Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 May 2020 doi:10.20944/preprints202005.0330.v1

IDENTITY THEFT IN SOUTH-EAST ASIA: CAUSES AND PRECAUTIONS

AKM BAHALUL HAQUE[1], RABEYA SULTANA[2], MOHAMMAD SAJID FAHAD[3] AND TALEBUL ISLAM[4]

[1]Department of Computer Science and Engineering, North South University, Dhaka, Bangladesh
bahalul.haque@northsouth.edu
[2]Department of Computer Science and Engineering, North South University, Dhaka, Bangladesh
rabeya.sultana1@northsouth.edu
[3]Department of Computer Science and Engineering, North South University, Dhaka, Bangladesh
mdsjdfhfd@gmail.com
[4]Department of Computer Science and Engineering, North South University, Dhaka, Bangladesh
talebulislam@northsouth.edu

ABSTRACT

As technology evolves, our digital footprint keeps increasing. Now, everything we do is largely related to us being online, connected and logged. Therefore, if someone's online data is exposed, then their life will be compromised. This is called identity theft and in this era of technology, it has become one of the most serious forms of crime. When someone's data is compromised, there is a huge chance of harming the person financially, morally and socially. New technology and the knowledge gap it creates when it first comes out is perfect for identity thieves to exploit. If we are not cautious, our future will be very different than what we dream of due to the very technology created to make it better. Hence, we need to understand the technology, identify the loopholes and educate ourselves to avoid being held captive by our digital footprint.
.

KEYWORDS

digital footprint; exploit; identity theft; technology

1. INTRODUCTION

Identity theft [1] is the crime of acquiring personal information of another person for the sole purpose of assuming that person's identity or name to make transactions or purchases. Identity theft is committed in many different ways. Some identity thieves go through personal belongings, electronic devices, social accounts or even trash to find more about their target. Other methods include using their understanding of high tech corporate databases to steal lists of customer information. Several tools are can be also used in the process of fishing information. Once they have the information they are looking for, identity thieves can do whatever they want ranging from ruining their records to using the information to become that person entirely.

2. Hacker's Motive

The term "Motive" sounds negative while illustrating someone's intention to harm the other one. From the word motive, people do urge for "motivation".

Every coin has two sides to motivation. As good hackers (ethical hackers) and bad hackers (unethical hackers) both exist so there must exist a thick line difference between their motives. So here, the cases that should arise first are "From where the motive behind those hackers do generates from" and "why do they start hacking". Depending on the categories of hackers, the motive can be divided into two categories:-

Good motives may include:

- First, the aim is to help gain access to an infected device whose login password has been changed by other malicious software, people or by any means.
- To help any organizations to get back its data whose private information has been leaked
- To keep track of any illegal activities going on the web by " Man-In-The-Middle" approach
- To catch those unethical hackers who have caused harm to any organizational devices.

Bad motives may include:

- Due to any sort of personal enmity (revenge), bad hackers try to gain access to the victim's device to cause severe harm by changing and destroying data.
- They may cause harm to celebrities due to defame them so they can also change the victim's password so that they can get access to any social media sites and make illegal use of their information and pictures (defame).
- They can attack any bank's account for transferring all money to their account to become rich (financial gain).

3. The topology of the effect

There may be many types of identity theft but the division of their types is mainly based on how the victim's personal information was misinterpreted and misused. [2]

1. **Credit Card or Debit Card Identity Theft:** Some fraudsters gather another person's information through plastic cards also called credit or debit cards. Under some relevant laws, it can be said that if the fraudulent use someone's credit card, that is also a form of identity theft [2].

2. **New Account Identity Theft:** Once the fraudsters gather the information then they use that information to create a different or maybe the same identity just like the victims. That personal information is used to open new accounts in their name to make other frauds. This sort of identity theft is named as New Account Identity Theft [3, 4].

