Applied Computer Systems

ISSN 2255-8691 (online)
ISSN 2255-8683 (print)
May 2019, vol. 24, no. 1, pp. 9–17
https://doi.org/10.2478/acss-2019-0002
https://content.sciendo.com

Social Media-Related Cybercrimes and Techniques for Their Prevention

Tariq Rahim Soomro[1*], Mumtaz Hussain[2]
[1] *College of Computer Science & Information Systems, Institute of Business Management, Karachi, Pakistan*
[2] *Freelance programmer, Karachi, Pakistan*

Abstract – **Since a past decade, social media networking has become an essential part of everyone's life affecting cultural, economic and social life of the people. According to internetlivestats.com, in March 2019 the Internet users reached 4 168 461 500, i.e., 50.08 % penetration of world population. According to Statista, in 2019 there are 2.22 billion social media networking users worldwide, i.e., 31 % of global social media networking penetration and it is expected that in 2021 this number will reach 3.02 billion. These social networking sites are attracting users from all walks of life and keeping these users' data in the cloud. Today's big challenge is related to an increase in volume, velocity, variety and veracity of data in social media networking, and this leads to creating several concerns, including privacy and security; on the other hand, it also proves as a tool to prevent and investigate cybercrime, if intelligently and smartly handled. The law enforcement agencies are putting their utmost efforts to prevent cybercrime by monitoring communications activities over the Internet. In this paper, the authors discuss recommendations and techniques for preventing cybercrime.**

Keywords – **Cybercrime, cybersecurity, social media.**

I. Introduction

Social media is affecting cultural, economic and social life of the people, and it has become an essential part of everyone's life. Social media networking is a platform that enables users to participate and share multimedia content, for example, text, audio, video, images, graphs and animations through a medium of a website or an application. These contents are cloud-based big data contents and can be viewed in the form of volume, variety, velocity, veracity, volatility, quality, discovery and dogmatism [1]. According to [2], in March 2019 the number of Internet users reached 4 168 461 500, i.e., 50.08 % penetration of world population. According to [3], in 2019 there are 2.77 billion social media networking users worldwide, i.e., 35.9 % of global social media networking penetration and it is expected that in 2021 this number will reach 3.02 billion. These users are of different age group, different cultures, different religions, different social attitude, behaviors, and they use different devices to connect to the social media sites. Keeping in view the popularity of these networking sites, users of all kinds are attracted to these social media sites to meet friends and family, to share their daily routine with the loved ones and find new acquaintances. These social networking sites are attracting users from all walks of life and keeping these users data in the cloud [4]. The way we started living in the online world today is changing the way regarding our privacy and security. Today's big challenge is related to an increase in volume, velocity, variety and veracity of data in social media networking, and this leads to creating several concerned, including privacy and security; on the other hand, it also proves as a tool to prevent and investigate crime, if intelligently and smartly handled. The current era is the era of information and information is everywhere and today there are several ways people are communicating and sharing information through Twitter, Facebook, and other social media tools, through blogs, content sharing, for example, images and videos, as well as through mobile messaging.

According to [5], in 2000 'Love Bug' computer worm infected rapidly computers worldwide and damage was between 7 billion USD to 10 billion USD. In 2004, 35-year-old musician from the UK murdered 31-year-old school teacher, as he was obsessed with sexual images, which he viewed just hours before the murder. In 2011, urban disturbances spread across numerous English cities; it was believed that new social media had been used by participants as a means of disseminating information about incident in real time and as social coordination to facilitate riots. These are a few crime examples, which have been seen recently in the new form of electronic communications. The rapid connectivity has opened up the opportunities for criminals to exploit security vulnerabilities on the Internet. Cybercrime as well as traditional crime has been seen on the Internet. This leads to 'safe havens' for a criminal in early era as new crime forms are being explored by a criminal, and there is less awareness by the community using the electronic communications [6]. Social media is today's medium for community communications as well as for all sorts of Internet-based crime. This social big data, for examples, tweets, blogs, chat messages, including SMS and phone calls can be used in real time to prevent crime or to be used offline to investigate the crime. Social media is not only communication medium for community, but also a medium for criminal community as the response time on this medium is very fast (real time). Currently social media is also becoming the medium for law enforcement agencies to prevent crime. The law enforcement agencies are putting their utmost efforts to prevent crime [7] by monitoring communications activities over the Internet, but there are several challenges they are struggling with, for example, big data challenges [1], cloud challenges [4], real time monitoring challenges, for example, privacy concerns, unstructured text monitoring challenges, multi-lingual text monitoring challenges, multiple website monitoring challenges,

[*] Corresponding author's e-mail: tariq.soomro@iobm.edu.pk

anonymous identifications as in some cases secured communication is going on and many more [8]. Other than these text related challenges, image monitoring, audio and video monitoring etc. are also the important challenges.

Peaceful community and peaceful world are the dreams of every country, every human and every researcher, but if there is a community, there is also a possibility of crime. Crime is changing its shape from traditional to electronics. Use of social media is growing on the one hand and the crime using electronic medium is also growing on the other hand. Criminals are using this quick response real time social media to plan, execute or commit the crime, and law enforcement agencies are using the same social media to control, prevent, protect and investigate the crime. This paper is organised as follows: Section 2 explores social media and cybercrime; Section 3 discusses preventive measures; Section 4 presents a summary of research findings, and finally conclusions and the future research areas are discussed.

II. Social Media and Cybercrime

According to “Criminal Use of Social Media” white paper from the National White Collar Crime Centre (NW3C) [9], social media has been on rise in past several years, which changes the communicational landscape. Social media sites, such as Facebook, Twitter, and YouTube, have millions of active users. Using these websites, people communicate instantaneously with each other with convenience. Social media sites are used by people to communicate with each other, and by the public sector for advertisement and recruitment of new employees. Statista’s data on social media users as of January 2019 are shown in Fig. 1.

