Identity Theft and Social Media

Shareen Irshad[1] and Tariq Rahim Soomro[2]

[1]Department of Computer Science SZABIST Dubai Campus, Dubai, UAE
[2]College of Computer Science & Information Systems, IoBM, Karachi, Sindh, Pakistan

Summary
Over a very short span of time, the world of social media has seen tremendous improvement. From Websites offering only simple instant messaging and blogging facilities initially, to full-grown social networking sites; such as Facebook and Twitter allowing users to engage in multiple simultaneous activities. Social media today has undoubtedly become the talk of the town due to its immense utilization. However, this does not mean that this evolution only brought about positive changes. On the other end of the spectrum, social media Websites have contributed in providing new and creative ways to criminals and fraudsters to perform their crimes. They have taken the traditional crimes to whole a new level. In addition, it has become very common for criminals to boast about their crimes on social networking sites giving rise to "Performance Crimes". One particular crime that has seen a striking increase in levels is Identity Theft. This study tries to shed light on the evolution of Identity Theft on social media platforms; and how this rich repository of personal information has become a breeding ground for identity thieves.

Keywords:
Social Media, blogging, crimes, personal information, Identity Theft.

1. Introduction

The meaning of "Identity theft" can be visualized from multiple aspects but they all boil down to one basic definition as explained by [1], which says that it is the illegal or unauthorized use of personal information belonging to someone else for one's own benefit. The crime of Identity theft has not only been in the limelight up until recently, but it was a prevalent issue long before the Internet. Traditionally, it was something known as "dumpster diving", where the identity thieves had to physically go around snooping in trash bins to look for personal information, such as discarded bills and documents that identified a person. There were a number of traditional ways ranging from very complex to utterly simple that an identity thief could use to gain access to personal data [2]. For example, if someone was entering a credit card number or a calling card number in a public place; criminals often used a method called "shoulder surfing", where they would watch the person from a nearby place in an attempt to capture that information. Another way is to eavesdrop on a conversation in which the person might be giving a pin over the phone. Another method that a fraudster would use was to retrieve discarded mails that contained applications for pre-approval of credit cards. The recipients would often throw away such mails without shredding the enclosed contents and this gave the criminals an opportunity to activate those credit cards for their own use without the victim's knowledge [3]. The evolution of Identity Theft can be seen in Table 1 from as early as 1800s to its predicted state in 2020 and beyond [4]:

Table 1: Evolution of Identity Theft

Era	Type of Identity Theft
1800-1918	The outlaws of this era killed people to assume their identities
1919-1921	Identities were stolen to cast votes multiple times
1922-1930	The smugglers created their own version of witness protection programs and murdered people to attain legal documents to create new identities
1931-1959	Youngsters created fake IDs to buy alcohol
1960-1969	Introduction of credit cards gave criminals new ways of identity theft
1970-1989	Frank Abagnale the famous con artist stole identities to cash cheques
1990-1998	Technology advancement increased cases of identity crimes
1999-2000	Introduction of Internet and search engines like Google led people to give away personal information
2001-2003	The credit reporting agencies were instructed to provide credit reports to customers to prevent fraudulent accounts being opened
2004-2015	The National Crime Victimization Survey was updated to include new forms of Identity Theft
2016	Identity Theft was the most popular consumer complaint for 15 consecutive years
2017	American banks increased their security causing criminals to use other platforms for stealing identities
2018-2020	Technology is evolving and new apps are being introduced; so that thieves are gaining more and more access to personal information through these new apps

There is a range of criminal offences under identity theft that offenders perform using low technology methods. Some of them are mentioned below along with their impacts:

Manuscript received January 5, 2018
Manuscript revised January 20, 2018

1.1. Low Technology / Traditional Methods of Identity Theft

1.1.1 Financial Identity Theft:

This usually involves fraud with bank accounts and credit cards [5]. There are several techniques offender uses to perform financial Identity Theft, such as [6]:

- The imposter may open a new credit card account under the victim's name, Social Security Number and date of birth and then utilizes the entire card limit. He then obviously doesn't pay any bills which cause the victim to become a defaulter
- The fraudster may even change the mailing address of the victim, which will make the real owner of account be unaware of any charges
- The fake person might also create a new bank account under the victim's name and write bounced cheques.

The impact that a Financial Identity Theft has on its victims is immense. The victim suffers from financial stress as well as emotional stress [7].

1.1.2 Medical Identity Theft:

This type of identity theft usually occurs, when someone tries to use other people's personal data such as name, Medicare number etc. to buy medical supplies, drugs or even present false billings to the Medicare. This category of theft can cause serious problems in the victim's life by disrupting credit ratings and can even lead to wrong information being fed into the victim's medical records [8].

1.1.3 Criminal Identity Theft:

This is one of the cruelest forms of identity theft and probably the one that is hardest to revert. The thief basically, assumes someone else's identity as their own and uses it to commit crimes rather than just exploiting the victim's bank account. This is performed by giving a fake self-identification during an interrogation to the law officials, when the thief gets caught for a crime. This crime can have dramatic consequences on the victim. To start with, the victim might be issued an arrest warrant without his/her knowledge, which could end him/her behind bars. This would eventually lead to a permanent criminal record and would affect his/her future endeavors such as jobs, loans etc. [9].

1.1.4 Synthetic Identity Theft:

This kind of identity theft is the most dominant and significant nowadays. It involves building a fictitious identity by combining real information with fabricated data. This new identity may have the Social Security Number (SSN) of one person, the date of birth of another person along with the name of a third person. To provide this identity with a financial history, the fraudster may apply for credit cards, make purchases and perform some other related activities [10]. The consequence of a Synthetic Identity Theft is a fragmented credit file. This means that when a thief uses a part of a person's SSN, the real person becomes associated with the synthetic identity due to that SSN [11].

1.1.5 Child Identity Theft:

The general crime of identity theft does not only happen with adults, but apparently with children too. The most obvious reason is that underage children do not usually understand or are aware of the importance of personal information. When the minor finally becomes old enough to use this information for some official work, they find themselves victims of this crime. This can have a very disturbing effect on the child if for example, they apply for a driver's license and find out they have tons of pending tickets [12]. Usually children's personal information are required by school forms so parents should be aware of how his/her data is being stored, utilized or even discarded to avoid any misuse [13].

1.1.6 Drivers' License Identity Theft:

This type of identity theft does not require someone to have any special fraud skills. In fact, the only thing the criminal needs is the persons' drivers' license, when it gets lost or gets into wrong hands. The thief either sells this license or may use it when he/she gets caught speeding or gets involved in any transportation crime. Because of this, the police will eventually hold the real person accountable, which may destroy that person's reputation and may cause financial troubles [14].

