ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Study on Cyber Turpitude from Cyber Criminals

Kartheek Ravula [1], Gopinadh Adapa [2]

M.Tech Student, Department of Computer Science & Engineering, Chirala Engineering College, Chirala (AP), India.

ABSTRACT: In the existing world, our country has seen an extraordinary guide of cyber depravity whether they are relevant to Trojan hazards, e-mail air attack, Denial-of-service hazard, information stealing, or the most casual crime is hacking the data. In spite of technological measures being chosen by corporate companies and individuals, we have observed that the cyber depravity has risen over the final era. Since consumer of computer system and World Wide Web (internet) are raised globally in large number regularly, where it is not difficult to access any data easily within a few seconds by using net which is the midway for extremely large information and a big base of information transmitted around the world.

Fig1: Cyber Crime

Some careful measures should be captured by all of us although using the net which will help in challenging this bigger hazard cyber crime. In this research paper, we are sifting about the miscellaneous types of cyber depravity, and cyber crime as a threat to persons, possessions, and society and also here we are explaining the concepts of cyber crime in a diagrammatical way. Actually in this paper we are proposed miscellaneous preventive measures to be taken to stop the cyber crimes. And also now a day's cyber criminals are providing hacking as a service. There is a large group of services are available by the cyber-criminals. These groups are always stealing your money, your confidential data etc. All of these black services are almost maintained or administrated by the cyber-criminals. Anyhow number of services are became white services. Every time cyber-criminals having concentration on your credit cards and marketplaces. In this paper we are describing about all of these services that are provided by the cyber-fools.

KEYWORDS: Cyber crime, Cyber depravity, Cyber criminals, Cyber criminal services, hacking, Credit card hazards, Cyber fraud.

I. INTRODUCTION

In the existing world, our country has seen an extraordinary guide of cyber depravity whether they are relevant to Trojan hazards, e-mail air attack, Denial-of-service hazard, information stealing, or the most casual crime is hacking the data. In spite of technological measures being chosen by corporate companies and individuals, we have observed that the cyber depravity has risen over the final era. Crime of cyber, adduce the act carry out a criminal act using internet network as a bridge for communication. However there is no technological description by any legal body for cyber depravity, in most cases it is generally defined by the computer crime research center as – "illegal crimes perform an action on the World Wide Web (WWW) using the electronic device like computer, one or the other as a tool or a targeted someone." Each class of cyber crimes involve twain the computer device and the human behind it as victims, it just rely upon which of the twain is the predominant aim. Cyber depravity or cyber crime could contain everything as

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

easy to theft millions of currency from the bank accounts. Cyber depravity could also contain non-financial offenses, such as developing and delivered tiny or abundant programs composed by programmers called virus on different computers or entering secret business information on the World Wide Web (internet). A valuable form of cyber depravity is identity looting or identity theft, in which convict use the net to theft personal data from other users. Miscellaneous categories of social sites are used for this intention to recognize the identity of curious peoples. There are 2 methods this is accomplished-

1) Harming
   And
2) Phishing.

Twain ways bait users to imitational or fake websites, in these types of sites, where they asked to enter the personnel login information like Bank account numbers, mobile numbers, credit card numbers, address, etc. And other information convicts are using to "theft" other person recognition.

Fig2: Cyber Crimes through internet

II. ANCIENT TIME

World's first cyber crime was reported in the year 1820 which is not impulsive considering the verifiable truth that the calculating machine (abacus), which is ideation to be the primeval form of a data processing machine (computer), has been all over around 3,501 BC. In Bharath, China, and Japan. The epoch of modern computers, howbeit, starting with the analytical engine of Babbage. In 1821s Joseph-Marie Jacquard, a yarn manufacturer in France created a machine called loom. This tool allowed the repetition of a series of steps in the weaving of different special material fabrics. Finally it shows in a fear amongst employees of Joseph-Marie Jacquard that their immemorial employment and occupation were being endangered. They committed action on sabotage to dishearten Joseph-Marie Jacquard from additional use of the further new technology. This is the world's first cyber depravity or cyber crime was recorded.

