Identity Theft (Emerging Trends in Security Issues in Information Security)

S. Brindha K. Swetha
3rd-year CSE
Associative Professor: R. Kavitha
Parisutham Institute of Technology and Science

Abstract:**The quintessential crime of the information age is identity theft, the malicious use of personal identifying data.In this paper we model identity and its use in credit transactions.whereas type of identity theft occur in equilibrium, including new account fraud, existing account fraud, and friendly fraud.**

I. INTRODUCTION:

The meaning of "Identity theft" can be visualized from multiple aspects but they all boil down to one basic definition , 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 . 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 preapproval 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. The evolution of Identity Theft can be seen in Table 1 from as early as 1800s to its predicted state in 2020 .

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

Table1:Evolution of Identity Theft.

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.

Traditional Materials and Methods:
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.

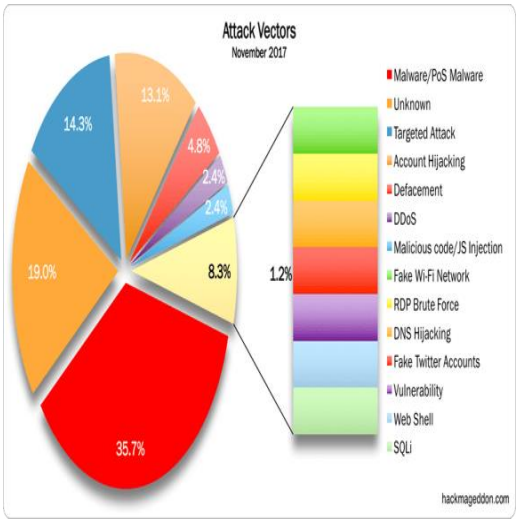

Figure:1 Attack vectors

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.

II. LOW TECHNOLOGY / TRADITIONAL METHODS OF IDENTITY THEFT :

1.Financial Identity Theft:
This usually involves fraud with bank accounts and credit cards . There are several techniques offender uses to perform financial Identity Theft.

• 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 .

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 .

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. .

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. 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 .

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. 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 .

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.

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.

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 such as watsapp ,facebook,twitter etc..

III. TOP SOCIAL MEDIA CRIMES:

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 Figure2 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.

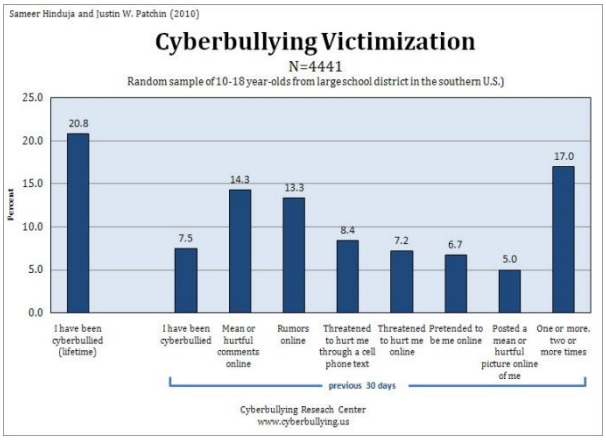

Figure:2 Cyberbulling Victimization

2.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

3.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. 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.

4.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.

Figure 3:business spying

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 ecommerce 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. 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. 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.

IV. 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 studyaccumulated 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

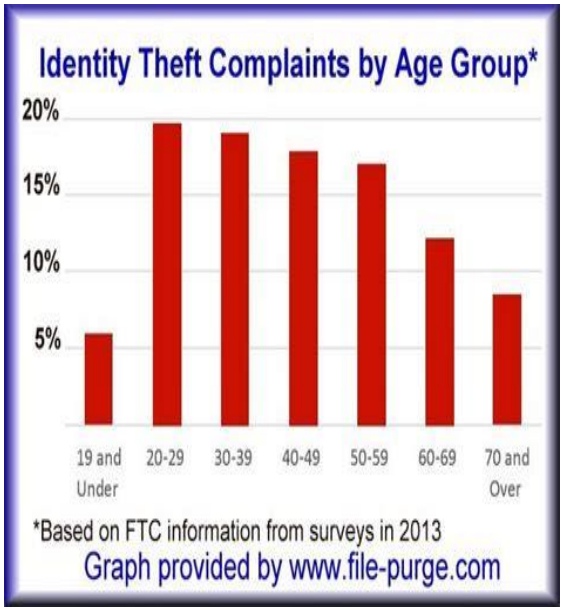

Figure:4 Identity Theft Complaints By Age Group

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.