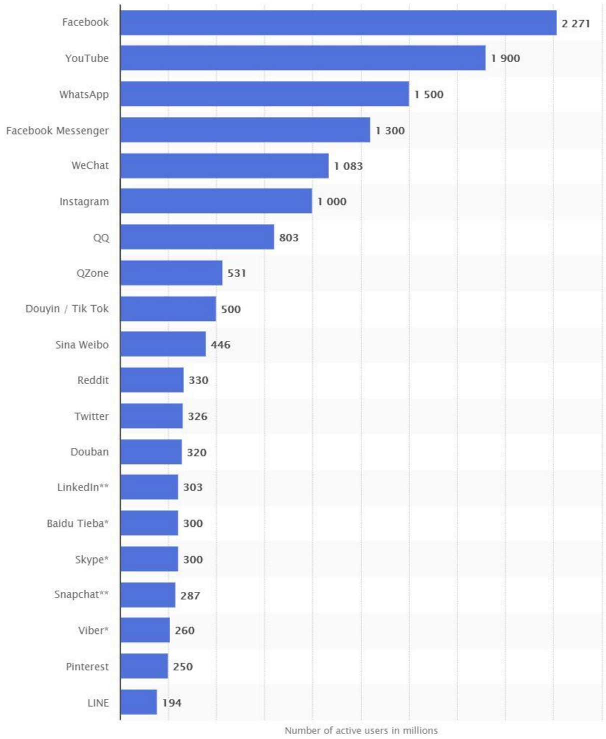

Fig. 1. Social media users as of January 2019 (Source: [3]).

According to the report of NW3C [9], social media networking is the most popular online activity; the Internet PC users are spending more than 12 minutes on social media networking out of 1 hour, while mobile Internet users are spending more than 18 minutes on social media networking out of 1-hour usage. With this changing nature of communication, criminals are using social media websites for their own malevolent motives. The report of NW3C discussed six crime types using social media [9]:

1) Burglary via social networking;
2) Social engineering and phishing;
3) Malware;
4) Identity theft;
5) Cyber-stalking;
6) Cyber-casing.

A. Burglary via Social Networking

Here criminals search social media for a potential target for burglary. Social media users usually post their personal activities, for example, they are having dinner or going somewhere for vacations. Criminals look for this type of information to find easy targets, where they find large time frame to burgle the property [9]. According to BBC report, robbery of 10 million USD worth jewellery from Kim Kardashian last year is the prominent example of this type of crime. She was robbed in Paris at gunpoint before returning to New York. According to the BBC report, French police suspected that criminals got aware of Mrs. Kardashian million-dollar procession after she posted picture on Twitter just three days before the robbery happened [10].

B. Social Engineering and Phishing

Social engineering uses psychological manipulation to get personal information [9]. People using social networking sites receive messages from their friends requesting immediate financial assistance. Actually, these messages were not sent by their friends, but by the criminal who stole their friends’ emails and passwords. Due to its ease in nature, the computer security firm Trend Micro calls Facebook a “minefield of scams” [9]. Symantec Corporation’s article describes phishing as one of many techniques of social engineering [11]. Cybercriminals make use of various methods to get potential target information by social engineering tricks and tactics. Phishing emails might look like from the boss asking employees login credentials or from the bank of the individual. Cybercriminals make sure of making their target scared so that they do as instructed rather than think rationally [11]. Criminal using this technique sends millions of emails in hope of receiving useful information. The most common form of phishing is to make a Facebook or Bank like page [12]. The rate of phishing is decreasing, but an increase in malicious emails from 43 % in 2017 to 48 % in 2018 was reported by the Internet Security Threat Report (ISTR) in 2018. Its statistics is shown in Fig. 2 for ready reference [13], [14].

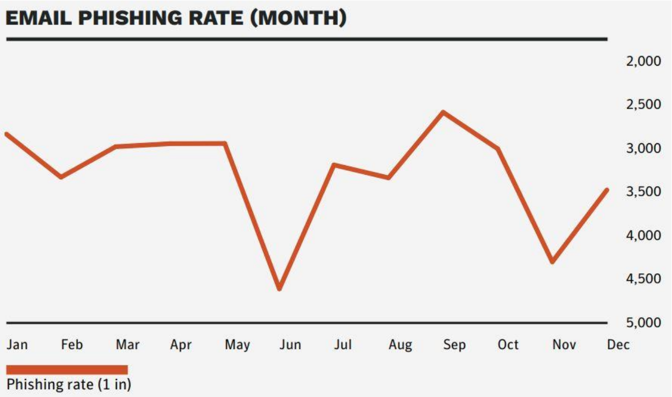

Fig. 2. Phishing rate during 2018 (Source: [14]).

C. Malware

Social media provides a great platform for spreading viruses and malware. Developers of adware, malware and viruses hide their destructive programs in links, attachments and messages, which are a normal task in any social networking website. Once users respond to them, the malware infects their computer without their knowledge. According to the developer of Sophos antivirus, victims of malware through social media are 40 % of its users. Microsoft reported that 19 million PCs were found infected by a rogue virus. Furthermore, business community considers their use of social media by their employees as a network security risk. Sophos conducted a survey from more than 500 companies and 70 % of them were concern about their network security due to use of social media by their employees [9]. According to the Symantec ISTR 2019 [14], a significant decrease can be observed in new malware variants in 2018, but a type of banking Trojan malware, called Emotet, aggressively increased its market share from 4 % in 2017 to 16 % in 2018. The statistics of new variants in last 3 years are shown in Table I.