3. **Existing account takeover identity theft:** Apart from making a new account to harm victims, there also exists a kind of identity theft where criminals can achieve access to existing accounts of the victims. Once they get full access to the victim's existing account, they can claim any information regarding that person's accounts. This kind of identity theft is called an Existing account takeover identity theft [5].

4. **Tax Identity Theft:** Some people do not pay taxes. These thieves use this opportunity to pay off the tax and get their TIN. Later on, that TIN can be used for other cases [5].

5. **Employment Identity Theft:** In some countries, people use SSN that is called Social Security number. The person who cannot get a job due to criminal records or poor credit will try to steal the Social Security number of some educated people to get a job in their name. This is called Employment Identity Theft [5]

6. **Senior Identity Theft:** These cannot be generalized into other categories of identity theft but these people almost suffer from all types of identity theft other than children or elderly identity theft [5].

7. **Estate Identity Theft:** People are immortal but their information is mortal. Even after death, identity theft does not stop because a fraudster still can use that person's information to gain access to his accounts and other sectors [5].

8. **Financial Identity Theft:** People do keep their money in banks and financial institutions to be sure that money is safe. But fraudsters even can gain access to victim's bank accounts to get control over all the money [3].

9. **Medical identity theft**: Fraudsters use other people's insurance information so that they can receive medical treatment on free by the victim's name whose information has been stolen. This is known as medical identity theft [3].

10. **Criminal identity theft**: Committing crimes will ultimately lead to jail for many years. So to avoid going to jail or to be safe from any sort of punishment, some criminals use other people's information as their identity to hide their own identity [3].

11. **Driver's license identity theft**: Drivers should be more careful regarding their driving license because hackers may steal the license. They will sell it to someone who looks like the driver and that might cause huge trouble later on. [3].

12. **Social Security identity theft**: Fraudsters use SSN to cause harm to some people. This important information can be used by many fraudsters to avoid taxes. This will also help them to commit other illegal activities [3].

13. **Synthetic identity theft:** Combining the information of victims to create a new identity is more powerful. This process is called Synthetic identity theft.[3].

14. **Child identity theft**: kids are less used to modern technologies and less even don't have access to credit cards so kids can also become victims of identity thief but in less amount. They are usually victimized by family members themselves as they are the only people that have exclusive information about the children [3].

15. **Business identity theft**: In this kind of identity theft, the fraudster uses the name of the business, the organizations or the enterprise for performing illegal activities. They try to get loans on by using those organization's names [3].

4. SOURCE OF THE INFORMATION BREACH

To identify the source of this information breach we first need to take into account how the theft is done:

1. **Credit Card or Debit Card Identity Theft:** Credit card fraud is when the fraudster uses your credit card or credit account to make a purchase you didn't authorize. If you lose your credit card or have it stolen, it can be used to make purchases or other transactions, either in person or online. Fraudsters can also steal your credit card account number, PIN and security code to make unauthorized transactions, without needing your physical credit card.
2. **New Account Identity Theft**: This is usually done by making a social account with accurate name, picture, and general information. The thief then impersonates as the person using this fake profile and hides behind the internet.
3. **Account takeover identity theft:** This is one of the crucial forms of identity theft. This is more effective as the user's account is compromised. Speaking it from a social network perspective, the account will already have valuable information within it. The account will have chat history, likes, dislikes and personal pictures that the thief can easily get their hands on. This is more devastating as causing anything in this account will cause less suspicion and will have a great deal of information.
4. **Estate Identity Theft:** This form is very famous in developing countries where there is less digitalized documentation. There are two main types. One, the person impersonates as the owner of the estate or the property and sells them the property. This is surely a fake and the intention is to get the money. The other one can be that the person acts to be someone else and sells a piece of land that does not belong to him.
5. **Driver's license identity theft**: This is very common among corrupted countries, here the driver uses fake licenses to get anything they want.

Social Security identity theft: This only occurs in most developed countries as in developing countries there is less of a database. However, as counties develop people are new to the idea and thieves take that as an advantage. So, regular citizens are used for their social security number or some countries' voter ID number. Once someone has that someone can access almost anything. During the time the government took to implement precautions, many took advantage of it.