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%) . These victims also confessed to suffering emotional and financial burdens.

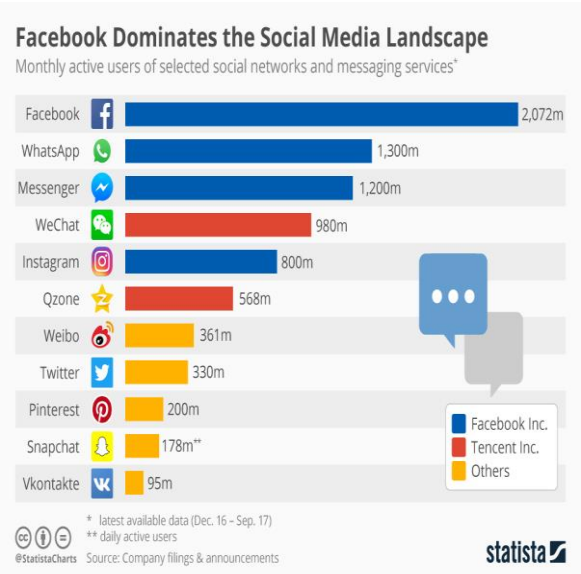

Figure:5 social media usage

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 . According to 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.

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.

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.

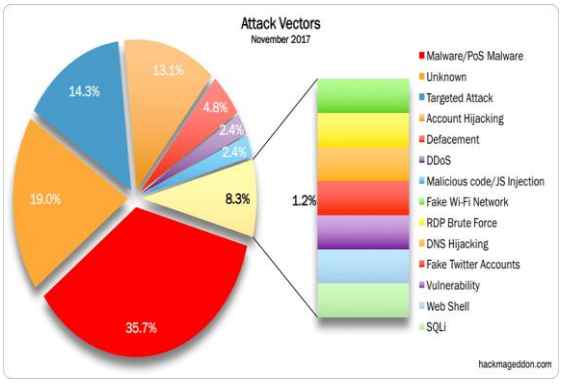

Figure:6 Attack Vectors

V. 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 followingprecautions should be taken when interacting on social media sites

Never Display Details of Personal or Financial Documents.

- Turn Off Automatic Login Features
- Avoid Posting Location Updates
- Setting Stringent Privacy Setting
- Use of Strong and Unique Passwords
- Always Connect with Authentic People
- Using Double Authentication
- Avoid Using Same Passwords for Multiple Accounts
- Never Keep Credit Card Information Online
- Avoid Geo-Tagging Photos
- Use of Protection Services
- Enabling Alerts of Unusual Activity:

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. 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.

VI. CONCLUSION:

In this paper ,we present the effects of identity theft ,in which range it is growing to a extend and our steps to make our file safe and secure. Identity theft is a widespread problem affecting approximately 8 million people each year. To understand the crime of identity theft and thus increase the likelihood that policymakers and law enforcement are effective in reducing this crime, more research needs to be done. First, a number of laws have been passed to provide help to consumers and victims of identity theft and to assist law enforcement; however, the effectiveness of these laws has not yet been assessed. Although much of this legislation is relatively new, future research should evaluate the degree to which legislation is an effective strategy in reducing identity theft. Second, there is very little research on identity thieves themselves. Researchers should consider further developing this line of inquiry by expanding the work of Copes and Vieraitis (2007) to include active offenders and offenders convicted at federal, state, and local levels.

REFERENCES:

[1] Merriam-Webster, Incorporated, "Definition of identity theft," 2017. [Online]. Available: https://www.merriamwebster.com/dictionary/identity%20theft. [Accessed 3 May 2017].
[2] Spamlaws.com, "The History of Identity Theft," 2017. [Online]. Available: http://www.spamlaws.com/id-thefthistory.html
[3] J. Velasco, January 2016. [Online]. Available: http://socialnomics.net/2016/01/13/4-case-studies-in-fraudsocial-media-and-identity-theft
[4] Z. Meyer, August 2018. [Online]. Available: http://www.freep.com/story/money/business/2016/08/28/child-id-theft-problem/89352016/.
[5] A. Levin, February 2014. [Online]. Available: http://www.huffingtonpost.com/adam-levin/7-ways-toavoid-identity_b_2634967.html
[6] K. Bell, April 2017. [Online]. Available: https://www.cultofmac.com/477737/instagram-finallycracking-fake-accounts
[7] YouTube, 2017. [Online]. Available: https://youtube.com/yt/press/statistics.html