III. DEMONSTRATION

Fundamentally cyber crimes can be arranged in two groups, determined for the intention of understanding as Ilk I and Ilk II cyber crime.

Ilk I cyber crime has the following properties:

It is commonly a lone episode from the angle of victim. For instance, the sufferer unrecognized downloads or installs a Trojan horse which place a key blow logger on his/her device. Instead of the victim might obtain an email containing what claim to be a connector to a known tuple, but in fact it is a link or connector to an inimical websites. We have large number of key logger software's are available in the sites to commit this offence.

It is frequently ease by offence wear programs such as keystroke loggers, computer virus*, malevolent program or Trojan horses.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Approximately some ilk's of blemishes or vulnerabilities in software products frequently provide the footing for the assailant (that means attacker). For instance, felon controlling an internet site may bring benefit of vulnerability in a net web browser to place a Trojan horse on the victim's computing machine.

Fig3: Types of viruses

Instance of this ilk of cyber crime include but are not restricted to phishing scam, stealing or bad handling of information or service through virus, stealing identity, and bank criminal offence.

Ilk II cyber crimes:

At the other extremity of range, includes, but is not restricted to actions such as computing machine related humbug, counterfeit antivirus, cyber stalking and molestation, minor predation, robbery, travel swindle, false phony written agreement scams, blackmail, stock exchange manipulation, corporate spying, and designing or carrying out terrorist actions.

The attributes of ilk II cyber crimes are:

- It is commonly an on-going episode of event, involving repeated fundamental interactions* with the aim. For example, the aim is communicated in a chat room by somebody who, extra time, tries to build a kinship. Finally, the felon exploits the kinship to commit a criminal offence.
- It is usually facilitated by computer program* that do not match into the categorization crime ware. For example, colloquy may take place utilizing (Instant messaging). Customers or files may be changed by using File transfer protocol (FTP).

IV. CYBER OFFENCE IN INDIA

During the year (twelvemonth) 2011, 2012, 2013, 2014 and 2015 (till May), a full number of 21,698, 27,600, 28,480, 48,170 Indian sites were hacked by several hacker group disperse across globally and potentially to touch 85,000 by 2015, adds the analysis. (Source: ASSOCHAM INDIA (The Associated Chambers of Commerce & Industry of India)).

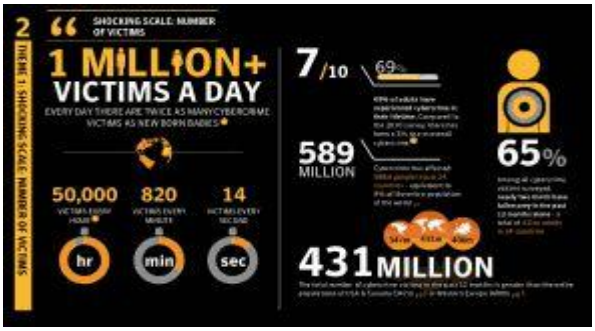

Fig4: Cyber offence in India

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

V. SOME OCCUPATIONS GIVING LIFE TO CYBER OFFENCES

There are 3 forms of masters in the cyberspace:

1. Information Technology professionals

❖ Afterward cyber offense is all about internet, many forms of Information Technology professionals are quite eminent alive in the same, which contain but are not limited to:

- Electronic network organizer or engineer
- Cyber protection software masters
- Cyber forensic adepts
- Information Technology administration professionals
- Licensed internet security scrutinizers
- Cyber-terrorists or Ethical Hackers

2. Cyber Law Proficient's

Cyber law has arise a miscellaneous disciplinary path and therefore specialization in managing cyber frauds is needed. Cyber act professional handle:

- Patent violation.
- Cyber protection for Identity stealing for credit cards and other fiscal transactions.
- Common cyber act or law
- Online payment crime
- Copyright violation of software, euphony (Music) and video

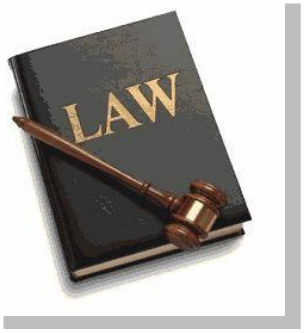

Fig5: Cyber Law Proficient's

3. Cyber act enforce by the professionals

A miscellaneous agency plays a role in cyber act enforcement, which contain the electronic-governance agencies, cyber offence research cells and cyber labs for forensic. From each one would have various types of professionals.