6. **Identity theft in Photocopy Center -** Identity theft is a major issue worldwide. Many countries over the world are a victim of this issue. European countries are more vulnerable to this type of crime as technologies there are more advanced for hackers. Southeast Asian countries are also affected by this crime. The procedure of being the attack on this sort of theft is already discussed. But many of us always forget to figure out some minor issues that can change into a major issue. For example, the risk of using a photocopy center for copying any documents. In Southeast Asian

countries, a huge amount of people use the photocopy center for a regular academic, business, job or personal purposes. But there are huge risks of using it, especially in Southeast Asian countries where law enforcement is not that strict. The risks are discussed are below:

- Sometimes, we need to make a photocopy of our NID (national identification card) for educational, job or business purposes. If the photocopy worker keeps one extra photocopy of your NID then he can use that for identity theft purposes.

- Bank papers are more at a crucial risk if there are photocopied from photocopy centers. That is why; almost every bank has its photocopy machine to avoid identity theft.

- Some students do the photocopy of their board result certificate. This can be used as identity theft purpose for making fake results by that same name or making some new identity.

- 4. Tax paper or trade license paper are more at a risk for businessman because it can be used to make or start a new business by that same name.

Therefore, to avoid this sort of risk, every institution should have its photocopy machine. Even, ordinary people should also buy this for their home.

5. VULNERABILTY IN THE SYSTEM

As time passes, identity theft has gradually increased in day-to-day life. As everything happens for a reason, so does identity theft. Some motives behind identity theft have already been discussed, so now the question may arise “**how and why** identity theft has been gradually increasing"?

Before going into the concepts of “**how and why**”, it should be highlighted that which countries are more vulnerable to identity theft. As seen in The Straits Times [6], Asian people are more vulnerable to identity theft especially ATM cards, credit cards, and debit card identity theft. In Southeast Asia, ATM-related fraud issues affected 42 percent of people.

The Straits Times [5], it has been mentioned that about 35 percent of South-east Asian people were more worried about identity theft based on data violation. So this data violation and stealing data has been the main issue and the root cause that has caused a faster growth in identity theft. ATM cards consist of very private personal information. It has PID (personal identification number), bank information, home addresses, and most important signatures of the customer whether electrical or manual [5]. So this data and information are collected by hackers through different websites. After collecting this data, hackers modify and create a new identity by using those data. Moreover, the most dangerous thing that also happens is that they use the same information about the victim so that they can get access to all the money accounts of the victim.

Identity theft is increasing day by day due to the " Easy Exploitation of finding Weaknesses in Specific Technologies and Information Systems”[6]. Here also the credit card fraud is playing a major role in Asian countries that targets a specific technology which is ATM cards, Debit cards, and Credit cards. Either the fraudster uses several procedures to change credit cards that are stolen from victims or they have collected from various websites by illegal access to get access to victim's financial records [7]. So in this way, identity theft is gradually increasing in Asian countries.

Asian countries are more vulnerable to identity theft. Some reasons are illustrated below:

1. **Use of Manual Databases**: Before the use of the electronic database, there exist manual databases. Even nowadays, there are some Asian countries like India, Pakistan and Bangladesh uses manual databases for business purpose as well as educational purposes in the village. Some fraudsters steal information from those manual databases to create a new identity for the use of using one person's identity to commit a crime that leads to criminal identity theft.
2. **Financial Needs:** While visiting any website, sometimes there comes some request that wants personal information while pretending to be doing a security check. But those are fraudsters that are fooling people around. So as Asian countries are not yet developed countries and they are economically they are not rich, so the number of poor and needy people are more there. So there exist some people who want to be rich through illegal way and they choose the way of hacking to invade bank accounts, atm cards, credit cards or debit cards. So due to these reasons, Asian people are more affected easily by identity theft.