1.1.7 Tax Identity Theft:

A Tax identity theft usually occurs, when the fraudster tries to file a tax refund using someone else Social Security Number. The victim remains unaware of this until he/she claims a refund, upon which realizes that a refund was claimed already using his/her SSN [15].

The above mentioned categories of Identity Theft were just a few out of a huge number and these were mainly practiced, when the technology was still in its maturing stages and had not flourished to the extent it has now. Today, Identity theft has taken a completely new meaning with the advent of technology's most significant invention, the "Social Media".

1.2 Social Media

It is simply described as, a collection of applications that are based on the Internet, which allows its users to generate and exchange information. Its ability to connect societies from all around the world through a single platform attracted more and more people towards it [16]. Initially, social media Websites like Facebook, Twitter, and Instagram thought to be used specifically by the younger generation for socializing and it could not benefit businesses in any way. However, as the saying goes "not all that glitters is gold", these Websites have their fair share of disadvantages as well. The main objectives of this study are two-fold. First to understand the different types of identity theft taking place; on social media networks; and second how the crime of identity theft affects the users of social media and to what extent they are aware of its consequences together with prevention techniques to avoid it. This evaluative study also aims to create awareness among users of Social Media about the importance of one's personal information and its availability in public. This paper is organize as follows; section 2 of this study will cover the literature review. Section 3 will shed light on extended forms of this crime along with a short survey to get an insight about how aware the users of Social Media are regarding the crime of stealing identities followed by section 4, where the results of the survey will be discussed. The last section of the study will highlight possible prevention techniques and future work.

2. Literature Review

In this era, it comes as no surprise that social media networks have become so popular not only among teenagers, but even among adults and professionals. This is due to a number of various reasons depending upon each individual's priorities. Its popularity among the teenagers and non-tech people can contribute to the fact that they are very user-friendly and do not require any technical knowledge to navigate through them. In fact, their mobile versions are even simpler, which allows further lot of people to interact with each other. For professionals, social media sites like LinkedIn gives them a platform on which they can publish their accomplishments, best traits, achievements and skills that help them get recognition among potential employers, colleges and like-minded individuals. In addition, they can also highlight their brands and startups or search for jobs relative to their domains [17]. As more and more people are becoming aware of this technology and opting to use these platforms as a way of communicating and connecting with others, various companies are viewing this as an opportunity and creating more of these platforms simultaneously.

A recent statistic of June 2017 [18] shows the most popular social networking Websites in the world. Again, Facebook takes the lead with 1.94 billion active users followed by Youtube with 1 billion users. The popularity of Facebook is evident in this statistic as there is a huge gap between Facebook and its counterparts. The top five most favored social networking sites according to number of active users as seen in Figure 1 are Facebook, Youtube, Instagram, Twitter and Reddit.

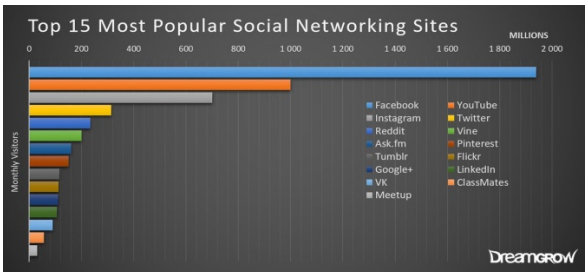

Fig. 1 Most popular social media site (June 2017) [18]

Apart from becoming popular for networking, these sites have also become popular for various crimes that take place within these virtual realities that actually affect an individual's life to catastrophic extents. According to [19] the major crimes that are committed using these social networking sites are as follows:

2.1 Top Social Media crimes

2.1.1 Cyber-bullying/Stalking/Online threats:

This is a very common and often repeated crime, where the person doing it does not even realize he/she is committing a crime. The following Figure 2 shows 10 studies conducted from 2007 to 2016 that depict the victimization rate of cyber-bullying. As seen in the figure there is a general increasing trend from 2007 to 2016 i.e. from 18.8% to 33.8% respectively [20].

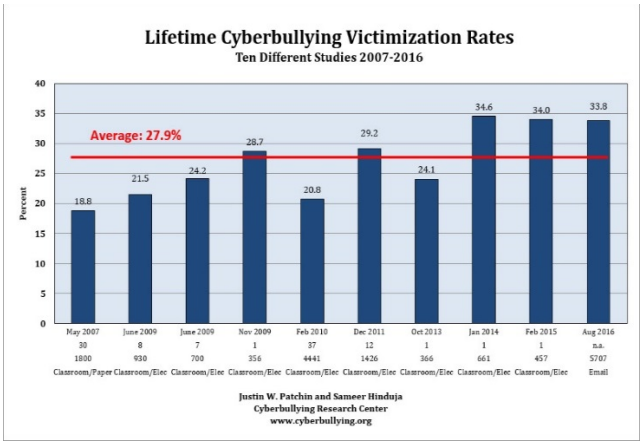

Fig. 2 Victimization rate of cyber-bullying [20]

2.1.2 Trade of illegal products:

This particular crime involves buying and selling products and services that are either illegal or banned in a certain locality. It usually consists of buying drugs, alcohol, etc. For example, according to [21] a 15-year old student was arrested in Kentucky on accounts of carrying an unlicensed and loaded gun on school premises. Upon interrogation, he confessed that he had bought the gun on Facebook.

2.1.3 Uploading videos and pictures of criminal activity:

With the Smartphone technology improving day by day along with social media, the criminals are tempted to post and upload their acts of crime to these platforms for the public to see. Although this does sound bizarre, but it gives the law enforcement agencies an edge to catch the criminals quickly. According to [22], Vester Lee Flanagan posted a video on Twitter, which showed him shooting his two other co-workers. Similarly, four people were arrested in Chicago for live streaming a video on Facebook in which they tortured a teenager.

2.1.4 Robberies during vacations:

A very common practice among social media users is to post their vacation statuses on their pages for their friends and family to see, but some of them leave these statuses as public for everyone to see. This makes them an easy target for burglars to rob their houses, when they are away on vacations. According to [23], a news channel reported that three local men were arrested on charges of burglary of more than 18 houses in New Hampshire and they confessed that they used social networking sites to target their victims.

2.1.5 Hacking and Identity theft:

Logging into someone else's account for intentional misuse has become quite common nowadays and so has Identity theft, where fake accounts or accounts for impersonation are made solely for the purpose of fraud. Figure 3 [24] shows the statistics of a US research depicting how victims of Identity Theft increased from 2013 to 2015 to a whopping total of about five hundred thousand victims in 2015.

