www.ijifr.com | Volume 5 | Issue 3 | November 2017

International Journal of Informative & Futuristic Research | ISSN: 2347-1697

Cyber crimes as a growing menace

Paper ID	IJIFR/V5/ E3/ 021	Page No.	8914-8925	Research Area	Cyber crime
Key Words	Netizens, Identity Theft, Social Media, Cyber Crime				

1st	Dr. Deepti P. Lele	Associate Professor , International Institute of Management Studies , Pune , India
2nd	Dr. Shraddha Purandare	Associate Professor Institute of Future Education & Entrepreneurship Leadership, Pune , India

Abstract

In our modern technology driven age keeping our personal information private is becoming more difficult. The fact is now days, we are more connected virtually than in reality. People are converting from citizen to netizen. The usage and importance of social media is increasing a lot. Despite of knowing, that social media a public platform, people keep on sharing personal information knowingly or unknowingly on this platform. Many innocent individuals fall prey to cyber crimes around the world as technology is evolving at a rapid pace. Cyber crimes are only crimes that cause harm to another individual using a computer and a network.When privacy and confidential information is lost or interrupted by unlawful individual it gives way to high profile crimes such as hacking, identity theft, cyber warfare and many more crimes which occurs across the border.A major growing problem over the world is Identity Theft, which is referred as a crime of new millennium. The main focus of this research paper is to highlight crimes related to such identity theft and legal provisions related to cyber crimes and identity theft. It covers areas like impact of identity theft on victim and the measures which may help victims from future incidence of identity theft.

I. INRODUCTION

In today's modern society, internet is one of the educational and productive tools in order to become knowledgeable and stay well connected. It is difficult to function, without using technology. Many people use internet for running their business effectively while others use technology in order to communicate on various social networking sites such as

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume - 5, Issue -3, November 2017
Page No. : 8914-8925

Twitter, Facebook or LinkedIn. Despite the beneficial uses,[1] this tool often puts consumers at risk for say identity theft through scamming, phishing and even hacking. Therefore, consumers need to become more aware of various protective measures against online hazards.

Cyber-crime is any illegal activity committed on the internet that uses a computer as its primary means of theft. Cyber crimes can be computer related or computer generated crimes. Common types of cybercrime include hacking, terrorism, fraud, illegal gambling, cyber stalking, cyber theft, forgery, flowing of viruses, cyber pornography and illegal or prohibited online content. Theft, including a lost or stolen wallet or pocketbook or the theft of a victim's mail, was the most common means of obtaining the victim's personal information (cyber crime in India). Cyber crime is a threat to national and international socio-economic, political and security system. Therefore, law enforcing agencies must have detail knowledge and understanding about varying nature of cyber crime.

The main focus of this research paper is to highlight crime related to identity theft. Through identity theft,[2] a person, without someone's knowledge acquires a piece of their personal information such as their social security number, or even their bank account data and uses it to commit fraud or criminal activities. Methods such as spam advertisements and even phony programs that have viruses are used often. Many computers used in cyber attacks have actually been hacked and are being controlled by someone far away. In CNN article,[3] "Suspect in Celebrity Hacker Case", the staff gives an account of how the criminal Christopher Chaney hacked into many celebrities' online accounts and obtained nude pictures and other personal information stating that he was "addicted" and "didn't know how to stop".

" In current era, world is not run by weapons any more, or energy, or money. It is run by ones and zeros little bits of data and it is all electrons. Though a World war is out there, it's not about who has the most bullets but It is about who controls the information – what we see and hear, how we work, that we think. It's all about information." [4]The movie traced on Information Technology to commit theft in superhighway and information is the commodity to theft.

II. OBJECTIVES OF THE STUDY

The objectives of this research work are to touch all the important facets of the cyber crimes.

1. To understand the concepts and types of cyber crimes.
2. To study legal provisions related to Identity theft under Information Technology Act 2000

[1] International Journal of Enterprise Information Systems (IJEIS) 1(2) Copyright: © 2005 |Pages: 20
DOI: 10.4018/jeis.2005040102)

[2] Identity Theft and E-Fraud as Critical CRM Concerns Alan D. Smith (Robert Morris University, USA) and Allen R. Lias (Robert Morris University, USA)

[3] https://www.megaessays.com/viewpaper/204916.html

[4] (Lines fro, the Chapter "COSMOS", in the movie Sneakers, MCA/Universal Pictures, 1992.)