3. **Avoiding Arrest:** A criminal may save himself from being arrested by using another's identity instead of already having a criminal record. So it means that the police will be looking for that person to get arrested, not the true criminal. These sorts of criminal identity theft occur more in Asian countries as people of those countries have no such strict law to follow so criminals use this procedure to have themselves and harm others.

6. AFTERMATH (IMPACT ON VICTIMS)

As each coin has two sides, identity theft also has two sides in the case of its victim. "Identity theft can be called **Dual Crime** [7]". It is termed as so because it usually affects two victims. The first victim is the one whose identity is stolen and the second one is the organization whose services are stolen.

The victims can be categorized into three types. They are illustrated below:

1. **Children as victims of identity theft:** The Identity Theft Resource Center also reports that every week there are only 2 to 3 new child cases. Ultimately it shows that a minimum of 104-156 child victims per year which is very less in the amount [8]. Therefore, it can be concluded that the rate of children as victims is low compared to other victims. Children are not more use to technologies, business or any institutions so they are less vulnerable to be affected by other people from these sectors. Usually, it has been seen that some family members are more likely to commit this type of identity theft since they have almost all the access to the child's "identity" as well as information [6]. Due to these reasons, children lose their trust in family members; they became depressed, which ultimately hamper their mental state at such a young age. Their education is also affected

due to these reasons as they cannot concentrate on anything because as they are still so young so it takes a lot of time for them to overcome compared to elder people.

2. **Institutional victims:** Some organizations and institutions are victims of identity theft. These institutions can be educational, business, information technology, and armed services. It has been seen that institutional victims are more in number more to others [7]. Students and service holders may be at a higher risk compared to others. Some countries use Social Security Numbers (SSN). This is also used among institutions of higher learning. These people have more possibilities for getting a credit, debit or ATM card. Ultimately, this leads them to get associated with identity theft issues like Social Security identity theft or Credit card identity theft [8]. Due to these reasons, their lives are greatly hampered as they suffer from the financial crisis as their accounts are hacked which ultimately leads to mental depression.

3. **The elderly as victims:** Elderly people over the age of 65 are less likely to get involved in any sort of identity theft like credit card identity theft or money transactions on a routine. As a result, they are less likely to get involved by identity theft. The main problem with these adults is that they usually do not file any complain even if they are victimized. It has been seen that adults aged over 55 were less enthusiastic to complain a report against identity theft that happened with them within the past 5 years was 9 percent than the population as a whole, which was 13 percent [10]. These old people are not much affected as they are either retired from the job, dependent on their children or living in an old home so these financial losses do not affect them much compared to their families which take their responsibilities.

7. CAVEATS BEFORE STATISTICS

When reviewing or gathering any type of agency data or statistics, several additional caveats must be taken into account. They are illustrated below:

1. Not many attempts are made to differentiate between the problems of identity theft from the problem of identity fraud. This should be considered and taken into account while gathering statistics so that these are not mixed up. To be on the safer side, both data can be collected separately [7].

2. When it comes to the time to estimate or gather the specific features of identity theft from existing agency data, then it is quite difficult to do so but that does not mean that the information is not useful. It is quite impossible to separate water from oil, but due to the new acknowledgment of identity theft as a specific crime, agencies are likely to reshape how they gather and record information to include identity theft [7]

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 May 2020 doi:10.20944/preprints202005.0330.v1