2.1.6 Business Spying:

The fraudster can easily pose as an employee of a company by creating a Facebook page and may invite other employees to join. This may lead to leaking of company's confidential information and sabotaging its image [25].

Fig. 3 Increase in victims of Identity Theft [24]

A report conducted by RSA Security Inc. called "2017 Global Fraud and Cybercrime Forecast" says that social media frauds had initially started in 2011, when e-commerce accounts and credit cards began publishing. These sites became a breeding ground for frauds as they were usually easy, free and had a global reach [26]**.** Apart from crimes such as bullying, stalking, harassing that take place on social media sites, Identity Theft is also one of them, but has a greater impact on the victim as compared to the others. Social networking sites like Facebook, Twitter, LinkedIn have penetrated so deeply into the lives of anyone, who just has basic knowledge about the use of the Internet. Little do they know that these platforms have become a breeding ground for criminals and especially identity thieves [27]. Even today, the primary purpose of Identity Theft has not changed, but only methods of intrusion and platforms have transformed. Some of the ways that were being used years ago and are still adopted for acquiring personal information are listed below:

- **Phishing:** Phishing refers to a kind of fraud in which the criminal tries to gain access to personal information,

such as account information or login credentials by impersonating as a trusted entity. This usually performed by two methods. First sending links of fake Websites that capture your login and password credentials and second by becoming friends with the person by sending false acquaintance messages, which the person unknowingly accepts [28]. On social networking sites, this is accomplished by sending requests to play a Quiz, complete a survey or share something for a free giveaway [29].

- **Social media cons:** This is a common scheme, which fraudsters use on Facebook, where they steal someone's identity and send out plea messages for cash to that person's friends and family. Concerned family and friends get tricked and send out money to these criminals [29].
- **Identity Spoofing:** This occurs, when criminals create fake accounts of musicians, politicians, actors etc. to gather sensitive data from other people or in hopes to tarnishing their image [30].
- **Hacking:** A very common and easy method for criminals is to steal identities nowadays through social media accounts. This is mostly due to everyone's habit of using the same password for almost all accounts. Once the hacker gets access to your social accounts, they can easily get hold of your bank account data, online shopping details, and credit card details or even use your social accounts to perform criminal activities [31].

3. Materials and Methods

The methodology used for this study is based on qualitative as well as quantitative methods. The initial and major part of the study takes on a qualitative approach. The study first begins to evaluate secondary data to find the various ways and methods of Identity Theft that criminals adopted. The study then precedes to identity the top social networking sites that are used extensively in the recent times and then links them to the different crimes that emerged when social media giants like Facebook, Twitter, and Instagram etc. began surfacing the Internet. In addition, as the focus revolves around the crime of Identity Theft on social media platforms, the study moves forward by describing the ways and tactics that thieves use to forge identities on social media sites in this modern age.

Furthermore, to cover the quantitative part of the study and to collect primary data, a short survey is used. The questionnaire comprises of about 10 questions in total and contains questions related to social media usage, awareness of various crimes taking place on these platforms and user's perception of those crimes. This was through a web-based survey with close-ended questions, where the participants could only choose answers from a fixed set.

4. Results and Findings

The online survey named "Awareness of social media crimes" conducted as a source of generating our primary data to get an estimate of quantitative data for study-accumulated 104 responses during the course of two and a half months. The majority of the respondents found to be from Asia that formed total of 86.5% of the population followed by participants from North America, Africa, Australia, South America and Europe in the same order. Out of this distributed population, 69.2% were female and the rest were male. As seen in Figure 4 the ages of these participants are spread over a spectrum starting from teenagers to over 50 year olds. The majority were 20-27 year olds with 67% followed by 28-34 year olds with 17%, 13-19 year olds with 9%, 43-50 year olds with 3 % and a small minority from the 35-42 and 50+ age ranges.

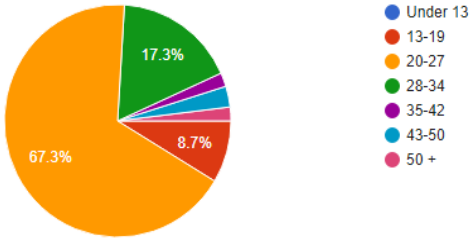

Fig. 4 Age statistics

The immense use of social media sites was clearly visible in our survey as well. A whopping 98.1% of people admitted to having a personal profile on at least one of these sites among which the top contender was undoubtedly Facebook with 101 users. The second in line was Instagram with 77 users followed by Google +, Twitter, Snapchat and some other networking site with 52, 51, 42 and 19 users respectively as shown in Figure 5.

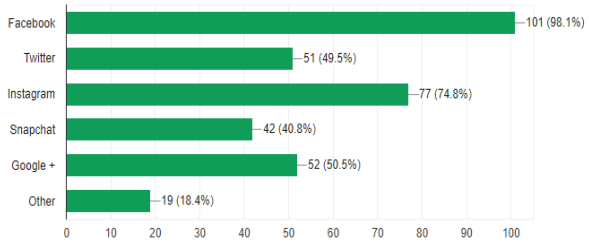

Fig. 5 Platform with most number of users

The survey then proceeded to ask if the participants were aware that social networking platforms are used to commit various crimes. To which 88% responded in agreement while 12% said they did not know. Furthermore, to get an in-depth analysis of how users perceived the nature of various crimes being practiced on social media, a question was asked to rate the crimes on a scale of 1 to 5 where 1 indicated least severity, while 5 indicated most severe. As seen in Figure 6, 52 people thought cyber-stalking/bullying was the most severe crime on social media followed by Identity Theft with 42 users. Other crimes such as Scams, posting videos of criminal activity, buying illegal items and robbery were rated severe in the same order.

The last section of the survey collected information regarding victimization. 92% of the respondents said they were never victims of social media crimes, while the 8% who had fallen prey were mostly victims of scams (56%) followed by harassment (44%), defamation of character (38%), bullying/stalking (38%), identity theft (20%) and robbery(20%) as shown in Figure 7. These victims also confessed to suffering emotional and financial burdens.

