private data by using Facebook™ apps without their approval[20].

### *5.5.* phishing and Social engineering

Phishing is a popular web danger whereby the attackers develop as well as regulates a fake website that resembles the genuine ones. This is usually among the first option among cybercriminals and they used that in carrying out different crimes like espionage, used to gain individual's data like password, user name, credit card details, and bank details, cyber-bullying, and illegal activities[20].

In attacks constituting phishing, victims are drawn to press on the pages affected, which can then spread the danger between victims[31]. Making a bank like a page or Facebook is the most common method of phishing[32]. According to internet security threat reports (ISTR) in 2018, the number of phishing is diminishing, but malicious emails have risen from 43 percent in 2017 to 48 percent in 2018[24, 33].

### *5.6.* Identity Theft Online

Theft that entailing to define fraud identity online is the most prevalent cyber-crime. According to researchers identity theft can be described as a try to access an individual's data for illegal activity [34]. Without the individual's consent to fraud or steal the money, it is used to steal another's identity. A stolen identity is used by criminals to procure illicit goods, illegal acts, etc. [21]. For the year 2016, the annual summary of consumer complaints by the Federal Trade Commission ( FTC) had a total of 399 225 complaints hence classified identity theft in the third position[35]. In 2018, The FTC Announced that identity theft comes top third complaint, 444,602 records out of 3 million records are the total number of identity fraud reports and the average number of identity theft incidents risen by 11.3 percent in 2018[36].

### *5.7.* Cyber-Stalking

Cyber-Stalking is taken as the use of the Internet and other imaginative technologies in deliberate and hostile ways to harm others. It may also use email threats that contain offensive materials such as nude photographs, videos showing abuse or obscenity, and posting nasty comments that may also be used[20] and may cause the victim to feel annoyed, violated, and emotionally anxious[45].

Receiving unwelcome phone calls, voicemails, and text messages are the most commonly learned stalking technique for both male and female victims[23].

## 6. Preventive Procedures And Protection Mechanisms For Cyber Crimes In Social Media

Technological advancements can also be applied to manage, deter, protect, and prosecute crime in the same way that a criminal uses social media to commit a crime. offenders, on the one side, social media sites can scan for their possible targets; law enforcement authorities can also use similar media to press charges against the perpetrators[37]. For example, it is normal to use social media in arresting the city's most wanted criminals by the Toronto police[38]. Duncan Smeed, George R. S. Weir, and Fergus Toolan suggested that all users of social media whether as individuals and businessmen should be vigilant and careful with the posting of personal data that can be used by criminals against them [37].

It is necessary to incorporate security measures, some methods that should be used for controlling cyber-crimes include; keep all software up-to-date, know your friends well, using current antivirus software, learn basic security measures, never provide sensitive information, and use passwords that are protected and distinguished[39]. Also, the author addresses security managers, security issues, and network that often turn to network policy management services like antivirus, firewall, anti-malware, perfusion framework spam filter, intrusion, and anti-virus software to avoid attacks and take the appropriate reaction [40, 41]. It is important to solve security matters, a system for protecting data from social media attacks.

## 7. Finding And Discussion

After we explained the cybercrimes on social media, and the safeguards that can be taken to prevent and protect social media from these cybercrimes. This segment address the Evaluation of cybercrimes concerning social media and their countermeasures. The common cybercrimes and possible protection measures to prevent them are compiled in **Table 1**.

Table.1. Recommendations and techniques for prevention from cybercrime

| Cyber Crime | Recommendations and techniques for prevention |
|---|---|
| Spamming | • Spam filter[40,18].<br>• Algorithms for detecting various types of spammers[22].<br>• Internal Protection Mechanisms[22].<br>• Test the "Completely Automated Public Turing Computers and Humans Apart" (CAPTCHA) [29].<br>• Empowering verification [26]. |
| Hacking | • Empowering authentication[26].<br>• Providing suitable security tools[26].<br>• Firewalls [16].<br>• Anti-virus software[16]. |
| Malware | • Anti-malware, and anti-virus tools[26,40].<br>• A list of anti-threat strategies [44].<br>• Antivirus Gateway[33].<br>• IPS Interruption recognition or protection systems[33].<br>• solutions provided based web security gateway throughout the network[33].<br>• The full protection stack helps to protect against threats concerning emails [33].<br>• Firewalls [33.26].<br>• An email security application[28].<br>• Not click the suspicious messages[18].<br>• Be vigilant while uploading important information[18].<br>• Mount patches[18].<br>• SQL injection and XSS programs should be carefully installed to prevent attacks[18]. |