TABLE I
MALWARE GROWTH 2016–2018 (SOURCE: [14])

Year	New Variants	Percent Change
2016	357,019,453	0.5
2017	669,947,865	87.7
2018	246,002,762	−63.3

D. Identity Theft

Researchers in [15] describe identity theft as an attempt of getting personal information of an individual for a criminal activity. Research perceives identity theft as the intentional use of personal information of victim, without any legal authority, with criminal intentions [16]. According to the Internet Crime Report 2016 of the FBI's Internet Crime Complaint Centre's (IC3), identity theft was ranked seventh with 16 878 victims, and loss of 58 917 398 USD [17] was recorded only in the USA. As per Internet Crime Report 2017 [18], identity theft was the sixth biggest complaint with 17 636 victims and loss of 66 815 298 USD only in the USA in 2017 [18]. This clearly shows an increase in total number of victims and overall loss in dollars comparing it from the report of previous year. The Federal Trade Commission's (FTC) annual summary of consumer complaints, for the year 2016, ranked identity theft third with a total of 399 225 complaints [19]. In 2017, the FTC received a total of 2.7 million complaints of fraud, and identity theft was ranked second highest with 371 061 complaints [20]. The identity theft became top third complaint to the FTC in 2018, and the total number of identity theft complaints was 444 602 out of 3 million reports. Despite losing the ranking, the total number of identity theft complaints had increased by 11.3 % in 2018. Figure 3 shows the statistics from the Consumer Sentinel Network Data Book 2018 [21].

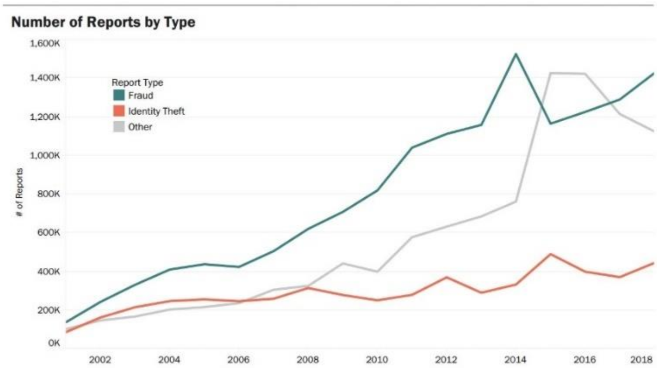

Fig. 3. Identity theft complaints from 2002 to 2018 (Source: [21]).

E. Cyber-Stalking

The stalking inside the cyber world by using the social media or any other online medium, which may cause feelings of irritation, abuse and emotionally anxiety to the victim, is cyber-stalking [22]. The report on cyber-stalking by NW3C [22] further stresses the intentional motives of cyber-stalker by differentiating it with identity theft. The report states that identity thieves are not concerned with the effects of their actions on victim, while cyber-stalkers are well aware and do it deliberately. According to Alexis A. Moore [23], in the USA one woman out of twelve and one man out of forty-five will be stalked in their lifetime. Moore's article reflected upon the fact that female of ages between 18 and 29 are mainly the victims of cyber-stalking, but females in general are not always the target. A survey at the University of Pennsylvania shows that 56 % of cyber-stalking victims are male. According to the Bureau of Justice Statistics (BJS) [24], every 14 out of 1000 persons at the age of 18 are victims of stalking and around 1 out of 4 victims complaints about some sort of cyber-stalking in form of e-mail and instant messaging. According to [25], one out of ten Americans has experience of online harassment and 7 % of American adults have faced cyber-stalking.

F. Cyber-Casing

The Report on Criminal Use of Social Media by the National White Collar Crime Centre [9] explains cyber-casing as a process, which is used to produce real world location using various data available in online resources. One of the prominent features that social media sites have offered in recent years is geo-tagging [9]. With widespread use of mobile applications, geo-tagging is a major trend of social media sites [26]. Mobile applications have played a vital role in promotion of this trend without any legal purpose [26]. Geographical information is the prime element in the process of cyber-casing, which helps criminals plan and execute their mischievous plans [26].

Apart from the above-mentioned crime types, the National White Collar Crime Centre also published a separate report for each new emerging crime. The list of social media related crime:

1) Credit card fraud;
2) Cyber intrusion and data breaches;
3) Disaster fraud.

G. Credit Card Fraud

A credit card or debit card fraud is a type of identity theft in which an unauthorized person uses someone's credit card information for withdrawing cash from it or makes purchases [27]. Criminals can use the Internet for credit card fraud or do it in-person. This unauthorized use can be done in various ways, using lost or stolen card, account takeover by reporting card lost or stolen after getting sufficient information, and by skimming, which involves an electronic attachment that appears valid such as a self-service credit card swipe at a gas pump etc. Complaints regarding credit card were ranked 11th with a total of 42 003 complaints in the Consumer Sentinel Network Data Book [28].

H. Cyber Intrusion and Data Breaches

A data breach is an act of incident in which personal information, like medical record, financial details, and driver's license number are exposed illegally. Data breach can happen electronically or in hard copy [29]. The indictment of 5 Chinese military members by the US Justice Department is an example of data breach [30]. Two ninth graders hacking an ATM in lunch hour [31] and the ongoing discussion about the involvement of Russia in the 2016 US presidential election are some examples of data breach [32]. According to the FBI's Internet Crime Report (IC3) 2017 [18], the second highest number of victims were of data breach with 30 904. IBM Security and Ponemon Institute interviewed more than 2 200 IT professionals from 477 companies and their 2018's annual report stated that an average total cost of a data breach accounted for 3.86 million USD [33].