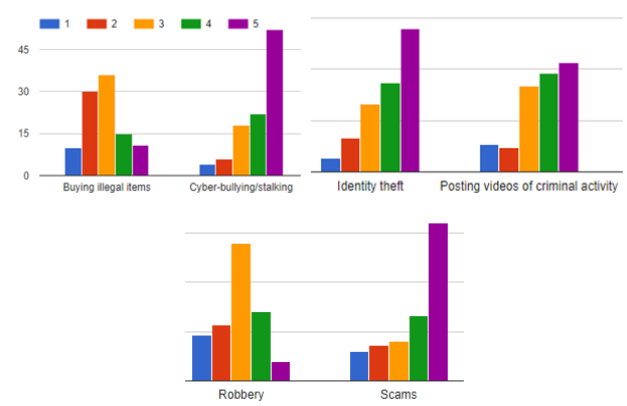

Fig. 6 Severity level of crimes

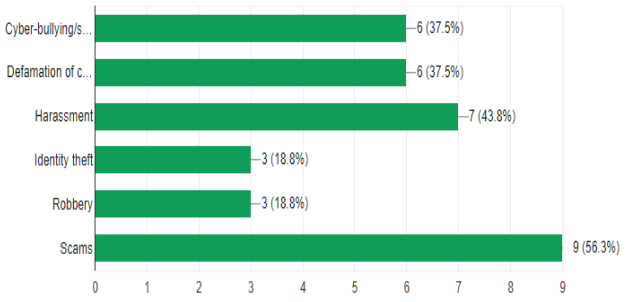

Fig. 7 Victims of social media crimes

In addition to the survey, secondary data from literature was explored during the course of this study and it was safe to say that cybercrimes had definitely created annoyance and inconvenience on the lives of the victims especially in situations, where finance was involved. Cybercrime was not limited to a single crime but rather an array of crimes including but not limited to hacking, stalking, spoofing, forgery, Identity Theft and many more [32]. According to [33] the top ten countries that were a source of cybercrimes in 2016 are shown in Figure 8, where USA is at the top followed by China, Brazil, India and so on.

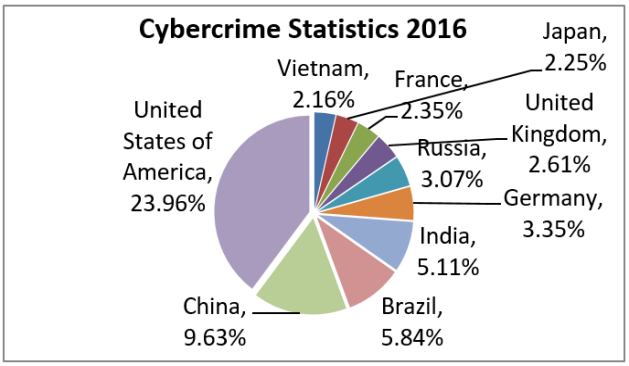

Fig. 8 Cybercrime statistics 2016 [33]

Due to the ever-increasing rate of these cybercrimes, it is estimated that by 2021, the cost of damages caused by these crimes will hit an annual figure of $6 trillion. Microsoft estimates that 4 billion people will be online by 2020 thereby increasing the surface attacks for humans [34].

With the immense use of social media networks nowadays, these crimes have shifted to new platforms that are providing criminals easy access to huge volumes of data. A very common crime that occurs through social media platforms such as Facebook is Social engineering [35]. When countries observe that certain social media platforms are becoming a major contributor to crimes, they often ban them as remedial methods. Figure 9 shows how different social media applications like Facebook, WhatsApp, Twitter, YouTube, Instagram, and Skype were ban in several countries in 2016 and the number of countries that had the most amount of user arrests due to their involvement in social media crimes [36].

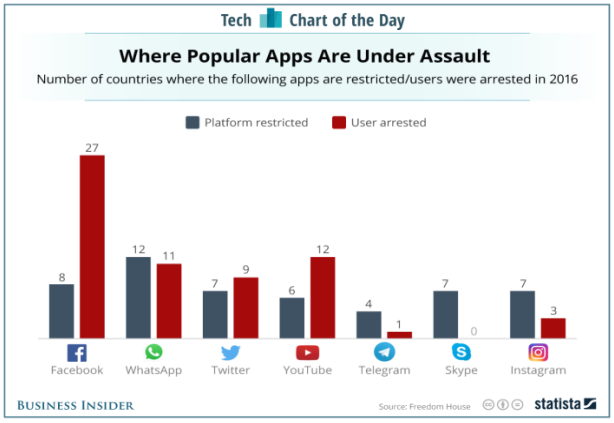

Fig. 9 Applications under assault [36]

Moving on to the specific crime of Identity Theft on Social Media platforms which was the main focus of our study, one must always keep mind that anything you do online can lead you to become victims of Identity Theft. This can start from as simple as posting a picture on Facebook or checking in on a location. It is estimated that annually 10 million Americans fall victims to online Identity Theft. Combined statistics from the Identity Theft Resource Center, The Aftermath Study, The Javelin report, The FTC, ID Theft Center.org and CBS New are reported in [37] as:

- It takes four years or longer for 9-18% of victims to realize that their IDs have been compromised.
- The victims suffer a loss of about $851 to $1378 on average on court cases.
- 47% of the victims face problems in getting credit cards because of Identity Theft
- About 11% of people who suffer from Identity Theft have trouble getting employed.
- 70% of the victims face multiple issues while trying to erase negative information from their records while some of them never succeed in doing so.
- 40% suffer from emotional stress
- 12% of them get arrest warrant issued against them for crimes that were committed by thieves.

Cifas (Credit Industry Fraud Avoidance System) a fraud prevention agency reported that 148,000 people had fallen prey to this crime in 2015 in the United Kingdom which was an increase of 56.6% since 2014 [38] [39]. In Australia 770,000 people were found to be victims of online identity theft in 2014 which had cost an individual about $4000 [40]. Furthermore, according to [4] each year about 15 million Americans identities used for fraudulent purposes that cause financial losses of more than $50 million. The victims are not only adults but children as well and about 1.3 million children's identities are misused annually [41]. According to a very recent statistic [42] [43], the crime of Identity Theft had hit an all-time high in 2016 in US where it was estimated that 15.4 million consumers were targets of some kind of ID fraud which amounted to a total of $16 billion of loses. The nature of social media to produce content through targeted advertisement has tricked its users into providing as much personal information as possible thereby increasing the number of users that fall prey to online identity theft [44]. The following section looks into how each of the top social media platforms affected by Identity Theft.

4.1 Facebook

Facebook being the most popular social network is a place that people have a lot of trust in. This is usually because they think their 'Friends' on Facebook are actually people they can trust. It was reported that one third of social media users provide no less than three pieces of information that can lead to stealing of their identity. This data can be names, date of births, pet names, phone numbers, mother's middle name etc. [45]. The different ways a thief steals someone's identity on Facebook as shown in Figure 10. The most common method was sending a private message to visit a Scam Website [46]. In 2012 Facebook admitted to a data leak that had caused the phone numbers and email addresses of 6 million users to be exposed to unauthorized users. This had happened due to a technical glitch in their database where users were provided with extra information which was supposed to be hidden when they wanted to download contact information of their friends [47] [48].

