International Research Journal of Computer Science (IRJCS)
Issue 08, Volume 5 (August 2018)
ISSN: 2393-9842
www.irjcs.com

INTRODUCTION OF CYBER CRIME AND ITS TYPE

Er. Navneet Kaur
Assistant Professor of CSE, ASIAN College, Patiala, India
batthnavneet87@gmail.com

Manuscript History
Number: **IRJCS/RS/Vol.05/Issue08/AUCS10080**
Received: 05, August 2018
Final Correction: 12, August 2018
Final Accepted: 20, August 2018
Published: August 2018
Citation: Navneet (2018). INTRODUCTION OF CYBER CRIME AND ITS TYPE. IRJCS:: International Research Journal of Computer Science, Volume V, 435-439.**doi://10.26562/IRJCS.2018.AUCS10080**
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India
Copyright: **©2018 This is an open access article distributed under the terms of the Creative Commons Attribution License, Which Permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited**

Abstract— Cyber crime is a social crime that is increasing worldwide day by day. So the cyber crime investigation is becoming a very complicated task to do without a proper framework. This paper mainly focuses on the various types of cyber crime like crimes against individuals, crimes against property, and crimes against organization. It also includes impact on the real world and society, and how to handle cyber crimes.

Keywords— Cyber crime; network; security; E-crime; social media; computer;

I. INTRODUCTION

A crime is an unlawful act punishable by a state or other authority. In current scenario Cyber Crime is increasing very fast as the technology is growing very rapidly. So the cyber crime investigation is becoming a very complicated task to do without a proper framework. There is wide range of different types of cyber crime today. Solution of each case requires a very complicated task. Today internet is the fastest infrastructure in everyday life .Man is able to send and receive any form of data .The scope of cyber security not limited to securing the IT industry but also other like cyber space. Cyberspace is interconnected technology. The term entered the popular culture from science fiction and the arts but is now used by technology strategists, security professionals, government, military and industry leaders and entrepreneurs to describe the domain of the global technology environment.

Cyber criminals are becoming more Sophisticated and are targeting consumers as well as public and private organizations. Cyber crimes are rises due to the lack of cyber security. All types of cyber crimes consist of both the computer and the person behind it as victims. Cyber crime could include anything such as downloading. Now many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes.

II. CYBER CRIME

A generalized definition of cyber crime may be "Unlawful acts wherein the computer is both a tool and target. Cyber Criminal is a person who commits an illegal act with a guilty intention or commits a crime in context to cyber crime. Some of the kinds of Cyber-criminals are mentioned as below.

- **Crackers:** These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.
- **Hackers:** These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers.

© 2014- 18, IRJCS- All Rights Reserved

- **Pranksters:** These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm.
- **Career criminals**: These individuals earn part or all of their income from crime, although they Malcontents, addicts, and irrational and incompetent people.
- **Cyber terrorists:** There are many forms of cyber terrorism. Sometimes it's a rather smart hacker breaking into a government website, other times it's just a group of like-minded Internet users who crash a website by flooding it with traffic.
- **Cyber bulls:** Cyber bullying is any harassment that occurs via the Internet. Vicious forum posts, name calling in chat rooms, posting fake profiles on web sites, and mean or cruel email messages are all ways of cyber bullying.
- **Salami attackers**: Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. a bank employee inserts a program into bank's servers, which deducts a small amount from the account of every customer.

Further, it is not easy to identify immediately about the crime method used, and to answer questions like where and when it was done. The anonymity of the Internet makes it an ideal channel and instrument for many organized crime activities.