I. Disaster Fraud

Disaster fraud is a criminal activity in which criminals deceive private organisations, individuals or the government bodies after a disaster. It can be done in many forms by a single person or a group of people. Common examples of disaster fraud include homeowners increasing damage estimates for personal gain against insurance or government fund, a group of people collecting charity in the name of disaster victims. According to the National Insurance Crime Bureau's (NICB) President and CEO Joe Wehrle, disaster fraud is "an unfortunate reality in post-disaster environments" [34]. Millions of people are affected in natural disaster such as earthquake, tornado, hurricane, flood or man-made terror attacks worldwide. People lose their property, home, or blood relatives and friends. In the aftermath of these disasters, organisations such as Red Cross, United Nations, and World Health Organization provide their services to help victims as much as they can. Unfortunately, criminals see these disasters as an opportunity for their personal gains. They make forge insurance claims and seek for financial assistance. According to FBI's Internet Crime Report 2017 [18], criminals make fake charities often after natural disaster and make illegal profit from those people who believe they are making contribution to the wellbeing of disaster victims. IC3 2017's report showed a total of 436 victims of disaster fraud, which accounted for 1 405 460 USD loss in the USA, and the Consumer Sentinel Network (CSN) Data Book 2017 [20] depicted a slow but steady increase in disaster fraud. The CSN's statistics showed 3174, 3483 and 3703 complaints in the year 2015, 2016 and 2017, respectively.

III. Preventive Measures

People use social media to express their thoughts regarding socio-economic issues, share events of their personal life and interact with each other. Ray Surette [35] discussed that with the advancement of social media people commit crime and post it on social media in form of text video and images. As social media is used by a criminal to commit crime, the same way the technology can be used to control, prevent, protect and investigate the crime. The regular use of social media in all walks of life has changed people's perspective of seeing crime and victimization [36]. Previously people used to make their own opinion on the basis of television and newspaper reports, but now social media is playing a vital role in it. Now individuals are sharing incidents happened with them as people in their social circle may help them catch the criminal [37]. Social media provides a vast amount of data in form of picture, text and videos, which law enforcement agencies use for profiling criminals and apprehending culprits. According to Jeremy Crump's report [38], UK's police forces started using social media in 2008. In the beginning, it was a decision of just a few officers to use it, but afterwards it became popular among the police officers. Eventually, the Association of Chief Police Officers (ACPO) recognized the use of social media in police force officially.

A. Preventing Burglary

There are two sides of every coin and use of social media is not an exception. Positive or negative use of social media depends upon its user [39]. On the one hand, criminals search for their potential targets using social media sites; on other hand, law enforcement agencies use the same media to apprehend them [39]. Toronto police's use of social media to arrest the city's most wanted criminals is such an example [40]. George R. S. Weir, Fergus Toolan and Duncan Smeed [39] concluded that all the social media users, whether businessmen or individuals, should be very cautious while sharing personal information that can be used against them. In this changing world, everything that people do has a digital sign and with an increasing digital sign of individual's activity, risk of misuse of this information is also getting bigger by each passing day [39], [41]. Burglary is not due to inception of social media sites, but they provide ease for a burglar to search for a soft target. If users are cautious and do not share their personal information then social media will not be much helpful for a burglar [39].

B. Preventing Social Engineering and Phishing

Social engineers are introducing new techniques of phishing and that is the reason because individuals and organisations should constantly enhance current anti-phishing techniques and search for new countermeasures [42]. There are various phishing techniques used by social engineers, such as deceptive phishing, malware-based phishing, SMiShing, vishing, cross site scripting and key loggers to mention a few [43]. With an increase in phishing techniques, different anti-phishing tools are released to counter them. These user-friendly anti-phishing techniques include one-time passwords (OTP), CAPTCHAs, digital certificates, genetic and attribute based anti-phishing algorithms [43]. Though these anti-phishing techniques are user-friendly, they are unable to provide complete defence against phishing. Social engineers make forge websites, which are highly similar to original ones, of banks and other financial service websites like PayPal and send thousands of emails in hope that victims will click the link inside their emails [42]. The text-based nature of this kind of phishing allows social engineers to use various media like social media and other messaging series to find their victims [44]. One countermeasure technique against phishing is to analyse the text of email using natural language processing (NLP) to assess the risk associated with it.

C. Preventing Malware

According to Kaspersky [45], malware can infect a computer in various ways and most common type of infect is the use of email. A suspicious email from a bank or a friend, who ask to open a link, is probably an attempt of malware. User vigilance is the first line of defence against malware. Individual's vigilance is obviously is not enough to protect computer or network, so the second layer of protection in form of antivirus is vital. In [46], researchers explored the security and threat landscape of smartphones. The research argued that immense amount of personal information, open source environment and lack of user's awareness made smartphones vulnerable to security attacks. In mobile devices, two widely used malware detection techniques are signature based and anomaly based. In signature-based detection techniques, smartphone activities are compared with previously known malicious activities, while in anomaly-based techniques, a model of normal system is created and malware is detected when system behaves in a different way.

D. Preventing Identity Theft

Protecting identity information and preventing identity theft are mutual processes for all stakeholders: identity owner, identity issuer, identity protector and identity checker [47]. Researchers define a framework for detecting, identifying and preventing identity theft. The framework discussed all the stockholders and their role and responsibility to prevent the identity theft. Identity owner is the person who owns an identity document such as birth certificate or passport and it is the responsibility of identity owner to protect it. The identity issuer is an individual or an institution that grants an identity to a person, such as a domicile, employee card. Law enforcement agencies, such as police, are responsible for the duties of identity protector [47]. Other researchers [48] also recommend that people should timely check their bank account and credit card details, do not keep all identity documents with them all the time and do not share personal information with others.

E. Preventing Cyber-Stalking

Modern technology has made life easy in all walks of life, but also provided ease for criminals to fulfil their dangerous plans [49]. The Internet has upgraded the stalking into cyber-stalking. Norton [50] differentiates cyber-stalking from stalking as online stalking, which makes use of technology, especially the Internet. In order to prevent cyber-stalking, Norton suggests individuals should be beware of their online presence. It suggests people search their own personal information and check what type of information is publicly available at these websites. One can always contact a particular website to remove personal information.