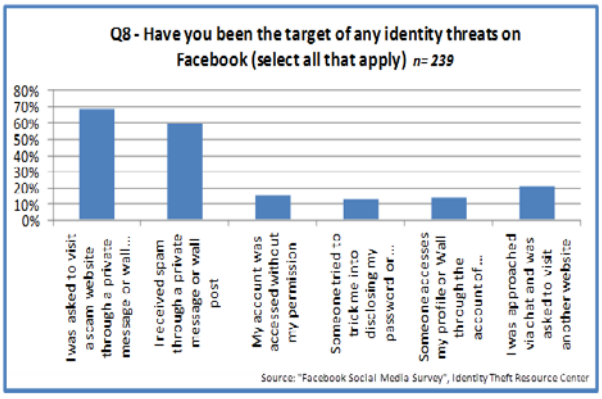

Fig. 10 Ways of Identity Theft on Facebook [46]

4.2 YouTube

YouTube is the second most used social media site with more than 30 million people visiting the site every day [49] and with over a billion registered users [50]. The issue of Identity Theft may not be as rampant as it is on other social networking sites, but it still persists. For example, a YouTube channel by the name "TheDiamondMinecart" that has over 12 million

subscribers has over 1000 accounts created with the same name. The purpose of these fake accounts is to re-upload the original content to have more views. There are many more popular accounts that are victims to impersonation and if all these revenue losses were to be summed up, it would be in six figures [51]. To combat this issue, YouTube recently introduced a change whereby users will not be able to gain any monetary profits until their channel had 10,000 lifetime views [52].

4.3 Instagram

Instagram is the third most popular social networking site with about 700 million daily active users [53]. But not all these are genuine users and according to a study conducted by Italian security researchers more than 8% of the accounts are fake or bot accounts [54] [55]. The purpose of these bot accounts have now transformed from just buying fake followers to actually stealing accounts for impersonation [56].

4.4 Twitter

Twitter is the fourth most popular social networking site among its counter parts, which means that it has also seen its fair share of security attacks. In 2013, Twitter announced that the information of around 250,000 users might have been compromised due to a phishing attack that was made on their network to steal the information of users [57]. This included passwords, email addresses and usernames of all those users of Twitter [58]. According to an analysis conducted by RAND Corporation, a Twitter account is costlier than buying a stolen credit card because it has greater rewards for the thief [59]. Furthermore, researchers in UK have found more than 350,000 fake accounts on Twitter that can potentially be used for various crimes [60] [61] while USC researchers estimate that 15% of Twitter accounts are not handled by humans but are in fact bot accounts. Out of the 319 million active users on Twitter, about 48 million are bot accounts [62].

4.5 Reddit

Reddit is the least popular social Website among its contenders with 250 million users to its name [63]. It is a virtual place where social content is gathered and curated by the users from all around the world, which is then promoted through voting by Reddit's registered members [64]. This social media platform actually has a story behind it. At the time of the birth of this website when it had no footprint on the internet, Reddit's creator Steve Huffman admitted himself that they had to create an army of fake accounts just to give it a boost and to give an impression that it was very popular [65] [66]. Although there may not have been lot of cases of Identity Theft in particular that led to financial or other loses, Internet shilling is something that has become quite common on these platforms. It happens when an organization poses as a genuine user and posts fake comments to change the course of a conversation and manipulate it the way they like [67].

Some countries have also claimed that when women get impersonated on these sites, they often suffer social and cultural ramifications [68]. As this crime has become very common on these platforms, the developers of these sites are now more vigilant and aware and are constantly taking measures to curb its affects. For example, due to numerous cases that emerged on Facebook that pointed towards Identity Theft, Facebook introduced a security feature that alerted its users in the form of an email or SMS whenever there was an unauthorized access to their account. This usually happens when someone tries to log into your account from a different location or from a device you do not normally use for logging in [69]. Similarly, Instagram has an option under its control setting where you can authorize or revoke certain third-party apps such as WordPress to access your accounts. Only applications that you think are authentic and are not involved in any kind of fraud should be authorize as some of these sites may be created for the sole purpose of Identity Theft by creeping into your personal details [70]. After reviewing all of the above statistics first in the form of primary data that our own survey provided and then through secondary data, it become evident that some precautionary and prevention techniques must be adopted in order to avoid situations of Identity Theft. The following section describes various methods that might prove to be helpful in the same regard.

4.6 Prevention Techniques

Social media has no doubt created an atmosphere and culture of unnecessary sharing and publicizing of personal information which should be kept hidden most of the time. This has eventually led criminals of Identity Theft to tap into these data and cause financial losses. Although sites like Facebook, Twitter etc. have taken considerable steps to curb the issue of online theft and protect user's privacy, it still remains a challenge for these organizations to allow them to share and interact limitlessly without pushing them to become victims of fraud [71]. As the trend of exploiting personal information is on the rise, it is important to take precautions on the user's end to avoid getting noticed and becoming victims to online identity theft. Perhaps the most effective method of avoiding becoming a victim to identity Theft is not creating a social networking account in the first place. But all thanks to the golden age and trend of social media sites, one is obligated and forced to use these platforms to stay up to date with the world. In these circumstances, the following

precautions should be taken when interacting on social media sites:

4.6.1 Never Display Details of Personal or Financial Documents:
This may seem like a pretty obvious step to many, but there are some people who just get over excited when they get a new credit card or their driver's license and want the whole world to know. So they post pictures displaying their achievements. This is something that criminals of Identity Theft are mostly looking for to steal identities. If you still decide to post pictures of your documents with your personals details on them, always blur out names and numbers printed on them [72] [73].

4.6.2 Turn Off Automatic Login Features:
Never allow social media application to auto log you in and also don't allow browsers to remember your log in details. In case if someone gets hold of your device, they won't be able to directly gain access to your account. Thus, preventing them from viewing your personal information [74].

4.6.3 Avoid Posting Location Updates:
When user's post about their vacations and whereabouts online, it gives the criminals solid information that they are going to be out of their homes at the time of update thereby allowing the thieves to break in and steal valuables or more importantly identifying documents to be used for impersonation [75].

4.6.4 Setting Stringent Privacy Settings:
In light of being aware that one's personal information such as name, photo, date of birth, location, place of work etc. are sensitive data, users should set their privacy settings such that they are visible to only themselves or to people they trust. This can be done by going into the settings of Facebook, Instagram, LinkedIn, Twitter accounts and changing the preferences for your personal data [76] [77].

4.6.5 Use of Strong and Unique Passwords:
This is the first and crucial step that one should adopt when creating an account on social media sites. Creating passwords that are strong, secure and unique such as making them alphanumeric with special characters helps in keeping identity thieves at bay [78].