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume - 5, Issue -3, November 2017
Page No. : 8914-8925

3. To study and examine practical implication of identity theft with the help of real time cases.
4. To suggest the reforms and remedial measures for the prevention and control of identity theft.

III. OVERVIEW OF CYBER CRIME

The term 'cyber' is derived from the term 'cybernetics' which means science of communication and control over machine and man. Cyberspace is the new horizon which is controlled by machine for information and communication between human beings across the world. Therefore, crime committed in cyberspace relating to machines or devices or cyber technologies are to be treated as cyber crimes. It is defines as" Offences that are committed against an individual or groups of individuals with a criminal motive to intentionally harm the reputation of the victim, cause a physical or mental harm or loss to the victim directly or indirectly, using modern communication networks such as internet, computers or mobile phones (Bluetooth/SMS/MMS)".

Cyber crimes are broadly categorized into three categories, namely crime against

1. Individual
2. Property
3. Government

Cybercrime may threaten an individual or nation's security and financial health. Wannacry cyber attack was such an example which affected many countries and companies, wherein the attacker threatens to publish the data of a person/ company online until a certain amount of ransom is paid. The attackers demanded ransom in bitcoins (a digital currency), Some of the cyber crimes are hacking, virus dissemination, logic bombs, denial of services, phishing, spamming, identity theft, data diddling, stalking, piracy etc. In India, at least one cyber attack was reported every 10 minutes in the first six months of 2017. In 2017, as per the Indian Computer Emergency Response Team (CERT-In), a total of 27,482 cases of cybercrimes have been reported across the world. These include phishing, site intrusion, virus, and ransomware.5 A total of 1.71 lakh cybercrimes were reported in India in the past three-and-a-half years. The number of crimes that have been reported so far (27,482) indicates that the total number is likely to cross 50,000 by December 2017.

IV. IDENTITY THEFT : A CYBER CRIME

4.1 Identity Theft: The unlawful use of another's personal identifying information" (Bellah, 2001, p. 222). Others have defined identity theft as "involving financial or other personal information stolen with intent of establishing another person's identity as the thief's own" (Identity Theft, 2004). The Federal Trade Commission (FTC, 2006) sees

[5] http://www.india.com/news/india/27482-cases-of-cybercrimes-reported-in-2017-one-attack-in-india-every-10-minutes-2341055/

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume - 5, Issue -3, November 2017
Page No. : 8914-8925

identity theft as "occurring when someone uses your personally identifying information, like your name, social security number, or credit card number without your permission, to commit fraud or other crimes." Identity fraud involves financial or other private information stolen, or totally invented, to make purchases or gain access to financial accounts (Higgins, Hughes, Ricketts, & Fell, 2005).

Identity Theft is a crime in which an impostor obtains key pieces of personal identifying information (PII) such as Social Security numbers and driver's license numbers and uses them for their own personal gain. This is called ID Theft. It can start with lost or stolen wallets, pilfered mail, a data breach, computer virus, phishing, a scam, or paper documents thrown out by you or a business dumpster diving). This crime varies widely, and can include check fraud, credit card fraud, financial identity theft, criminal identity theft, governmental identity theft, and identity fraud.[6]

4.2 Stages of Identity Theft:

- **Acquisition of the identity:** It involves the acquisition of the identity through theft, hacking, redirecting or intercepting mail or by purchasing identifying information on the internet.
- **Use of the identity: The** fraudster may use the identity to commit another crime resulting in financial gain to him like misuse of the credit card information to make online purchase, opening new accounts. Sometime the stolen information may be used to harass the victim, like posting of pornography or obscene material by fraudster posing himself as the victim.
- **Discovery of the theft:** Many cases of misuse of credit cards are discovered quickly, however in some cases the victim of an identity theft may not even know how or when their identity was stolen and theft may take 6 months to several years to come to the notice of the victim.

4.3 Common Ways to Commit Identity Theft Crime:

- **Theft:** There may be a theft of your wallet or bag containing bank credit cards, passport other identifying documents containing your vital personal information.
- **Hacking, unauthorized access to systems, and database theft:** Hackers gain access to a huge base of confidential data, decrypt it and misuse the same elsewhere for financial gain or commit fraud.
- **Phishing:** Phishing is the most prevalent method to steal the personal identifying information. The fraudster sends a fraudulent email with a link to a fake website that is exact replica of the original sites to fool the users so that they reveal their personal information.
- **Nigerian 419 Scam:** This scam is called as Nigerian 419 fraud (for the relevant section of the Nigerian Criminal Code).The victim receives unsolicited email