VI. TYPES OF CYBER FRAUDS

Cyber frauds can be fundamentally separated in to 4 types:

1. *Cyber frauds against peoples:*

Again this section having some categories:

Cyber frauds devoted against persons allow miscellaneous crimes transmission of minor- -pornography, cyber erotica, and molestation of a person utilizing a computer device such as via e-mail, bogus written agreement scams. There are some crimes which impact the character of individuals:

1. Molestation via E-mails
2. Cyber depravity
3. Slander
4. Hacking

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

5. Breaking
6. Email manipulating
7. SMS humbug
8. ATM card frauds
9. Humbug

1. **Molestation via E-mails:** This is very general form of molestation via sending alphabetical characters, attachment of data files and folders that is through electronic mail (e-mail).
2. **Cyber depravity:** It is conveyed as a physical menace that makes fear via the use of computer engineering such as net, electronic mail, phones, SMS, digital camera or webcam, internet sites* or videos.
3. **Slander:** It involves any individual with aim to lower down the self-respect of the individual by hacking his e-mail account, and sending few mails by using bad words to stranger individual mail account.
4. **Hacking:** It intends unofficial control all over the computer machine* and behave of hacking totally demolish the entire data and also computer programs. Hackers generally hacks wireless and mobile networks.
5. **Breaking:** It is pretend of breaking into your computing systems without your cognition and accepts and has manipulated with cherished confidential data point*.
6. **Email manipulating:** A duplicate e-mail may be stated to be one, which belies its source. It shows its source to be several from which really it's arise.
7. **SMS humbug:** Faking is a blocking via spam which means the unused and undesirable messages. Here a wrongdoer person theft identity of another individual in the pattern of cellular telephone number and sending messages through net and receiver gets the messages from the cellular telephone number of the victim. It is very dangerous cyber crime against any person.
8. **ATM card frauds:** ATM frauds that means Debit or Credit cards. Used by malefactor for their pecuniary benefits via withdrawing currency from the victim's savings bank account. There is ever unofficial use of ATM cards in this category of cyber crimes.
9. **Humbug:** Here every criminal theft passwords and information storage has done it with having shamed face which contributes to humbug and frauds and cheating.

2. Cyber frauds against property:

The second class of cyber offences is that of e-crime versus all types of property. These offences admit computer hooliganism and transmission of malign viruses or program. A new Mumbai engineering company in India lost much money in the business when the competitor, an industry major, theft the technical information from their computers with the assist of a corporate cyber sleuths software. There are certain crimes which consequences people's properties which are follows:

1. Offence for intellectual property
2. Cyber hooliganism
3. Hacking computer machine*
4. Sending computer virus
5. Cyber sin
6. Net time thievery

VII. MAJOR MENACE OF CYBER OFFENCE

In the present days, credit card stealing and money laundering is in rise. Cyber offence has also displayed the approaching threats of electronic banking. Email spoofing, credit card frauds, and online database frauds are most elegant crimes recently. Every month we see a new cyber crime technique's in our countries. Where is the ending of these types of crimes? So, that's why we want better security of our information and maintain the accuracy of our retrieved data. Is it a better solution to stop these types of crimes? And the answer is 'No'. Why? Every minute the cyber criminals are searching for new techniques to do these types of frauds. So, every individual should maintain their data accurately or securely. Change their transaction cards like credit cards and debit cards and their master cards pin number every 6 months. And don't tell their confidential numbers to other ones even they are their family members also. Every one they forget all these things and simply write their pin numbers in the back side of those cards and on

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

their purses and on their house wall for recognition purpose. But, it is not safe. Because hackers are besiege around of you. So, be careful. But, in our countries I don't see any accurate law's to stop these types of offences. In these types of offences the government role is also very important to control these types of cyber depravities. Want some hefty laws to punish the cyber criminals just like hanging. Then only these types of offences will be reduced. So, be careful people from this type of cyber-deceit.