4.6.6 Always Connect with Authentic People:
While this may not seem like a problem because when for example when someone sends you a request on Facebook, you can verify that person through his name, profile photo or some other apparent attribute. This is what criminals do when they impersonate someone. They use other people's real names and publicly available pictures to try to trap other users by posing as someone they know. So, it is always recommended that you authenticate that person by checking his mutual friends with you or see how far back his previous posts go [79] [80].

4.6.7 Using Double Authentication:
This is one feature implemented on some social media platforms that makes it harder for thieves to gain access to someone's account. For example, Twitter allows users to turn on a setting that asks users to enter a one-time code sent to their mobile phones when they log in for the first time from a particular device [79].

4.6.8 Avoid Using Same Passwords for Multiple Accounts:
This is a very common habit among people to use the same password for their different accounts mostly because it is easier and convenient to remember. This very habit had led to the hijacking of Mark Zuckerberg's Pinterest and Twitter accounts when his LinkedIn password was leaked because he had used the same password for all three accounts. Although it does seem like a hassle to keep different passwords for every account, it saves you from a lot of trouble in the long run [79].

4.6.9 Never Keep Credit Card Information Online:
Under all circumstances avoid storing information related to your credit cards on these social networking sites. If this information gets into the wrong hands, your identity will most likely be exploited [81].

4.6.10 Avoid Geo-Tagging Photos:
Not all photos you post on social networking sites need to have a location tag with them. It is always better not to reveal where a particular picture was taken as this shows where you have been. This is very crucial information for identity thieves as it shows a pattern of locations you usually go to [82].

4.6.11 Use of Protection Services:
Services like Identity Guard and LifeLock provide solutions against identity theft for safeguarding your social media accounts. If one feels they need professional services to protect their accounts, these services are the way to go [82].

4.6.12 Enabling Alerts of Unusual Activity:
Facebook and other application provide an option to enable alerts when someone else tries to log into your account from a different device or perhaps from a different location. It is always helpful to enable these notifications to prevent unauthorized people logging into your accounts [82].

5. Discussion and Future Work

The basic purpose of the survey that was conducted during the course of this study was to get an idea of how aware the general public is; when it comes to the knowledge of crimes that are conducted on social networking sites. It comes as no surprise that the usage statistics of these social media sites have seen a dramatic increase in the recent years. According to a survey conducted by the PEW Research Center, the number of adult users of social media sites in America increased from 5% to 69% from 2005 to 2016 [83]. This increase can clearly be mapped to the ability of these platforms to be so engaging and entertaining for all age groups. It is human nature to be curious about what others are doing in their lives and social media sites are perfect places that cater these needs. But like everything else around the world that provides benefits on one side, also has its own drawbacks on the other. Similarly, social networking platforms are no different. They may be providing ease in connectivity, but they also open doors for criminals who use it to their advantage. As the world of social networking has been around for a quite a time now, people are now realizing that it can do more than just what meets the eye. Coming back to the results of the survey that was conducted to collect our primary data, it showed that the sample comprised of an uneven distribution of people from continents such as Asia, North America, Africa, Australia, South America and Europe in the same order with respect to percentage. There were a greater percentage of women than men and the age group that became a majority who used these social networking sites was between 20 and 27 followed by age groups of 28-34, 13-19, 43-50, 35-42 and 50+ respectively. Additionally, as expected, only 2% of the population didn't have any social networking accounts. Out of the 98% that did have accounts, most of them were on Facebook followed by Instagram, Twitter, Google+ and Snapchat. This pattern of social media platform popularity was similar to the trend we saw in our secondary data.

Moving on to the main aspect of the survey related to awareness of social media crimes, 88% of the population said they were aware of the fact that these sites are being used to commit crimes while only 12% didn't think this was the case. An interesting statistic was seen when they were asked to rank the severity level of different crimes being committed on social media websites. Although people were aware that these platforms were being used to commit crimes, their perception of how extremely it affects its victims was varied. According to the population, among the various social media crimes, bullying/stalking had topped the list for being the most severe followed closely by Identity Theft and posting videos of crime online. Other crimes such as scams, robbery and purchase of illegal items were down the list. In practicality, Identity Theft leaves a greater impact on the victim both financially and emotionally. Digging a little deeper, the survey then proceeded to see how many were actually victims of any these crimes. It was found out that a small percentage of about 8% had been victims out which online scams were the most popular followed by harassment, stalking, character defamation, Identity Theft and lastly robbery. The last part of the survey ended with two questions which were related. The first one asked the respondents whether they had suffered from an emotional or financial turmoil to which the majority (61%) agreed to. The connected question inquired about whether a precautionary measure was taken or not after recovering from the impact of the crime to which 72% of the participants responded with a Yes. While the focus of this study was to identity the different aspects of Identity Theft on social media platforms along with latest statistics of how this crime is prevailing around the globe, it was found that past researches were mainly conducted on general crimes on social media and not focused on Identity Theft or any crime in particular. The collected secondary data in addition to the primary data from our survey indicates that the users of social networking sites are more observant and vigilant these days as compared to older times. But somehow, either due to ignorance or mere carelessness, they still fall prey to crimes such as Identity Theft. Furthermore, all the secondary data that has been gathered related to Identity Theft points towards some important and crucial information. Firstly, the repercussions of Identity Theft have always been severe and become even more catastrophic when money gets involved. Secondly, people need to become more careful when they provide their personal data on social media platforms and must restrict the availability of this data to people they trust. Last but not the least, anyone can become a victim of Identity Theft on social media sites but the activities of teenagers and adolescents must be monitored by their guardians to prevent their identities from falling into the wrong hands.

Without a doubt, numerous researches have been conducted in the past trying to find insights into the variety of crimes that take place on social media sites. Different studies have taken place to understand how these crimes have evolved over time. Similarly, as the crime of Identity Theft is not new, a number of investigations have been made in the form of surveys and experiments to see how someone's identity can be misused for fraudulent purposes. But all these studies have been conducted in traditional terms and not specifically on social media networks. As social media is the hot topic nowadays, future research needs to be done to see how specific crimes like Identity Theft are creeping into these websites that is used by almost everyone. Furthermore, latest statistics need to be drawn to see how Identity Theft has

increased since the introduction of social networking sites in the recent years.

References

[1] Merriam-Webster, Incorporated, "Definition of identity theft," 2017. [Online]. Available: https://www.merriam-webster.com/dictionary/identity%20theft. [Accessed 3 May 2017].

[2] Spamlaws.com, "The History of Identity Theft," 2017. [Online]. Available: http://www.spamlaws.com/id-theft-history.html.

[3] The United States Department of Justice, "IDENTITY THEFT," February 2017. [Online]. Available: https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.