7.1 Tables showing Statistics

Identity Theft Type	Theft Sub-type	Reports	Difference From Previous Year	Reference
Credit Card Identity Theft	New Accounts	130,928	+24%	[11]
	Existing Accounts	32,329	-6%	
Employment or Tax-Related Identity Theft	Tax Fraud	38,967	-38%	[11]
	Employ Wage-Related Fraud	30,592	+44%	
Phone or Utility Identity Theft	Mobile Telephone–New Accounts	33,466	+28%	[11]
	Utilities–New Accounts	21,994	+0%	
	Landline Telephone	7,738	+28%	
	Mobile Telephone	4,983	+6%	
	Landline Telephone	1,453	+25%	
	Utilities	1,322	+20%	
Bank Identity Theft	Debit Cards, Electronic Funds Transfer or ACH	23,219	+0%	[11]
	New Accounts Fraud	19,639	+12%	
	Existing Accounts	12,990	+2%	
Lease or Loan Identity Theft	Business or Personal Loan	20,328	+82%	[11]
	Auto Loan\Lease	18,815	+89%	
	Non-Federal Student Loan	6,327	+78%	
	Apartment or House Rented	5,439	+50%	
	Real Estate Loan	5,178	+17%	
	Federal Student Loan	5,082	+119%	
Government Document Identity Theft	Government Benefits Applied For\Received	16,021	-10%	[11]
	Other Government Documents Forged	5,645	+5%	
	Driver's License Forged	4,493	+19%	
	Passport Forged	703	+35%	
Other Identity Theft	Other	87,765	+121%	[11]
	Medical Services	13,833	+103%	
	Online Shopping or Payment Account	10,294	+18%	
	Social Media	9,439	+23%	
	Evading the Law	4,439	+7%	
	Insurance	3,675	+24%	
	Securities Accounts	1,877	+15%	

Table 1. Identity Theft Types

 doi:10.20944/preprints202005.0330.v1

Year	Identity Theft
2001	86,250
2002	161,977
2003	215,240
2004	246,909
2005	255,687
2006	246,214
2007	259,314
2008	314,587
2009	278,360
2010	251,074
2011	279,191
2012	369,958
2013	290,098
2014	332,545
2015	490,112
2016	398,952
2017	371,034
2018	444,602

Table 2. Identity Theft notified to the authority (Europe)

Identity Theft Type	=<19	20-29	30-39	40-49	50-59	60-69	70-79	>=80
Bank Identity Theft	1,405	9,055	11,508	9,575	8,444	6,531	2,852	1,053
Credit Card Identity Theft	1,565	24,863	40,182	32,048	24,095	16,214	6,363	1,980
Employment or Tax-Related Identity Theft	7,860	13,747	13,803	10,585	9,051	6,203	2,455	1,186
Government Documents or BenefitsFraud Identity Theft	1,071	3,326	4,600	4,638	3,963	3,988	1,462	824
Loan or Lease Identity Theft	830	10,596	15,556	11,459	6,391	2,847	820	249
Other Identity Theft	2,118	20,448	31,878	23,461	14,876	8,524	3,164	988
Phone or Utilities Identity Theft	957	13,468	18,027	12,621	8,586	4,979	1,637	528

Table 3: Identity Theft faced per age group

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 May 2020 doi:10.20944/preprints202005.0330.v1

7.2 Tables showing Statistics in South East Asia

Southeast Asia is the home to many developing countries with the emerging use of modern technology like digital national identity card system and birth certificate for almost anything in the system including banking. A recent study shows the victim of identity theft in such areas.

Country	Worried	Neutral	Not worried
China	44%	30%	26%
India	65%	18%	17%
Malaysia	57%	19%	24%
Singapore	63%	29%	8%

Table 4: Percentage of people worried about identity theft

Country	Strongly	Neutral	Other
China	83%	11%	6%
India	71%	15%	14%
Malaysia	77%	12%	11%
Singapore	67%	24%	9%

Table 5: Percentage of people thinks security is the most important element online

Country	Strongly	Neutral	Less	Not Willing
China	9%	32%	37%	37%
India	26%	33%	27%	14%
Malaysia	8%	28%	42%	22%
Singapore	4%	35%	36%	25%

Table 5: Percentage of people thinks security is the most important element online

As per the data above, many citizens of the developing countries are now aware of identity theft. Now many are insecure about sharing their personal information online and they are aware of the consequences if someone's information is to be leaked. So now is the time to spread awareness so that people listen and avoid being exploited.

The main issue is found in developing countries. However, these countries are slowly increasing their defenses after facing many attacks. Bangladesh Bank has been facing similar attacks. If not by their own, countries are hiring some experts to fortify their positions.