VIII. AFFECT OF CYBER-FRAUDS ON BUSSINESS

Now a day, all the organizational work is done in online only. Thus every sector is entirely dangerous to cyber-crime. Cyber crimes constantly affect the business companies at any size. Still, we say that in the Information technology (IT) industry SME's are the biggest stack holders. Pilferage and copyright protection are the crucial threats.

IX. MAJOR AFRAID FOR THE POLIS AND THE BUSSINESS COMPANIES SO FAR AS DISVOVERING CYBER CRIMES

Indian companies do not require to be advertised for the wrong reason. If they are in problem, they examine about their best to classify it out via own-in house protection security device.

As much as, polis are related they are commonly loath to take up cyber perpetrate cases as inquiry is majorly labour-intensive and valuable.

X. CYBER CRIME AS A SERVICE

In the present days, cyber felons are provided some hacking services also to the present world. These services are used by same type of minded people (criminals). So, it effects on folks daily life. The following services are provided by the hackers:

1. Service for Retrospection (like Commercial market places)
2. Service for crime ware
3. Service for cybercrime infrastructure
4. Hacking as a service
5. Spam services

These types of services are provided by the hackers to do criminal offences regularly.

XI. DUE CARES FOR PREVENTION OF CYBER CRIMES

In the last world, we want some precautions to decrease the cyber offences. So we want some list for protection:

1. Protection,
2. Precaution,
3. Preservation Prevention and
4. Perseverance.

- Recognition of exposure via education will help the responsible companies to meet these targets.
- Don't exchange your pin numbers to strangers via e-mail, phone messages, while chatting, and any other social networking sites. etc.,
- Avoid sending your personal photos to strangers because we are seeing every day; they misuse your photos day by day.
- Update your Anti-virus regularly against virus attacks.
- Don't do the shopping in any unsecured websites, first check the site ratings and decide which one is popular. Do your shopping in popular sites only, because by the popularity they will update more security to all the data available in the sites.
- Don't share your credit card and debit card numbers to the strangers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

- Keep an eye on your children to prevent any molestations or harassments in online from any one.
- Always check the traffic of your personal websites; it is the minimum responsibility of an owner of the sites, because users are increases day by day, we don't know who the hacker in that users list. So that's why watch your sites regularly for preventing the cyber crimes.
- It is so important to put passwords to your databases and websites to control the information.
- Strict cyber laws are passed by the government, so that's why every netizen should remember this in mind and be careful to do the offences.
- IT department passes certain protection guidelines for your computer machines* and also they introduce some more strict statutory laws also for cyberspace.
- Across the globe, cyber threat is a big threat across all over the world; some steps should be taken by the international level for the protection in cybercrime.
- Provide total justice to all the victims of cybercrimes and by way of compensation and hacker should be punished hardly just like hanging. Already we have punishment hanging in our laws. Apply this type of punishments to these types of crimes also. So that it will expect the criminals of cyber crimes in the world.

XII. SIMULATION RESULTS

This Paper totally explains about the Cyber crimes, faced by the world. In the Fig1 we are showing the main title of the paper. It shows about, what paper is it? In the Fig2 we are showing, what are the cyber crimes are done via internet, and those all internet crimes are explained there. And in Fig3 we are explained about types of cyber crimes what are done in the present world. In Fig4 we are explained about what are the cyber offences are done in the present world and also we are explained the survey results what the offences are done in this year. In Fig5, it shows about the cyber laws. Finally, this paper gives the knowledge about cyber crimes are done in various fields.