F. Preventing Cyber-Casing

Checking-in at a restaurant, announcing flight details or uploading pictures on social media with a famous place in background are routine activities of social media users, but these activities put people at risk. Alex Merton-McCann from McAfee [51] explains that cyber-casing is a process of using geo-tagged data by criminals. Fridland and Sommer [52] think that educating users about the risk of sharing location and providing them authority to make informed decisions will help reducing misuse of location data.

G. Preventing Credit Card Fraud

Credit card fraud has been on rise in past several years, and due to heavy losses, the researcher community is constantly searching for new ways of detection and prevention [53]. Credit card transaction screening techniques, such as address verification services (AVS), card verification methods (CVM), personal identification numbers (PIN) and biometrics, are some basic checks, but an effective and economical fraud detection system is the need of the day. The researcher [54] stresses that the tremendous use of neural network in banking and finance sector shows its success in the field.

H. Preventing Cyber Intrusion and Data Breaches

The need of securing user's information is all time high and needs a proper solution, otherwise breaches will occur constantly. In [55], researchers argue that third-party APIs, distributed storage and lack of standard service level agreement for security are the main causes of data breaches. In [55], researchers propose a Petri net privacy preserving framework (PPPF) to make a secure cloud platform.

I. Preventing Disaster Fraud

According to Richard and Valerie [56], prevention of disaster fraud is much cheaper than detection. Fraud prevention is economical in terms of money, resources, employee morale and good will of involved entity. The authors of this report suggested that public awareness, publishing and broadcasting regarding the disaster fraud made people cautious about imposters. Swift response of police at a local disaster site and strict checking of identification can also keep imposters away from the disaster victims. Technology can also play its role in detection and prevention of disaster fraud. The National Insurance Crime Bureau (NICB) developed a system named Predictive Knowledge, which gathers and examines insurance data of various states of the United States to stop, identify and probe insurance fraud.

IV. Findings

Social media has shown its potential in various matters of life, whether it is about gathering public for an uprising against government or to reduce the space between the astronauts and science lovers all around the world. A report of Aljazeera shows that protest organizers heavily depend on social media sites, such as Facebook and Twitter [57]. With the vast amount of data available at social networking sites, the possibility of the usage of big data in different walks of life is numerous [58]. Marketers can use social networking sites to understand consumer behaviour and design effective marketing campaigns [59]. The UK government started monitoring social media feeds of Facebook, Twitter and blogs [60]. Big data have recently received little attention from computational criminologists [61]. In their study, researchers discuss the challenges and the affordance of the field in a detailed manner. These studies make use of routine activities, but the key limitation is the dismissal of text used in post of social media and only focus is placed on routine activities [61].

The summary of this study is demonstrated in Table II, which lists the types of cybercrime, as well as recommendations and techniques for their prevention.

TABLE II
Recommendations and Techniques for Cybercrime Prevention

Cybercrime	Prevention tips	Preventing techniques
Burglary via Social Networking	Do not share location Do not share home address Do not share personal information with friends of friends Limit your connection to only those whom you know Check your privacy setting and control how others can tag you Limit your app permissions	Required physical security, such as security cameras, door locks, monitory blind spots, motion-activated floodlights and/or indoor lights with random timers etc. Techniques: Time series approach, random forest based model [62], multi-layer perceptron, self-organising map, rule induction, genetic algorithms and case based reasoning [63]
Social Engineering and Phishing	Do not send sensitive information over the Internet before checking a website's security. Do not respond to unsolicited call, email or visits for personal or financial information Do verify the legitimacy of a doubtful email by directly contacting the company.	One-time password (OTP) CAPTCHA Digital certificates Genetic and attribute based anti-phishing algorithms Techniques: Neural network, IREP [64], C4.5 algorithm [64] [65]
Malware	Install updated antivirus User vigilance required Pay attention to the uniform resource locator (URL) of a website. Malicious websites may look identical to a legitimate site	Signature-based malware detection [66] Anomaly-based malware detection. Techniques: N-grams, API/system calls, assembly instructions, and hybrid features [67]
Identity Theft	Owner should destroy (expired) identity documents, such as driving license with expired date Restrain sharing identity documents on social media, e.g., boarding pass etc. Do not keep/store identity documents within system, e.g., credit card etc.	Three-factor authentication (3FA) Biometrics Anti-identity theft software like LifeLock by Symantec Techniques: SD and CD algorithms [68], outlier detection, hidden Markov model, genetic algorithm and logistic regression [69]
Cyber-Stalking	Keep work and social networking email address separate Do not place all the information online, such as date of birth or employment history Use photographs that do not identify location Do not use legal name on social media; use nick name Utilize the privacy settings available to various platforms, such as Facebook, Twitter and others	Gather and document as much evidence as you can Block and report to authorities against cyber-stalker Techniques: association rule mining, text mining [70], cyber-stalking detection framework and signature-based data mining [71]
Cyber-Casing	Switch off your GPS on smartphone Do not publicly publish holiday status or photos until you have returned Do not mention the times you will be available at home when selling items on online market places	Use online tools, like tool.geoimgr.com, to check and remove if an image contains geo locations. Techniques: SVM classifiers [72]