7. SOLUTION

In today's modern era, identity theft is a big challenge for us. By protecting our personal information we can minimize this risk. To ensure the protection of personal information there are few main ways and these are given below:

1. Always Keep Personal information Secure Offline: [13]

- Make sure all identification and financial documents are in a safe and private place.
- Make sure your wallet and purse keep in a safe and private place at work.
- At the swiping time of credit or debit card at the ATM Booth, make sure there is no one behind on you. [12]
- Keep eye tracking in the charges on the credit card statements every month.
- Try to limit your carry. Keep your Social Security Card at home and memorize your Social Security number.
- Check credit card report in every month
- Personal information can be provided only when:
  – You know how it will be used.
  –You know how they will safeguard it.
  – Make sure you know the basic detail information with whom you are dealing with.
- Social Security number can be provided only when you need to provide it and to those, you know and ask why this number is needed and how it will be used.
- Document s that has no need any longer (such as receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, etc), should be shredded.
- Make sure in your house your mailbox is fully secured so that other people can't access it. Try to post outgoing mail in post office collection boxes.

2. Always Keep Personal information Secure Online: [13]

- Don't share any personal information through phone, mail or over the internet without knowing the source very deeply.
- Remove personal information such as username, password, email, etc using a "wipe" utility program to overwrite the entire hard drive before disposing of a computer to others.
- Use a strong password by using a complex combination of numbers and upper and lower case letters so that nobody can guess it.
- Don't share every movement of your daily life on social media.
- Never login to your online personal account from other's devices.
- Never share personal information on publicly accessible sites.

3. Ensuring Device Security [13]

- Use security software such as anti-virus software, anti-spyware software, and firewall protection to save the device from viruses, spam, and malware, etc.
- Always avoid phishing email that is sent by stranger people.
- Be aware of the public wireless network area when you will send your personal information through this network.
- Don't use the auto-login feature as it saves the user's username and password that

may lead him\her to a problem when the laptop is stolen by the thief.

- Before the installation of any software and application or visiting website on electronic devices, make sure to read perfectly the Privacy Policies of this website, software or application.
- Always use a secure browser for online transactions to guard personal information.

Legislation

Every year the rate of identity theft is increasing at an alarming rate. To stop this crime the proper legislation is needed to implement. Different countries have enacted their legislation to stop this identity theft. Few legislation acts are given below with briefly:

1. USA

1.1 The *Identity Theft and Assumption Deterrence Act: It is introduced in 1998 against the problem of identity theft.* The Act amended Title 18, US Code, section 1028 to make it a federal crime to "knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law". [14]

1.2 The *Fair and Accurate Credit Transactions Act* of 2003 ("FACT Act"): This Act addresses the problem of identity theft to relate to credit information. The FACT Act gives the power to the consumers regarding credit reporting.

1.3 The *Computer Fraud and Abuse Act* of 1984 ("CFAA"): It gives a better solution to identity theft claims. The CFAA provides civil remedies for certain types of computer crimes and covers computers used by the federal government, financial institutions, or computers located outside the United States.

2. India

2.1 The Information Technology Act, 2000 or ITA, 2000 or IT Act: It was introduced in 2000. This law deals with cybercrime. [15]

2.2 The object of the *Information Technology Amendment Act* of 2008 (ITAA) was to protect e-commerce and e-transactions involving information exchange and electronic data exchange. [16] This Act added new offenses in sections 66A to 66F that handle the offense of identity theft and identity fraud by use of the Internet. In Section 66C, it addresses punishment for identity theft and section 66D ensure punishment for cheating by using a computer network resource. Identity theft is now a punishable offense in India.

3. South Africa

Protection of Personal Information Act 4 of 2013 ("POPI"): This Act is introduced in 2013. The main key term of this act is, it refers to personal information as "information relating to an identifiable, living natural person and where applicable, an identifiable, existing juristic person". In POPI, the term "data subject" is defined as the "person to whom personal information relates". This law helps to protect personal information.