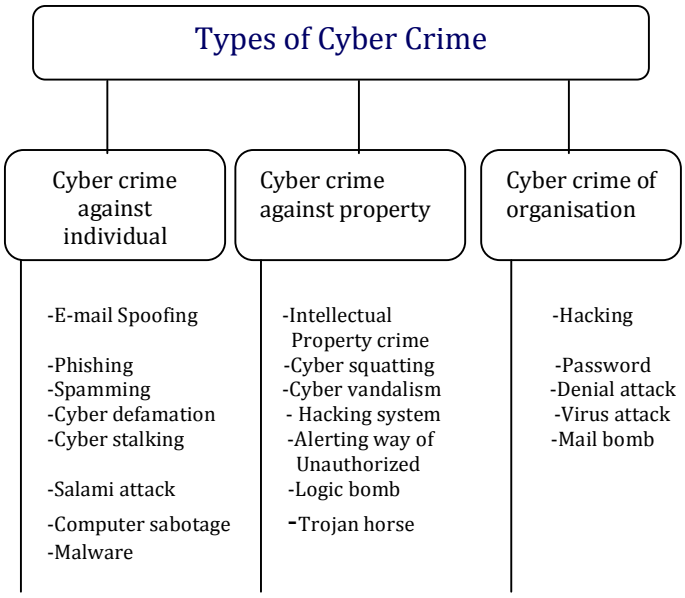
III. DIFFERENT REASON BEHIND CYBER CRIME:

There are many reasons why cyber-criminals are doing cyber-crime that are mentioned below:

A. For the sake of recognition.
B. For the sake of quick money.
C. To fight a cause one thinks he believes in.
D. Low marginal cost of online activity due to global reach.
E. Catching by law and enforcement agency is less effective and more expensive.
F. New opportunity to do legal acts using technical architecture.
G. Official investigation and criminal prosecution is rare.
H. No concrete regulatory measure.
I. Lack of reporting and standards
J. Difficulty in identification.
K. Limited media coverage.

IV.DIFFERENT TYPES OF CYBER CRIME

As discussed earlier that cyber crime is different from the conventional crime. Same as conventional crime, cyber crime also constitutes of many types. Some of the types of cyber crime as shown in figure 1.1 as the cyber crime evolve with the invention of new technique itself.



© 2014- 18, IRJCS- All Rights Reserved

4. 1) Cyber crime against individual:

i) E-Mail Spoofing: this means a spoofed email is one that appears to originate from one source but actually has been sent from another source. This can also be termed as E-Mail forging. The main goal of the attacker in this case is to interrupt the victim's e-mail service by sending him a large number of emails.

ii) Phishing: Phishing means trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account. The criminal then has access to the customer's online bank account and to the funds contained in that account. The customers click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred

iii) Spamming: Spam is the abuse of electronic messaging system to send unsolicited bulk messages indiscriminately

iv)Cyber defamation: It involves any person with intent to lower down the dignity/image of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

v) Cyber stalking and harassment: The use of Internet to repeatedly harass another person group, or organization. This harassment could be sexual in nature, or it could have other motivations including anger.

vi) Computer sabotage: the use of the internet to halt the normal functioning of a computer system through the introduction of worms, viruses, or logic bomb is referred to as computer sabotage.

vii) Malware: Malware is any software that infects and damages a computer system without the owner's knowledge or permission and takes control of any individual's computer to spread a bug to other people's devices or social networking profiles.

4.2) Crime against property:

i) Intellectual Property Crimes: Any unlawful act by which the owner is deprived completely or partially of his rights is a crime. The most common type of crimes are software piracy, infringement of copyright, trademark , theft of computer source code, etc.

ii) Cyber Squatting: It involves two persons claiming for the same Domain Name either by claiming that they had registered the name first. For example two similar names i.e. www.yahoo.com and www.yahhoo.com.

iii) Cyber Vandalism: Vandalism means damaging property of another. Thus cyber vandalism means destroying or damaging the data or information stored in computer when a network service is stopped or disrupted.

iv)Hacking Computer System: Hacking in simple terms means an‖ illegal intrusion into a computer system and/or network‖. Hacking attacks include Famous social networking sites such as facebook, Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer system. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company.

v) Altering in an unauthorized way. This requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes; Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions.