[4] J. Velasco, January 2016. [Online]. Available: http://socialnomics.net/2016/01/13/4-case-studies-in-fraud-social-media-and-identity-theft/.

[5] J. Stroup, "The Many Types of Identity Theft," 28 March 2017. [Online]. Available: https://www.thebalance.com/the-8-types-of-identity-theft-1947176.

[6] S. F.H. Allison, A. M. Schuck and K. Michelle Lersch, "Exploring the crime of identity theft: Prevalence, clearance rates,and victim/offender characteristics," Journal of Criminal Justice, vol. 33, no. 1, 2005.

[7] Equifax, "A Lasting Impact:The Emotional Toll of Identity Theft," 2015.

[8] Office of Inspector General, U.S. Department of Health and Human Services, "Medical ID Theft / Fraud Information," [Online]. Available: https://oig.hhs.gov/fraud/medical-id-theft/.

[9] McAfee, "What is Criminal Identity Theft?," October 2014. [Online]. Available: https://securingtomorrow.mcafee.com/consumer/identity-protection/criminal-identity-theft/.

[10] Equifax, "The New Reality of Synthetic ID Fraud," 2015.

[11] M. Osakwe, December 2016. [Online]. Available: http://www.nextadvisor.com/blog/2016/12/15/what-is-synthetic-identity-theft/.

[12] B. Singer, 2013. [Online]. Available: http://www.parents.com/kids/safety/tips/what-is-child-identity-theft/.

[13] The Federal Trade Commission, August 2012. [Online]. Available: https://www.consumer.ftc.gov/articles/0040-child-identity-theft.

[14] Mountain Alarm, June 2016. [Online]. Available: https://www.mountainalarm.com/blog/9-most-common-types-of-identity-theft/.

[15] IRS, April 2017. [Online]. Available: https://www.irs.gov/uac/taxpayer-guide-to-identity-theft.

[16] J. van Dijck, in The Culture of Connectivity: A Critical History of Social Media, Oxford University Press, 2013.

[17] M. Fita, November 2012. [Online]. Available: https://www.brandignity.com/2012/11/6-reasons-why-social-networking-is-so-popular-these-days/.

[18] P. Kallas, June 2017. [Online]. Available: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/.

[19] G. Khoury, February 2017. [Online]. Available: http://blogs.findlaw.com/blotter/2017/02/5-common-types-of-social-media-crime.html.

[20] J. W. Patchin and S. Hinduja, "Lifetime cyberbullying Victimization rates," [Online].

[21] R. Byrne Reilly, "Buying a gun on Facebook takes 15 minutes," February 2014. [Online]. Available: https://venturebeat.com/2014/02/26/exclusive-buying-a-gun-on-facebook-takes-15-minutes/.

[22] G. Mohney, "Murder on Facebook spotlights rise of 'performance crime' phenomenon on social media," April 2017. [Online]. Available: http://abcnews.go.com/US/murder-facebook-spotlights-rise-performance-crime-phenomenon-social/story?id=46862306.

[23] N. Bilton, "Burglars Said to Have Picked Houses Based on Facebook Updates," September 2010. [Online]. Available: https://bits.blogs.nytimes.com/2010/09/12/burglars-picked-houses-based-on-facebook-updates/?_r=0.

[24] C. Chipurici, June 2016. [Online]. Available: https://heimdalsecurity.com/blog/how-to-prevent-identity-theft-20-steps/.

[25] R. Siciliano, November 2010. [Online]. Available: http://robertsiciliano.com/blog/2010/11/05/15-facebook-fiascos-to-watch-out-for/.

[26] K. A. Frenkel, February 2017. [Online]. Available: http://www.cioinsight.com/security/slideshows/cyber-criminals-found-a-home-on-social-media-sites.html.

[27] Elsevier, "Identity theft rises sharply as fraudsters target social media," Computer Fraud & Security, vol. 2016, no. 7, July 2016.

[28] P. Hoelscher, 2017. [Online]. Available: http://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-attacks-by-demographic/social-networks/#gref.

[29] Experian, "Facebook Fraud: Identity Theft through Social Networking," 2010. [Online]. Available: https://www.protectmyid.com/images/education_center/pdf/050TypesofFraud/7_types%20of%20fraud_social%20networking.pdf.

[30] MediaSmarts, [Online]. Available: http://mediasmarts.ca/digital-media-literacy/digital-issues/cyber-security/cyber-security-spam-scams-frauds-identity-theft.

[31] N. Farhoud, August 2016. [Online]. Available: http://www.mirror.co.uk/news/uk-news/how-hackers-can-steal-your-8576657.

[32] NCSA, 2017. [Online]. Available: https://staysafeonline.org/stay-safe-online/protect-your-personal-information/id-theft-and-fraud.

[33] J. Cook, May 2017. [Online]. Available: http://www.businessinsider.com/worlds-10-cybercrime-hotspots-in-2016-ranked-symantec-2017-5/#10-vietnam-216-1.

[34] S. Morgan, June 2017. [Online]. Available: http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html.

[35] J. Boone, 2011. [Online]. Available: http://www.iacpsocialmedia.org/wp-content/uploads/2017/01/NW3CArticle.pdf.

[36] E. Kim, January 2017. [Online]. Available: http://www.businessinsider.com/whatsapp-is-banned-by-the-most-number-of-countries-but-facebook-users-drew-the-most-arrests-2017-1.