[6] http://www.neerajaarora.com/identity-theft-or-identity-fraud/)

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume - 5, Issue -3, November 2017
Page No. : 8914-8925

declaring that he has won the lottery after his email being selected from thousands of other emails. These scams qualify as identity crimes because they involve collecting personal and bank information

- **Skimming:** Skimming can occur when a criminal attaches a small skimmer gadget to an ATM which records the magnetic stripe details of the ATM card and the camera films the personal identification number filed by the user.
- **Dumpster Diving:** A method perpetrators use by going through a victims garbage, dustbins or trash bins. They obtain copies of cheques, credit card statements, bank statements, receipts, and carbons and search for anything bearing your name, address, telephone number, and credit card number.[7]
- **Morphing**
- It is editing the original picture by unauthorized user or fake Identify. Generally in this category of crime, female's pictures are downloaded by fake users and again repost on websites by creating fake profiles after editing it.[8]

4.4 Legal background and provisions of identity theft: Indian Scenario

- **Information Technology Act, 2000**
- India has enacted the Information Technology Act in the year 2000 based on the Modern Law on Electronic Commerce adopted by the United Nations Commission on International trade law.
- Certain new sections have been added to Section 66 as Sections 66-A to 66-F prescribing punishment for offences such as obscene electronic message transmissions, identity theft,
- **Punishment for identify theft**
- Whoever, fraudulently or dishonestly make use of the electronic signature, password of any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh (See Information Technology Act 2000. Section 66-C)
- **Research Methodology –**
- This research paper is based on qualitative analysis. The researcher has explored the qualitative analysis with the help of real life case studies. This research study is related to registered and unregistered cases of identity theft in Pune city. It utilizes both primary and secondary data. For primary data collection, in depth interviews of victims and in charge police inspectors of cyber cell were conducted.
- The secondary data consists of available information in the form of published as well as unpublished material. Various sources like online articles, books, reports etc. were used understanding statistics on Cyber Crimes.

[7] http://www.neerajaarora.com/identity-theft-or-identity-fraud
[8] 2012 Criminal LJ. Journal Section at p. 162

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume - 5, Issue -3, November 2017
Page No. : 8914-8925

- The scope of research is limited to cases of Identity theft taken place in Pune only. Purposive sampling method was used to obtain data. As a matter of policy to protect Identity of the victim, their information has been kept confidential.

V. QUALITATIVE ANALYSIS- REAL LIFE CASES

5.1➔ Case 1 -Whatsapp case -Identity Theft

5.1.1 Introduction and background

Whatsapp, we can't live without it! It has emerged as the most popular messaging app today. We share our thoughts, problems, solutions, suggestion, consultancy, business through WhatsApp.Rather it has become an addiction. The main reason behind the popularity of WhatsApp is it is a cross-platform app that uses the Internet to send text messages, images, video, user location and audio media messages from one smartphone to another instantly.

But at the same time, N number of reports of bugs, hacks and Trojans that have been discovered about WhatsApp, which raise a question mark about security. It is essential to know whether your information and messages on WhatsApp are secure or not.

5.1.2 Facts of the case:

Amaraja was a well known and successful business woman in Pune. She owned 4 hotels. She used to manage all her business through WhatsApp. She was a part of rich & wealthy circle of the city. One fine morning, she started receiving calls, messages from her well wishers, friends, and relatives asking whether she was undergoing any business turbulence. Amaraja got furious and annoyed by such calls, messages. Everybody was asking her that why she needed Rs. 50000/-? Amarja got shock of her life, as she never asked anybody to help her. N enquiry, her friends and relatives updated her that they received a Whats App message last night from Amaraja, which stated that she needed money on urgent basis and demanded Rs. 50000/. In the series of messages, Second message stated that she had incurred heavy losses in business and requested them to transfer money to her account. Message did mention about not disclosure of these facts to anyone including her husband. Amarja felt embarrassed on hearing these details.

Some of her friends transferred the amount in good faith but some of them decided to verify the details before transferring amount.

Amaraja was astonished as she never sent such type of messages. All her friends and relatives, who transferred the amount, were victim of cyber crime.

5.1.3 Key Issues

1. Which type of cyber crime is this?
2. What is the liability of Amaraja?
3. Which sections of IT act 2000 are applicable in this case?
4. What would be the punishment?