4. More laws against identity theft are given below:

- **International Law**

 doi:10.20944/preprints202005.0330.v1

Convention on Cybercrime (2001)

European Union Data Protection Directives (1995)

- **Bangladesh**

Article- 43(b) of the Constitution of the People's Republic of Bangladesh
Section- 7(h), 7(i) and 7(r) of the Right to Information Act, 2009
Section 54 of the ICT Act

- **United States of America**

California Database Protection Act of 2003

California Online Privacy Protection Act of 2003

California Security Act of 2003

Computer Fraud and Abuse Act of 1984

Electronic Communications Privacy Act of 1986

Gramm-Leach-Bliley Act of 1999

Identity Theft and Assumption Deterrence Act of 1998

Identity Theft Enforcement and Restitution Act of 2008

Identity Theft Penalty Enhancement Act of 2004

Identity Theft and Tax Fraud Prevention Act of 2013

Right to Financial Privacy Act of 1978

- **United Kingdom**

Identity Cards Act of 2006

Data Protection Act of 1998

Fraud Act of 2006

Theft Act of 1968

- **South Africa**

Electronic Communications and Transactions Act 25 of 2002

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 May 2020 doi:10.20944/preprints202005.0330.v1

8. CONCLUSIONS

Therefore, in conclusion, the problem regarding identity theft is far from over. Every time a new technology emerges, someone somewhere will find a way to exploit it. This is no the first time and will not be the last. All problems aside, technology does make life better and it is a blessing to be born in this era. In the case of identity theft, we have to be careful and spread the precautions to fix the problem. As time passes and people get to know more and more about the situation and its ways, people will defend themselves even more.

REFERENCES

[1] Julia Kagan, “Identity Theft” https://www.investopedia.com/terms/i/identitytheft.aspAccess: 13rd Nov, 2019

[2] Identity Theft, Journal of Economic Perspectives—Volume 22, Number 2—Spring 2008—Pages 171–192.

[3] The ultimate invasion of privacy, Identity theft, 2011 Ninth Annual International Conference on Privacy, Security, and Trust.

[4] Harvard Journal of Law & Technology Volume 21, Number I Fall 2007 IDENTITY THEFT: MAKING THE KNOWN UNKNOWNS KNOWN

[5] https://www.lifelock.com/learn-identity-theft-resources-types-identity-theft.html Access: 23rd Nov, 2019

[6] https://www.straitstimes.com/business/identity-theft-atm-fraud-top-concerns-for-asians Access: 18th Oct, 2019

[7] https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf Access: 23rd Dec, 2019

[8] “Targeting kids for identity theft” - K Davis - Kiplinger's Personal Finance, 2004 - elibrary.ru

[9] The Impact of State Government Fiscal Crises on Local Governments and Schools

[10] https://journals.sagepub.com/doi/abs/10.1177/0160323X0403600201 Access: 23rd Dec, 2019

[11] Fear of Cyber-Identity Theft and Related Fraudulent Activity, https://www.tandfonline.com/doi/abs/10.1080/13218719.2012.672275 Access: 23rd Nov, 2019

[12] https://www.balancepro.net/idtheft/pdf/BALN_IDTheft_Solutions_Mar13.pdf Access: 23rd Dec, 2019

[13] https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-securehttps://www.hg.org/legal-articles/need-of-personal-data-protection-laws-in-bangladesh-a-legal-appraisal-48450 Access: 18th Dec, 2019

[14] FBI 2014 http://goo.gl/TWBoep. Also, see Lane and Sui 2010 *GeoJournal* 44; Winmill, Metcalf, and Band 2010 *DE & ESLR* 25-26. Access: 23rd Dec, 2019

[15] For a detailed discussion of these laws, see Grant 2006 *J Tech L & Poly* 11-14. Also, see Sandeepan "Identity Theft" 115 for a discussion of the ITA.

[16] Mohanty 2011 *IJLT111*

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 20 May 2020 doi:10.20944/preprints202005.0330.v1