| | |
|---|---|
| | • Filter suspicious links[18].<br>• Defense web service[22].<br>• Detection of signature-based malware[45].<br>• Detection of Anomaly-based malware[45].<br>• API/system calls, N-grams, hybrid features and assembly instructions used techniques[45].<br>• Individual's vigilance [45]. |
| Distributed Denial of Service attacks | • Test the "Completely Automated Public Turing Computers and Humans Apart" (CAPTCHA) [29].<br>• Egress/ Ingress Filtering techniques [29].<br>• Methodology of D-WARD [29].<br>• Technique Hop Count Filtering (HCF) [29].<br>• Technique of SYN Cookies [29]. |
| phishing and Social engineering | • Awareness should be increased and training through education of the society regarding cybercrime and more specifically phishing[15,25].<br>• Applying economic analyses [25].<br>• Social media users should remain extra careful against strangers and should therefore avoid visiting suspicious links and pages[18].<br>• Facebook Phishing Protector: is a Firefox add-on This add-on provides protection against various phishing attacks[22].<br>• Phishing Detection: for phishing websites and phishing urls[22].<br>• Get rid Installed Third-Party Applications. This issues are unknown to many[22].<br>• Personal data is frequently collected through users, third-party applications[22].<br>• Anti-phishing software[15].<br>• One Time Password (OTP) [45].<br>• CAPTCHA[45].<br>• Digital certificates[45].<br>• Using anti-phishing algorithms focused on genetics and attributes [45].<br>• Techniques such as Neural network, algorithm C4.5, and IREP. [45]. |
| Online Identity Theft | • Biometrics[45].<br>• Three Factor Authentication (3FA) [45].<br>• Techniques such as algorithms for SD and CD, a secret model of Markov, outlier identification, logistic regression, and genetic algorithm [45].<br>• Anti-identity theft applications, such as Life Lock by Symantec[45].<br>• Avoid sharing any personal information to strangers by e-mail or when speaking[5,16].<br>• Don't put an amount of personal information online [6,18,26]<br>• Using methods for authentication like: CAPTCHA, Multi-Factor Authentication (MFA), Identification of images-of-friends, and also requiring the user in certain cases to request a copy of his or her government-issued ID [22]. |
| Cyber-Stalking | • Blocking and reporting to authorities against cyber-stalkers [45].<br>• Track the OSN behaviors of your children. It is possible to do this monitoring manually or by using one of the monitoring software products[22].<br>• Collect and record as much proof as you can [45].<br>• Techniques: text mining, association rule mining, a detection system for cyber-stalking, and signature-based data mining [45].<br>• Avoid revealing any self-related information. As the disclosure of your identity in public places to strangers [5]. |

But despite all these solutions, social media still faces problems that cannot deal with all types of crimes, so it cannot reach a high level of security, without a doubt, there remains the need for further studies to improve the security of social media. Also, further research could be conducted to make these protection countermeasures more effective in social media.

## 8. Conclusion

We concluded that social media is an online tool that "facilitates interactions between users to share data, interests, and opinions". With the increasing number of social network users, the number of incidents carried out by criminals to access private data is also growing. There is a need to provide detailed awareness to the social media users about the various types of prevailing attacks. To fill this gap, this paper has synthesized existing cybercrimes along with their mitigation techniques. This will help social media users in a better understanding of the crimes and the awareness about the ways of protecting themselves from these attacks.