XIII. CONCLUSION

Finally we conclude, computing machine* crimes does have a forceful effect on the earth in which we alive. It affects all individuals' nay matter where they are coming from. Lots of hackers see the internet (WWW) as public place for every individual and they do not see their activities as criminal. Hackers are old as the cyberspace. In my thought, hacking and computer frauds are will be with us for an immense as we have the cyberspace (Internet). It is our part to keep the equivalence between, what is a crime? And what is the enjoyment? Fortunately, our government takes precautions to control these types of cyber crimes. Even though, total controlling of internet is not possible because internet is just like an ocean. So, that's why parents are put an eye on your children what they are doing on the internet, and also discuss with your children what is good in internet and what is bad, educate them regularly. Finally, in this paper, we are explaining about the types of hacking and about their nature in the present world. Because, what was the fraud was done yesterday may not be crime today so that's why alertness is more important. We want some strong techniques to protect our money. I think bio-metric is the good one for that. For example, in my opinion, in ATMs we are just inserting our card in the machine and after that we are entering our pin number, and next step is collecting our money and leave. Is it a secured one? And the answer is No. why? This is not enough. In the last step in the process of transaction a finger-print option is available, and then only the right person does the transaction. Because every individual finger-print is different from others. Change your passwords for every 6months. Put your pass words having 1 character, 1 special symbol, and 1 number and create it as strong. Most of the crimes in organizations are done by their employers only. Criminals are so intelligent in the technology wise; they are searching for new computer techniques every day for doing illegal actions. Criminals are always brilliant. They update their technical knowledge regularly. They place their wonderful knowledge for doing illegal activities. If they place their knowledge in the correct way, then our countries become most powerful and strongest. So, that's why, we want some cruel laws for stopping these types of frauds. In this paper, we are not encouraging hackers. We are just providing the knowledge about cyber crimes and their hacking services provided by the criminals and also we are discussing here about the prevention methods to stop these types of cyber offences. Since, users of computer machines* was increasing across the globe in huge number day by day, where it is so easy to obtain the information in the internet. Certain security measures should be taken by all of us when using the internet (WWW) which will help in challenging this big threat cyber crime or cyber depravity or cyber turpitude.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

REFERENCES

1. Steel.C. (2006), Windows Forensics: The Field Guide for Corporate Computer Investigations, Wiley.
2. Phil Williams, Organized Crime and Cybercrime: Synergies, Trends, and Responses, Retrieved December 5, 2006 from Available: http:// www.pitt.edu/~rcss/toc.html.
3. N. Leontiadis, T. Moore, and N. Christin. *"Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade*". In Proceedings of USENIX Security 2011, San Francisco, CA, August 2011.
4. Microsoft Inc. Microsoft security intelligence report, volume 9, 2010. Available: http://www.microsoft.com/security/sir/.
5. I. Henry, "*Machine learning to classify fraudulent websites*". 3rd Year Project Report, Computer Laboratory, University of Cambridge, 2012.
6. F. Lorrie, editor. "*Proceedings of the Anti-Phishing Working Groups*", 2nd Annual eCrime Researchers Summit 2007, Pittsburgh, Pennsylvania, USA, October 4–5, 2007, vol. 269 of ACM International Conference Proceeding Series. ACM, 2007.
7. Communications Fraud Control Association. 2011 global fraud loss survey. Available: http://www.cfca.org/fraudlosssurvey/, 2011.
8. Cyber Crime – A Threat to Persons, Property, Government and Societies. Available at: Volume 3, Issue 5, May 2013 ISSN: 2277 128X , International Journal of Advanced Research in Computer Science and Software Engineering, Research Paper Available online at: www.ijarcsse.com
9. Cybercrime Exposed, Cybercrime-as-a-Service.MCA fee White paper. Available at: www.mcafee.com

BIOGRAPHY

Kartheek Ravula, presently pursuing his M.Tech in Computer Science & Engineering from Chirala Engineering College, Chirala, Prakasam District, A.P, India. Affiliated to Jawaharlal Nehru Technological University, Kakinada. Approved by AICTE, New Delhi. He received B.Tech (Information Technology) degree in 2012 from JNTU Kakinada, India. His research interests are network security, Computer Networks (wireless Networks) etc.

Gopinadh Adapa, Presently pursuing his M.Tech in Computer Science & Engineering from Chirala Engineering College, Chirala, Prakasam District, A.P, India. Affiliated to JNTU Kakinada. Approved by AICTE, New Delhi. His research interests are Computer Networks etc.