5.1.4 Analysis:

Whatsapp is a big threat to one's privacy. One of the security experts, Bas Bosschert has discovered that WhatsApp backs up messages on Android in an insecure way that can be

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume - 5, Issue -3, November 2017
Page No. : 8914-8925

stolen and read by others through downloaded Android apps. However, this is only possible if person is allowing WhatsApp to keep a backup of his/her messages on the SD card. In case person's message backup option is turned off during the initial setup, then the messages are safe. But if it is not turned off, then these messages are in danger.

In order to prevent such type of attacks, one must clean the app from the device and then install WhatsApp all over again, without forgetting to turn off message backup option.

This is called hacking and identity theft. In current case, Cyber criminals first hacked the WhatsApp account of Amarja and sent the WhatsApp message to some of her contacts which is termed as Identity Theft.

1. Amaraja was not liable in this scenario. She wass not even aware of these messages. She herself was a victim in this case.
2. Sections 65, 66 of IT Act 2000 are applicable.
3. Following Punishment under section 65 would be applicable: Imprisonment up to three years, or with fine which may extend up to two lakh rupees or with both.
   Punishment under section 66- would be Imprisonment for a term which may extend o three years or with five which may extend to five lakhs rupees or with both.

5.2 ➔ Case 2- Nigerian Fraud

5.2.1 Introduction and background of the case

[9]Nigerian 419 scam is a major concern for the global community. The introduction, growth and utilization of information and telecommunication technologies (ICTs) have been accompanied by an increase in illegal activities. With respect to cyberspace, anonymous servers, hijacked emails, fake websites etc. are being used as a tool and medium for fraud by cyber scammers. Nigerian advance fee fraud on the Internet is an obvious form of cybercrime that has been affected by the global revolution in ICTs. This form of crimes is not exclusive to advance sums of money to participate into business proposals but also covers romance, lottery and charity scams. Estimates of the total losses due to this scam vary widely.

5.2.2 Facts of the case: Rajeev was an educated, dynamic individual working with a MNC. Rajeev received an email from suelisa@live.co.uk, a lady named Suli. Suli had mentioned in the mail that she was from Irak and wanted to send money to her relatives in India. But due to her ill health, she was unable to send it personally, hence asked for a help from Rajeev. Suli had provided 2 contact numbers in the mail. To authenticate this information, Rajeev called on these numbers and had a word with Suli to cross check the information. Then after many a times Suli called Rajeev, requesting him to help. Finally Rajeev decided to help her. Suli told him that she would return his money within a week's time along with 12% commission. Despite of refusal of Rajeev to accept such commission, she instated that she wanted to reward him for his help. She shared the

[9] https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume - 5, Issue -3, November 2017
Page No. : 8914-8925

details of a person to whom money should be transferred. To win confidence of Rajeev, she also shared name and number of her relative from England who was about to return money with commission. Based on this information, Rajeev transferred Rs 10 lakhs to a person whose details were shared. Later on, she again demanded Rs 75,000/- for a processing fees for sending that money with commission to India.

Rajeev received an email from *remit@RBIbank.in* stating that amount was successfully transferred. Email also expected him to fill up an online form with his personal details so that his account could be opened in RBI and money would be received from Suli. Though Rajeev filled up online form and provided all information, he did not receive any further communication from Ms Suli and RBI.

5.2.3 Key Issues:

What type of crime it is?

1. Which sections from IT act 2000 are applicable?
2. What would be the punishment?

5.2.4 Analysis:

ICHR report states that 80% of Indian netizens are of emotional kind. They think that nobody can harm them through Internet. But at global level, only 20-30 % of netizens are of emotional kinds but others are of destructive minds. They find out new ways of cyber crimes. So 70% Nigerian frauds happens in India.

In the general context, scammer updates a person a fake story about large amounts of money 'trapped' in central banks during civil wars or coups, often in countries currently in the news. Or they may inform about a large inheritance that how difficult it is to access because of government's restrictions or tax imposition in their country.

The scammer may contact you by way of email, letter, text message or social networking message. They offer a large sum of money for helping them transfer their personal fortune out of their country.

These scams are often known as 'Nigerian 419' scams because the first wave of this came from Nigeria. The '419' part of the name comes from the section of Nigeria's Criminal Code which outlaws the practice. These scams now come from anywhere in the world.

Scammers may ask for bank account details to help them transfer the money and use this information to later steal funds. At times, they may ask to pay fees, charges or taxes to help release or transfer the money through one's bank. These fees may even start as quite a small amount. If paid, the scammer may make up new fees that require payment before one could receive reward. They keep on asking for more money as long as one would be willing to part with it and one never gets back the money that was promised.