**References**

1. A. Power, "What is social media?," British Journal of Midwifery, vol. 22, pp. 896-897, 2014.
2. Mamoona Humayun., “Role of Emerging IoT Big Data and Cloud Computing for Real Time Application”,International Journal of Advanced Computer Science and Applications 11(4), 2020Internetlivestats.com, “Internet Users,” Internet Live Stats, 2019.
3. S. Inc., “Number of social media users worldwide from 2010 to 2021 (in billions),” Statista: The Statistics Portal, New York, 2019.
4. Gupta, S., et al. "Impact of cyber crime on adolescents through social networking sites." International Journal of Law 3.6 (2012): 104-7.
5. J.K. Kimutai. “Social. Media and National Security Threats: A Case Study of Kenya”, http://www.erepository.uonbi.ac. ke/ bitstream/handle /11295/76667/ Kimutai_Social%20 Medi %20And%20 National%20Security%20Threats%20A%2 0 Case%20 Study%20Of%20Kenya.pdf? sequence=4,2014
6. K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," Journal of Information Security and Applications, vol. 22, pp. 113-122, 6// 2015.
7. N. Al Mutawa, I. Baggili, and A. Marrington, "Forensic analysis of social networking applications on mobile devices," Digital Investigation, vol. 9, Supplement, pp. S24-S33, 8// 2012.
8. Humayun, M., Jhanjhi, N., Alruwaili, M., Amalathas, S.S., Balasubramanian, V. and Selvaraj, B., 2020. Privacy Protection and Energy Optimization for 5G-Aided Industrial Internet of Things. IEEE Access, 8, pp.183665-183677..
9. Khan, G. F. (2012). Social media for government. Berlin, Germany: Springer.
10. Khan, G. F., Swar, B., Lee, S. K. (2014). Social media risks and benefits: A public sector perspective. Social Science Computer Review, 32, 606–627.
11. Kalampokis, E., Tambouris, E., Tarabanis, K. (2013). Understanding the predictive power of social media. Internet Research, 23, 544–559.
12. Hamid, Bushra, Nz Jhanjhi, Mamoona Humayun, Azeem Khan, and Ahmed Alsayat. "Cyber Security Issues and Challenges for Smart Cities: A survey." In 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), pp. 1-7. IEEE, 2019.
13. J. C. Bertot, P. T. Jaeger, and D. Hansen, "The impact of polices on government social media usage: Issues, challenges, and recommendations," Government information quarterly, vol. 29, pp. 3040, 2012.
14. Munir, Asad, and Ghulam Shabir. "Social Media and Cyber Crimes in Pakistan: Facts, Propaganda, Awareness, and Legislation."
15. Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, 1-19.
16. Zain A.M., Saberi N.E., Jaafar F., Fauzi F.H.A., Ramli W.N.R.W., Lugiman F.A. (2015) Social Media and Cyber Crime in Malaysia. In: Hassan O., Abidin S., Legino R., Anwar R., Kamaruzaman M. (eds) International Colloquium of Art and Design Education Research (i-CADER 2014). Springer, Singapore. https://doi.org/10.1007/978-981-287-332-3_53
17. W. Luo, J. Liu, J. Liu, and C. Fan, "An Analysis of Security in Social Networks," in Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference on, 2009, pp. 648-651.
18. M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, "Towards Automating Social Engineering Using Social Networking Sites," in Computational Science and Engineering, 2009. CSE '09. International Conference on, 2009, pp. 117-124.
19. Patel, Poonam, et al. "A theoretical review of social media usage by cyber-criminals." 2017 International Conference on Computer Communication and Informatics (ICCCI). IEEE, 2017.
20. Alferidah, Dhuha Khalid, and N. Z. Jhanjhi. "A Review on Security and Privacy Issues and Challenges in Internet of Things." International Journal of Computer Science and Network Security IJCSNS 20, no. 4 (2020): 263-286.
21. M. Fire, R. Goldschmidt, and Y. Elovici, "Online Social Networks: Threats and Solutions," IEEE Communications Surveys & Tutorials, vol. 16, pp. 2019-2036, 2014.
22. NW3C, “Criminal Use of Social Media (2013),” NW3C, 2013.