[37] GuardChild, 2014. [Online]. Available: https://www.guardchild.com/identity-theft-statistics/.
[38] T. Evans, July 2016. [Online]. Available: http://www.telegraph.co.uk/money/consumer-affairs/sharp-rise-in-identity-fraud-as-scammers-use-facebook-and-other/.
[39] BBC News, July 2016. [Online]. Available: http://www.bbc.com/news/uk-36701297.
[40] M. Edwards, April 2015. [Online]. Available: http://www.abc.net.au/news/2015-04-14/identity-theft-hits-australians-veda/6390570.
[41] Z. Meyer, August 2018. [Online]. Available: http://www.freep.com/story/money/business/2016/08/28/child-id-theft-problem/89352016/.
[42] B. Sullivan, February 2017. [Online]. Available: https://www.usatoday.com/story/money/personalfinance/2017/02/06/identity-theft-hit-all-time-high-2016/97398548/.
[43] H. Weisbaum, February 2017. [Online]. Available: http://www.nbcnews.com/business/consumer/identity-fraud-hits-record-number-americans-2016-n715756.
[44] K. Lewis, 2017. [Online]. Available: http://www.anvilmediainc.com/marketing-resources/articles/social-media-id-theft-article/.
[45] R. Siciliano, May 2011. [Online]. Available: http://www.huffingtonpost.com/robert-siciliano/identity-theft-commited-u_b_243305.html.
[46] ProtectMyID, May 2012. [Online]. Available: http://blog.protectmyid.com/2012/05/04/social-media-threats-look-like-this/.
[47] G. Shih, June 2013. [Online]. Available: https://www.reuters.com/article/net-us-facebook-security-idUSBRE95K18Y20130621.
[48] S. Posel, June 2013. [Online]. Available: https://www.occupycorporatism.com/security-breach-facebook-apologizes-for-private-user-data-stolen/.
[49] D. Donchev, March 2017. [Online]. Available: https://fortunelords.com/youtube-statistics/.
[50] YouTube, 2017. [Online]. Available: https://youtube.com/yt/press/statistics.html.
[51] T. Lince, October 2016. [Online]. Available: http://www.worldtrademarkreview.com/Blog/detail.aspx?g=77175963-7d5b-4bf1-b82e-d3b4eda42f92.
[52] B. Popper, April 2017. [Online]. Available: https://www.theverge.com/2017/4/6/15209220/youtube-partner-program-rule-change-monetize-ads-10000-views.
[53] S. Aslam, June 2017. [Online]. Available: https://www.omnicoreagency.com/instagram-statistics/.
[54] L. O'Reilly, July 2015. [Online]. Available: http://www.businessinsider.com/italian-security-researchers-find-8-percent-of-instagram-accounts-are-fake-2015-7.
[55] K. Bell, April 2017. [Online]. Available: https://www.cultofmac.com/477737/instagram-finally-cracking-fake-accounts/.
[56] K. Knibbs, March 2014. [Online]. Available: https://gizmodo.com/watch-out-for-the-identity-stealing-spambots-of-instagr-1630093878.
[57] J. Hamada, February 2013. [Online]. Available: https://www.symantec.com/connect/blogs/phishing-easy-way-compromise-twitter-accounts.
[58] J. Mali. [Online]. Available: http://www.lifehack.org/articles/technology/identity-theft-through-social-networking-lessons-take-now.html.
[59] E. Markowitz, August 2014. [Online]. Available: http://www.vocativ.com/tech/internet/twitter-hack/.
[60] Hindustan Times, January 2017. [Online]. Available: http://www.hindustantimes.com/tech/twitter-has-massive-networks-of-fake-accounts-report/story-GikvXCTgY06ySmBmoJYGkO.html.
[61] BBC, January 2017. [Online]. Available: http://www.bbc.com/news/technology-38724082.
[62] M. Newberg, March 2017. [Online]. Available: http://www.cnbc.com/2017/03/10/nearly-48-million-twitter-accounts-could-be-bots-says-study.html.
[63] C. Smith, May 2017. [Online]. Available: http://expandedramblings.com/index.php/reddit-stats/.
[64] M. Rouse, December 2016. [Online]. Available: http://searchcio.techtarget.com/definition/Reddit.
[65] D. Mead, June 2012. [Online]. Available: https://motherboard.vice.com/en_us/article/z4444w/how-reddit-got-huge-tons-of-fake-accounts--2.
[66] Pipes to Platforms, 2015. [Online]. Available: http://platformed.info/seeding-youtube-megaupload-paypal-reddit/.
[67] J. McGregor, February 2017. [Online]. Available: https://www.forbes.com/sites/jaymcgregor/2017/02/20/reddit-is-being-manipulated-by-big-financial-services-companies/#471b12424c92.
[68] L. Smith, May 2014. [Online]. Available: https://thecybersafetylady.com.au/2014/05/facebook-identity-theft-scam-rise/.
[69] Damien, May 2010. [Online]. Available: https://www.maketecheasier.com/receive-facebook-alert-for-unauthorised-access/.
[70] M. Medina, October 2015. [Online]. Available: https://www.identityforce.com/blog/instagram-privacy.
[71] J. Lawrence, August 2016. [Online]. Available: https://memeburn.com/2016/08/identity-theft-social-media/.
[72] Security First Insurance Company, April 2015. [Online]. Available: http://www.securityfirstflorida.com/blog/identity-theft-prevention-tips-for-social-media.
[73] J. Mali, August 2013. [Online]. Available: http://www.sitepronews.com/2013/08/26/social-media-id-theft-scams-and-how-to-prevent-becoming-a-victim/.
[74] McAfee, March 2014. [Online]. Available: https://securingtomorrow.mcafee.com/consumer/family-safety/10-tips-protect-social-networks/.
[75] TransUnion, 2017. [Online]. Available: https://www.transunion.com/article/5-identity-theft-traps-to-avoid-on-social-media.
[76] J. Myhre, March 2013. [Online]. Available: http://www.businessnewsdaily.com/4194-social-media-security-tips.html.
[77] E. O'Loughlin, August 2016. [Online]. Available: https://securityintelligence.com/identity-theft-and-social-media-how-are-they-related/.
[78] D. Drager, January 2011. [Online]. Available: http://www.makeuseof.com/tag/9-ways-prevent-identity-theft-online-activities/.

[79] J. Steinberg, August 2016. [Online]. Available: https://www.inc.com/joseph-steinberg/8-ways-to-avoid-scams-when-using-social-media.html.
[80] P. Paganini, October 2013. [Online]. Available: http://securityaffairs.co/wordpress/19143/cyber-crime/social-media-security.html.
[81] A. Levin, February 2014. [Online]. Available: http://www.huffingtonpost.com/adam-levin/7-ways-to-avoid-identity_b_2634967.html.
[82] S. Strouvali, March 2015. [Online]. Available: https://securitygladiators.com/2015/03/06/protect-yourself-against-facebook-identity-theft/.
[83] Pew Research Center, January 2017. [Online]. Available: http://www.pewinternet.org/fact-sheet/social-media/.
[84] E. Copp, August 2016. [Online]. Available: https://blog.hootsuite.com/social-media-for-business/.

Shareen Irshad received her B.E in Software engineering from NED University of Engineering and Technology, Pakistan in 2014. She is currently pursuing her MS degree in Computer Science from SZABIST Dubai. Her research interest includes Social Media security and applications implemented through Internet of Things.

Tariq Rahim Soomro, Professor of Computer Science at College of Computer Science & Information Systems, Institute of Business Management, has received BSc (Hons) and M.Sc degrees in Computer Science from University of Sindh, Jamshoro, Pakistan and his Ph.D. (1999) in Computer Applications from Zhejiang University, Hangzhou, China. He has more than 23 years of extensive and diverse experience as an administrator, computer programmer, researcher and teacher. He has published over 70 peer-reviewed papers. He is Senior Member of IEEE, IEEE computer society and IEEE Geosciences & RS Society since 2005 and IEEE Member since 1999.