1. This type of cyber crime is called 419 Nigerian Fraud under Indian Penal Code and Identity Theft under Information Technology Act 2000.
2. Section number 420 Indian Penal Code , Section 66 C of Information Technology Act 2000 is applicable. This offence is cognisable but it is not bailable offence.

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume - 5, Issue -3, November 2017
Page No. : 8914-8925

3. Punishment under Section number 420 Indian Penal Code- The punishment which is given under section 420 of IPC for the offence is imprisonment for a term which may extend to seven years, and also be liable to fine.
   Punishment under Section 66 C of Information Technology Act 2000- Imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

5.3➔ Case 3- ATM Frauds

5.3.1 Introduction and background of the case

[10]We live in an age in which many of the crimes involve a computer at some point, but still we know very little about cyber criminals and what makes them tick. As we learn more about the rapidly-evolving field of cyber security and look at ways of detecting and preventing cyber crime, it's important that we start to ask ourselves what really goes in the mind of a cyber criminal.

Most ATM frauds happen due to the negligence of customers in using, and more importantly, negligence of banks in educating their customers about the matters which should be taken care of while in ATM. The number of ATM frauds in India is with respect to negligence of the Personal Identification Number (PIN). India is at number one position in ATM fraud.

5.3.2 Facts of the case-

Geeta went into a mall for shopping with her family on Sunday. For cash payment, he wanted to withdraw cash from ATM situated in the mall. But there was not any security guard and CCTV in the ATM. As Geeta was in need of money ,she withdrew money from that ATM. She also confirmed that money was withdrawn properly. After 2-3 days, she realized that somebody had withdrawn amount from her account by using her card, though she was possessing card with her.

5.3.3 Key Issues-

1. What type of crime is this?
2. Which sections from IT act 2000 are applicable?
3. What is the punishment?
4.

5.3.4 Analysis-

Cyber criminals are very intelligent. These criminals are more interested in money. ATM frauds are increasing day by day. In this type of fraud, criminals use different methods for robbery. For committing such fraud**,** a thief needs both PIN and the magnetic stripe information on the backside of the card. The PIN is not stored on the card's magnetic

[10] https://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca01834.html(ATM frauds)

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume - 5, Issue -3, November 2017
Page No. : 8914-8925

stripe. So, even if card is stolen or duplicated, the thief has to find some way to get the PIN. Common methods used to steal or duplicate cards and obtain the PIN are:

- **Easily identified PINs** – Your purse or wallet is stolen and the thief finds your PIN written down somewhere close to your card, or, tries a commonly used PIN, such as your birth date,.
- **Surf and Pick Pocket** – A thief watches as you enter the PIN and subsequently distracts you and steals your debit card..
- **Card Jam** – Various devices are used to jam your card in the bank machine. After your card becomes jammed, a helpful stranger suggests that you try to input your PIN a few times, but the card remains stuck. After you leave, they remove your card and have your PIN.
- **Skim and Clone-** (Transaction is sent to the financial institution) – There have been cases of equipment being set up at a business to illegally collect your PIN and card information. The person then swipes the card a second time to record the information into a hidden device which allows them to make a duplicate of the card. At the same time, a camera records your PIN information..
- **Bogus machines-** A bogus machine, that replaces the real PIN Pad, lifts your card and PIN information and issues a transaction receipt but does not actually send the transaction to the FI. The implicated employee covers your purchase by putting cash in the till so that the owner is unaware of any fraud since the outlet's books balance. At a future date, the employee uses the stolen data to create a card to empty the funds from your bank account.
- In these cases, if you are a proven victim of such a fraud, your losses would be covered by your financial institution
    1. This is called ATM fraud or Debit card/credit card fraud.
    2. Section numbers applicable – Section 66 c, 66 d.
    3. Punishment is 3 years jail or fine. This offence is cognizable and bailable.

5.4 ➔Case 4 -Identity theft through Mobile

5.4.1 Facts of the Case

Anil was habitual to save all the email ids, passwords, ATM Passwords in his mobile which was very risky. After two years of using mobile, Anil sold his mobile on OLX in offer. He was under impression that he had deleted all the data from the mobile before selling. Sunil, who purchased this mobile, happened to be a cyber criminal. He retrieved all the data from his mobile and committed cyber crimes by using the identity of Anil. When people filed the cases, police arrested Anil under different cyber crimes but in reality, Anil was not aware of all these things rather he was the victim in ATM fraud.

During the Police investigation, upon enquiry, Anil realized that he had saved all his sensitive personal information on his mobile.

5.4.2 Key issues:

1) What kind of cyber crime is this? Whether Anil is liable or not?