Credit Card Fraud	Continuous surveillance of vaults Regular and severe material accounting Employee log that touches critical material to sign for it Apply two-person rule to access critical property Encourage employee attention to security Seek security buy-in	Monitoring anomalies Techniques: address verification service (AVS), card verification value (CVV), decision tree, neural network, k-means clustering, hidden Markov model, and genetic algorithm [73]
Cyber Intrusion and Data Breaches	Design and conduct end-user awareness campaign Create and enforce the computer security policy Keep data only as long as you need it Prepare an incident response plan Deploy intrusion detection and preventions system Make routine vulnerability assessment Make sure all the login credentials have not expired	Verification and validation Personal identification number (PIN) Techniques: Petri net-based encryption, address verification service (AVS), card verification method (CVM), common vulnerability and exposure database (CVE), common weakness enumeration database (CWE), and national vulnerability database (NVD) [74]
Disaster Fraud	Public awareness Swift response of police Strict checking of identification	Look for the social media and web presence of the charity you wish to donate to Techniques: text mining and autoregressive integrated moving average (ARIMA) [75]

V. Discussion and Future Work

The Internet has changed everything that we do and how we do it. Emails have replaced letters, video call is today's way of meetings, and social media is the medium of social interaction with the rest of the world. People use social media to share their opinion, thoughts, routine, interact with friends, and make new acquaintances. The popularity of social media platforms is reflected in its user base of 2.22 billion in 2019, which is expected to reach 3.02 billion in 2021. With its huge population, social media is producing avalanche of big data, or we can call it social big data. Our data driven society may perceive this as an opportunity, but it comes with its own ever-evolving challenges, such as volume, variety, velocity, veracity, volatility, quality, and vulnerability. Along with the challenges, the productive use of this huge amount of big data is endless in all walks of life. Social media is an ideal place for anyone who is looking for a potential buyer of product or service, an employee for a particular vacancy, and ideal target for crime like burglary, identity theft, and cyber-stalking. Like for other professionals, social media is a good tool for law enforcement agencies as well as criminals. In this study, we have discussed nine different crimes that have strong connection with social media. One can be easily victim of burglary or social engineering in case where the social media account of his friend is compromised and victim does not know it. The case is a bit similar with malware and identity theft, if social media user is not using privacy settings, shares personal information more often publicly, and opens all the links he/she sees. If social media user does not want to become a victim of cyber-stalking or cyber-casing, he/she needs to be cautious about the information he/she shares publicly. User should check authenticity of email or a call asking for personal information in order to be safe from credit card and disaster fraud. Keeping security tools installed all the time is the first line of defence, when it comes to data breaches. This study has discussed all these crime types along with their statistics. Finally, literature is completed with the summarised chart of prevention recommendations and their techniques. The most common recommendation for all the crime types is to be cautious about the information a user is sharing publicly. Awareness of what hidden information an image, text or a video might hold that a user wants to upload on social media is not just an utmost need of today, but also a very efficient way to prevent a user from being a victim of any cybercrime.

In future, the authors plan to work on a design and features of a mobile application that will enhance the awareness of end-users. This application will help smartphone users to get to know various vulnerabilities of not just the smartphone, but also data, such as, text, image and videos it contains. Furthermore, big data analytics techniques can be used to fetch data from social media sites, such as, Facebook and Twitter to perform analytical operations. One of the many possible analytical operations can use an algorithm to check whether the social media images contain geo-location tag or not. It will help identify images that can be used in crime, for example, cyber-casing and removal of geo-location tag will help preventing crime. In terms of identity theft, cyber-stalking, and credit card fraud, various data analytics techniques could be used to identify what publicly available information of social media could make the user a possible victim. Visually grounded language plays a vital role in analysing image and video to prevent cybercrime.

References

[1] N. Thabet and T. R. Soomro, "Big Data Challenges," *Journal of Computer Engineering & Information Technology*, vol. 4, no. 3, 2015. https://doi.org/10.4172/2324-9307.1000133

[2] Internetlivestats.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] T. R. Soomro and H. Wahba, "Perspectives of Cloud Computing: An Overview," *Proceedings 14th International Business Information Management Association (IBIMA) Conference on Global Business Transformation through Innovation and Knowledge Management*, Istanbul, 2010.

[5] M. Yar, *Cybercrime and Society*. SAGE, 2016.

[6] R. Broadhurst, "Developments in the globallLaw enforcement of cyber-crime," *Policing: An International Journal of Police Strategies and Management*, vol. 29, no. 3, pp. 408–433, 2006. https://doi.org/10.1108/13639510610684674