23. Symantec, “Internet Security Threat Report,” Symantec Corporation, 2019.
24. Ubing, A. A., Jasmi, S. K. B., Abdullah, A., Jhanjhi, N. Z., & Supramaniam, M. (2019). Phishing website detection: An improved accuracy through feature selection and ensemble learning. International Journal of Advanced Computer Science and Applications (IJACSA), 10(1).
25. M. Omar Saeed Al, "Threats and Anti-threats Strategies for Social Networking Websites," International Journal of Computer Networks & Communications, vol. 5, pp. 53-61, 2013.
26. M. R. Faghani, A. Matrawy, and C. H. Lung, "A Study of Trojan Propagation in Online Social Networks," in 2012 5th International Conference on New Technologies, Mobility and Security (NTMS), 2012, pp. 1-5.
27. Alferidah, Dhuha Khalid, and N. Z. Jhanjhi. "Cybersecurity Impact over Bigdata and IoT Growth." In 2020 International Conference on Computational Intelligence (ICCI), pp. 103-108. IEEE, 2020.
28. M. AAMIR and M. A. ZAIDI, “A Survey on DDoS Attack and Defense Strategies: From Traditional Schemes to Current Techniques,” Interdiscip. Inf. Sci., vol. 19, no. 2, pp. 173–200, 2013.
29. A. Makridakis, E. Athanasopoulos, S. Antonatos, D. Antoniades, S. Ioannidis, and E. P. Markatos, "Understanding the behavior of malicious applications in social networks," IEEE network, vol. 24, pp. 14-19, 2010.
30. A. Cleeff, R. Wieringa, v. P. Eck, and V. N. L. Franqueira, "Engineering security agreements against external insider threat," Information resources management journal, vol. 26, pp. 66-91, 2013.
31. M. Sauter, “Nine Major Ways Criminals Use Facebook,” Fox Business, 2012.
32. B. Nahorney, “Internet Security Threat Report (2017),” ISTR, 2017.
33. M. Dadkhah, M. Lagzian and G. Borchardt, “Identity Theft in the Academic World Leads to Junk,” Science and Engineering Ethics, vol. 24, no. 1, pp. 287–290, 2018. https://doi.org/10.1007/s11948-0169867-x
34. FTC, “FTC Releases Annual Summary of Consumer Complaints (2017),” FTC, 2017.
35. F. T. Commission, “Consumer Sentinel Network Data Book 2018,” Commission, Federal Trade, 2019.
36. G. R. Weir, F. Toolan and D. Smeed, “The threats of social networking: Old wine in new bottles?,” Information Security Technical Report, vol. 16, no. 2, pp. 38–43, 2011. https://doi.org/10.1016/j.istr.2011.09.008
37. R. D'Amore, “Toronto police tap into power of social media to catch city's most wanted criminals,” CTV News Toronto, 2018.
38. Preparisi, Social Media Threats. Https://Www.Americanbar.Org/Content/D am/Aba/ Events/State_Local_Government/2017/Ho meland-Security/Social-Media-Threats Checklist. Pdf, 2017
39. Parlakkılıç, Alaattin. "Cyber Terrorism Through Social Media: A Categorical Based Preventive Approach." International Journal of Information Security Science 7.4 (2018): 172-178.
40. Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic.
41. Weulen Kranenbarg M, Ruiter S, van Gelder JL, Bernasco W. Cyber-Offending and Traditional Offending over the Life-Course: an Empirical Comparison. J Dev Life Course Criminol. 2018;4(3):343-364. doi:10.1007/s40865-018-0087-8
42. Kirwan GH, Fullwood C, Rooney B. Risk Factors for Social Networking Site Scam Victimization Among Malaysian Students. Cyberpsychol Behav Soc Netw. 2018;21(2):123-128. doi:10.1089/cyber.2016.0714
43. Hernandez-Suarez A, Sanchez-Perez G, Toscano-Medina K, et al. Social Sentiment Sensor in Twitter for Predicting Cyber-Attacks Using $\ell_1$ Regularization. Sensors (Basel). 2018;18(5):1380. Published 2018 Apr 29. doi:10.3390/s18051380
44. Soomro, Tariq & Hussain, Mumtaz. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. Applied Computer Systems. 24. 9-17. 10.2478/acss-2019-0002.
45. J. Clement, "Most popular social networks worldwide as of July 2020, ranked by number of active users(in millions)," 29 Oct 2020. [Online]. Available: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.
46. J. Clement, "Percentage of internet users in selected countries who have ever experienced any cyber crime as of December 2019," Statista, 28 May 2020. [Online]. Available: https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/.
47. J. Clement, "Global spam volume as percentage of total e-mail traffic from January 2014 to March 2020, by month," Statista, 24 Jun 2020. [Online]. Available: https://www.statista.com/statistics/420391/spam-email-traffic-share/.

48. Ponnusamy, V., Jhanjhi, N. Z., & Humayun, M. (2020). Fostering Public-Private Partnership: Between Governments and Technologists in Developing National Cybersecurity Framework. In Employing Recent Technologies for Improved Digital Governance (pp. 237-255). IGI Global.