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume - 5, Issue -3, November 2017
Page No. : 8914-8925

2) Which sections from Information Technology Act 2000 are applicable?
3) Who is the criminal? What is the punishment?

5.4.3 Analysis –

1) This is called as identity theft. In the present case, Anil was a victim in cyber crime. And Sunil took undue advantage of Anil. As Anil was unaware of cyber crimes committed, he was not liable in this case.
2) Section 66B, 66C, 66E from Information Technology Act 2000 is applicable.
3) Punishment for Section 66B- Imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

   Punishment of Section 66C - Imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

   Punishment of Section 66E - Imprisonment which may extend to three years or with fine which may extend up to lakh rupees or with both.

5.4.4 Findings:

1. Need of an hour is to run a massive campaign to create awareness about cyber crimes& cyber laws
2. To understand exact nature of cyber crime, it is essential provide appropriate training to Police Officer.
3. Amendments in Information Technology Act 2000 are needed to introduce more stringent punishment.

VI. RECOMMENDATIONS

Netiquettes/Preventive Measures

1. At most precaution need to be taken while downloading free songs, films, software.
2. Hacking and breaking into other peoples' computers /networks is a criminal offence.
3. Never use anyone else's user account and password, and never share your own user account and password with someone else.
4. Do not open attachments unless you know they have been received through trusted sources and they come from a known sender. (Phishing, Hackers).
5. Be careful while commenting on other's blogs and websites.
6. Change your password after every 3 months and keep it unique.
7. Watch your language. No potty mouths.
8. No spamming.
9. Remove all the personal information about the sender including their email id when you are forwarding any mail to bunch of people.
10. Give proper credit for intellectual property.
11. Wi-Fi Settings: Being in a corporate industry, one always needs to know that the basic Wi-Fi settings are set at WEP (wired equivalent privacy). Change it to WPA or WPA2/PSK.

ISSN: 2347-1697
International Journal of Informative & Futuristic Research (IJIFR)
Volume - 5, Issue -3, November 2017
Page No. : 8914-8925

VII. CONCLUSIONS:

Fraud and identity theft have been increasing with the use of e-commerce. In the U.S. alone, it has been estimated that victims may spend on average $1,500 in out-of-pocket expenses and an average of 175 hours in order to resolve the many problems caused by such identity thieves.[11] Organizations that engage in e-commerce as a large part of their business need to protect their customers against these crimes. As we tend to share a lot personal information, model construction and implications were generated concerning steps that employees and customers may take to avoid identity theft.[12]With the increasing boom in the internet industry, there's a growing dependency and need on to the internet. We as common citizens and corporate officials, have a certain day to day challenges when it comes to the internet. As everything has become digital but at the same time we should keep in mind that nothing is safe. Cyber crime awareness is a need of an hour.

VIII. REFERENCES:

[1] International Journal of Enterprise Information Systems (IJEIS) 1(2) 2005 Pp(20), visited on 4/10/2017
[2] Alan D. Smith and Allen R. Lias, Identity Theft and E-Fraud as Critical CRM Concerns
[3] https://www.megaessays.com/viewpaper/204916.html
[4] (Lines fro, the Chapter "COSMOS", in the movie Sneakers, MCA/Universal Pictures, 1992.)
[5] http://www.india.com/news/india/27482-cases-of-cybercrimes-reported-in-2017-one-attack-in-india-every-10-minutes-2341055/
[6] http://www.neerajaarora.com/identity-theft-or-identity-fraud/)
[7] 2012 Criminal LJ. Journal Section at p. 162
[8] https://www.scamwatch.gov.au/types-of-scams/unexpected-money/nigerian-scams
[9] https://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca01834.html(ATM frauds)
[10] Journal of Criminal Justice Volume 38, Issue 5, September–October 2010, Pp 1045-**1052**
[11] https://www.igi-global.com/article/identity-theft-fraud-critical-crm/2079

PAPER CITATION

Lele, P.D. , Purandare, S. :: "Cyber crimes as a growing menace" ***International Journal of Informative & Futuristic Research (ISSN: 2347-1697*****), Vol. (5) No. (3), November 2017, pp. 8914-8925, Paper ID: IJIFR/V5/E3/021.**
Available online through- http://www.ijifr.com/searchjournal.aspx

[11] Journal of Criminal Justice Volume 38, Issue 5, September–October 2010, Pages 1045-**1052**
[12] https://www.igi-global.com/article/identity-theft-fraud-critical-crm/2079