[7] "Social Media Use in Law Enforcement: Crime prevention and investigative activities," LexisNexis, 2014.
[8] J. Blomberg, "Fighting Crime Through Social Media and Social Network Analysis," SAS, 2012.
[9] NW3C, "Criminal Use of Social Media (2013)," NW3C, 2013.
[10] BBC News, "Kim Kardashian robbery: How do you sell high-profile diamonds?," Ocober 4, 2016.
[11] Symantec, "What is social engineering?," Symantec Corporation, 2015.
[12] M. Sauter, "Nine Major Ways Criminals Use Facebook," Fox Business, 2012.
[13] B. Nahorney, "Internet Security Threat Report (2017)," ISTR, 2017.
[14] Symantec, "Internet Security Threat Report," Symantec Corporation, 2019.
[15] 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/s11948-016-9867-x
[16] S. Irshad and T. R. Soomro, "Identity Theft and Social Media," *International Journal of Computer Science and Network Security,* vol. 18, no. 1, pp. 43–55, 2018.
[17] FBI, "Internet Crime Report (2016)," Internet Crime Complaint Center, 2016.
[18] FBI, "Internet Crime Report (2017)," Internet Crime Complaint Center, 2017.
[19] FTC, "FTC Releases Annual Summary of Consumer Complaints (2017)," FTC, 2017.
[20] F. T. Commission, "Consumer Sentinel Network Data Book 2017," Consumer Sentinel Network, 2018.
[21] F. T. Commission, "Consumer Sentinel Network Data Book 2018," Commission, Federal Trade, 2019.
[22] NW3C, "Cyberstalking (March 2015)," NW3C, 2015.
[23] A. A. Moore, "Cyberstalking and Women: Facts and Statistics," thoughtco.com, 2018.
[24] Bureau Of Justice Statistics, "Stalking". [Online]. Available from: https://www.bjs.gov/index.cfm?ty=tp&tid=973
[25] M. Duggan, "Online Harassment 2017," Pew Research Center, 11 July 2017. [Online]. Available: http://www.pewinternet.org/2017/07/11/online-harassment-2017/. [Accessed 16 March 2019].
[26] P. Saariluoma and H. Sacha , "How cyber breeds crime and criminals," The Society of Digital Information and Wireless Communications (SDIWC), 2014.
[27] NW3C, "Credit Card Fraud (2017)," NW33, 2017.
[28] FTC, "Consumer Sentinel Newtork Data Book 2016," Consumer Sentinel Newtork, 2017.
[29] NW3C, "Cyber Intrusion and Data Breaches 2017," NW3C, 2017.
[30] A. Kaphle, "These are the 5 members of the Chinese military charged with cyber-espionage," The Washington Post, 2014.
[31] J. Lyne, "14 Year Olds Hack ATM In Lunch Hour - How It Happened," Forbes, 2014.
[32] L. Harding, "What we know about Russia's interference in the US election," The Guardian, 2016.
[33] I. B. M. (IBM), "2018 Cost of a Data Breach Study: Global Overview," International Business Machines (IBM).
[34] NW3C, "Disaster Fraud 2017," NW3C, 2017.
[35] R. Surette, "How social media is changing the way people commit crimes and police fight them," LSE, 2016.
[36] A. McGovern and S. Milivojevic, "Social media and crime: the good, the bad and the ugly," University of New South Walse, Sydney, 2016.
[37] S. Schneider, "Hoffman Estates family turns to Facebook to help identify home burglars," Fox 32 Chicago, 2016.
[38] J. Crump, "What Are the Police Doing on Twitter? Social Media, the Police and the Public," Policy&amp; Internet, vol. 3, no. 4, 2011. https://doi.org/10.2202/1944-2866.1130
[39] 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
[40] R. D'Amore, "Toronto police tap into power of social media to catch city's most wanted criminals," CTV News Toronto, 2018.
[41] C. Rose, "The Security Implications Of Ubiquitous Social," *International Journal of Management & Information Systems (IJMIS),* vol. 15, no. 1, 2011. https://doi.org/10.19030/ijmis.v15i1.1593
[42] M. Rajab, "An anti-phishing method based on feature analysis," *Proc. The 2nd International Conference on Machine Learning and Soft Computing*, pp. 133–139, Vietnam, 2018. https://doi.org/10.1145/3184066.3184082
[43] L. J. Singh and N. Imphal, "A Survey on Phishing and Anti-Phishing Techniques," *International Journal of Computer Science Trends and Technology (IJCST),* vol. 6, no. 2, pp. 62–68, 2018.
[44] K. Thakur, J. Shan and A.-S. K. Pathan, "Innovations of Phishing Defense: The Mechanism, Measurement and Defense Strategies," *International Journal of Communication Networks and Information Security (IJCNIS),* vol. 10, no. 1, pp. 19–27, 2018.
[45] Kaspersky, "Learn about malware and how to protect all your devices against it," Kaspersky. [Online]. Available: https://www.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it. [Accessed 15 July 2018].
[46] D. He, S. Chan and M. Guizani, "Mobile application security: malware threats and defenses," *IEEE Wireless Communications,* vol. 22, no. 1, pp. 138–144, 2015. https://doi.org/10.1109/MWC.2015.7054729
[47] W. Wang, Y. Yuan and N. Archer, "A contextual framework for combating identity theft," *IEEE Security & Privacy,* vol. 4, no. 2, pp. 30–38, 2006. https://doi.org/10.1109/MSP.2006.31
[48] A. Hedayati, "An analysis of identity theft: Motives, related frauds,techniques and prevention," *Journal of Law and Conflict Resolution,* vol. 4, no. 1, 2012.
[49] Matt, "6 Ways to Avoid Becoming a Cyberstalking Victim," NAI, 2017.
[50] S. Symanovich, Norton Security Center, "Cyberstalking: Help protect yourself against cyberstalkers,", Retrieved February 2019.
[51] A. Merton-McCann, "Cybercasing – How Sharing Your Pics, Videos and Status Updates Can Get You Into Trouble", McAfee, 2013.
[52] G. Friedland and R. Sommer, "Cybercasing the joint: on the privacy implications of geo-tagging," in *HotSec'10 Proceedings of the 5th USENIX conference on Hot topics in security*, Washinton, DC, 2010.
[53] P. H. Tran, et al., "Real Time Data-Driven Approaches for Credit Card Fraud Detection," in *Proceedings of the 2018 International Conference on E-Business and Applications*, pp. 6–9, Vietnam, 2018. https://doi.org/10.1145/3194188.3194196
[54] J. T. S. Quah and M. Sriganesh, "Real-time credit card fraud detection using computational intelligence," *Expert Systems with Applications: An International Journal*, vol. 35, no. 4, pp. 1721–1732, 2008. https://doi.org/10.1016/j.eswa.2007.08.093
[55] C. Dhasarathan, V. Thirumal and D. Ponnurangam, "Data privacy breach prevention framework for the cloud service," *Security and Communication Networks,* vol. 8, no. 6, 2014. https://doi.org/10.1002/sec.1054
[56] R. G. Brody and V. J. Kimball, "Natural catastrophe and disaster fraud," Fraud Magazine, 2006.
[57] A. J. A. AGENCIES, "Timeline: Egypt's revolution," Al Jazeera, 2011.
[58] M. Kramer, "The Astronauts You Should Start Following on Twitter," National Geographic, 2013.
[59] C. Syme, "How to Use Social Media to Gather Valuable Marketing Data," Social Media today, 2014.
[60] K. Collins, "Government pays companies to monitor you on social media," Wired, 2015.
[61] M. L. Williams, B. Pete and L. Sloan, "Crime Sensing With Big Data: The Affordances and Limitations of Using Open-source Communications to Estimate Crime Patterns," *The British Journal of Criminology*, vol. 57, no. 2, pp. 320–340, 2016. https://doi.org/10.1093/bjc/azw031
[62] D. M. M. Alghamdi, "A Data Mining Based Approach for Burglary Crime Rate Prediction," University of Illinos, Chicago, Chicago, 2017.
[63] R. W. Adderley, "The Use Of Data Mining Techniques In Crime Trend Analysis And Offender Profiling," University of Wolverhampton, Wolverhampton, 2007.
[64] M. Al-diabat, "Detection and Prediction of Phishing Websites using Classification Mining Techniques," *International Journal of Computer Applications,* vol. 147, no. 5, pp. 5–11, August 2016. https://doi.org/10.5120/ijca2016911061
[65] P. Akansha and E. Meenakshi, "Detection of phishing websites using C4.5 data mining algorithm," in *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, 2017.
[66] Y. Ye, T. Li, D. Adjeroh and S. S. Iyengar, "A Survey on Malware Detection Using Data Mining Techniques," *ACM Computing Surveys (CSUR),* vol. 50, no. 3, October 2017. https://doi.org/10.1145/3073559
[67] M. Siddiqui, "Data Mining Methods For Malware Detection," University of Central Florida, 2008.

[68] C. Phua, K. Smith-Miles, V. Lee, and R. Gayler, "Resilient Identity Crime Detection," *IEEE Transactions on Knowledge and Data Engineering*, vol. 24, no. 3, pp. 533–546, January 2010. https://doi.org/10.1109/TKDE.2010.262

[69] A. Kshirsagar and L. Dole, "A Review On Data Mining Methods For Identity," *International Journal of Electrical, Electronics and Computer Systems (IJEECS)*, vol. 2, no. 1, 2014.

[70] C. Lekha and S. Prakasam, "Implementation Of Data Mining Techniques For Cyber Crime Detection," *International Journal of Engineering, Science and Mathematics* , vol. 7, no. 4, January 2018.

[71] X. Feng, A. Asante, E. Short and I. Abeykoon, "Cyberstalking Issues," in *2017 IEEE 15th Intl. Conf. on Dependable, Autonomic and Secure Computing, 15th Intl. Conf. on Pervasive Intelligence and Computing, 3rd Intl. Conf. on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech),* Orlando, FL, 2017, pp. 373–376. https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.78

[72] E. Spyrou and P. Mylonas, "A Survey of Geo-tagged Multimedia Content," in *IFIP International Conference on Artificial Intelligence Applications and Innovations*, Paphos, pp. 126–135, 2014. https://doi.org/10.1007/978-3-662-44722-2_14

[73] G. Suresh and R. J. Raj, "A Study on Credit Card Fraud Detection using Data Mining Techniques," *International Journal of Data Mining Techniques and Applications,* vol. 7, no. 1, pp. 21–24, June 2018.

[74] X. Li, J. Chen, Z. Lin, L. Zhang, Z. Wang, M. Zhou and W. Xie, "A Mining Approach to Obtain the Software Vulnerability Characteristics," in *Fifth International Conference on Advanced Cloud and Big Data (CBD)*, Shanghai, 2017. https://doi.org/10.1109/CBD.2017.58

[75] B. Gadidov and L. Le, "A Case Study of Mining Social Media Data for Disaster Relief: Hurricane Irma," in *SAS Global Forum*, 2018.

Dr. Tariq Rahim Soomro, Professor & Head of Computer Science Department at the College of Computer Science & Information Systems, the Institute of Business Management. He has received B.Sc. (Hons) and M.Sc. degrees in Computer Science from the University of Sindh, Jamshoro, Pakistan and his Ph.D. in Computer Applications from Zhejiang University, Hangzhou, China. He has more than 24 years of extensive and diverse experience as an administrator, computer programmer, researcher and teacher. His research focus lies on GIS, IDNs, distance education, e-Commerce, multimedia, UNICODE, WAP, P2P, cybersecurity, bioinformatics, ITIL, cloud computing, green computing, big data, IoT, quality of software, telemedicine, databases, programming and higher education. He has published in these areas over 80 peer-reviewed papers. He has been a Senior Member of IEEE, IEEE Computer Society and IEEE Geosciences & RS Society since 2005 and IEEE Member since 2000. He has been a member of the Project Management Institute (PMI) since 2007; Senior Member of the International Association of Computer Science and Information Technology (IACSIT) since 2012; Life Member of the Computer Society of Pakistan (CSP) since 1999; Global Member of the Internet Society (ISOC), USA, since 2006. He has been an active member of IEEE Karachi Section (Region 10), currently serving as a Secretary Karachi Section and served as Chair GOLD affinity Group and Member Executive Committee IEEE Karachi Section 2014, in the period 2017–2019 he also served as a branch councillor. He is a member of Task Force on Arabic Script IDNs by Middle East Strategy Working Group (MESWG) of ICANN. He also received the ISOC Fellowship to the IETF for 68th Internet Engineering Task Force (IETF) Meeting.
E-mail: tariq.soomro@iobm.edu.pk
ORCID ID: https://orcid.org/0000-0002-7119-0644

Mumtaz Hussain is a computer science graduate from SMI University, Karachi, Sindh Pakistan. He works as a freelance programmer. He has been an active member of IEEE since 2018 and a member of the Executive Committee IEEE Karachi Section 2019.
E-mail: mamtazali@gmail.com