4.3) Cyber crime against organization:

i)Hacking: It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs.

ii) Password sniffing: password sniffers are programs that monitor and record the name and password of network users as they login, at site.

iii) Denial of service attacks: the criminal floods the bandwidth of the victim's network. The attackers typically target site or service hosted on high-profile web servers such as bank, credit card payment gateways, mobile phone networks and even root name servers. Denial of service attacks are designed to consume resources so that other users are unable to use the resources and are therefore —denied service‖. In a Computer network environment, the key resources are CPU, memory, and bandwidth

iv) Virus attack: A computer virus is a malware program that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected.

V) E-mail bombing/mail bomb: refers to sending a large no of emails to the victim to crash victim's E-mail account or server crash.

vi) Salami attack: these attacks used for committing financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. a bank employee inserts a program into bank's servers that deducts a small amount from the account of every customer.

© 2014- 18, IRJCS- All Rights Reserved

Vii) Logic bomb: A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are available. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company.
viii) Trojan horse: Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system.

V. PRECAUTION FOR CYBER CRIME:

5.1). Use strong passwords.

i) Use separate ID/password combinations for different accounts, and avoid writing them down.
ii) Make the passwords more complicated by combining letters, numbers, and special characters. Change them on a regular basis.
iii)Use strong passwords with upper case, lower case, number and special characters and minimum of 6 characters.
iv) Don't use passwords that contain names, birthdays, phone numbers, etc.
v) Don't share passwords across multiple services i.e. same password for Gmail, Credit Cards, Work, Twitter, etc.
vi) Don't use sequential passwords for different services i.e. ABC10, ABC11, ABC12, etc.
vii)Don't store your passwords under your keyboard, in your drawer, in Outlook, Gmail, Phone, password wallet software, etc.
viii) Best place to store passwords is in your brain; second best is written on a piece of paper and kept in your wallet.
ix) Never tell your password to anyone, including people from support, customer service, helpdesk, etc.

5.2). Secure your computer:

i) Enable your firewall: Firewalls are the first line of cyber defense; they block connections from suspicious traffic and keep out some types of viruses and hackers
ii) Use anti-virus/malware software: Prevent viruses from infecting your computer by installing and regularly updating anti-virus software.

5. 3). Block spyware attacks. Prevent spyware from infiltrating your computer by installing and updating anti-spyware software.
5.4). Install the latest operating system updates: Keep your applications and operating system (e.g., Windows, Mac, Linux) current with the latest system updates. Turn on automatic updates to prevent potential attacks on older software.

5.5). Protect your data: Use encryption for your most sensitive files such as health records, tax returns, and financial records. Make regular backups of all of your important data.
5.6). Secure your wireless network: Wi-Fi (wireless) networks are vulnerable to intrusion if they are not properly secured.
5.7). protect your e-identity: Be cautious when giving out personal information such as your name, address, phone number, or financial information on the Internet. Ensure that websites are secure, especially when making online purchases, or ensure that you've enabled privacy settings.
5.8). Avoid being scammed: Never reply to emails that ask you to verify your information or confirm your user ID or password. Don't click on a link or file of unknown origin. Check the source of the message; when in doubt, verify the source.

VI. CONCLUSION

Network security is the vast topic that is becoming more important because the world is highly interconnected. This paper discussed different types of cyber crime. There is need to conduct research analysis of cyber crime to protect sensitive data. As such international laws and regulations combined with reliance on technologies are crucial to counter the crime research.

VII. REFERENCES

1. Ammar Yassir and Smitha Nayak, "Cybercrime: A threat to Network Security", International Journal of Computer Science and Network Security, 84 VOL.12 No.2, February 2012
2. Hemraj Saini, Yerra Shankar Rao," Cyber-Crimes and their Impacts: A Review", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 2,Mar-Apr 2012, pp.202-209.
3. Dr. Ajeet Singh," Cyber Crime: Challenges and its Classification", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),Volume 3, Issue 6, November-December 2014'.
4. www.uncjin.org/Documents/EighthCongress.html.

© 2014- 18, IRJCS- All Rights Reserved

5. Majesty,H., Cyber Crime Strategy, S.o.S.f.t.H. Department, Editor. 2010, The Stationery Office Limited: UK. p. 42.
6. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. London: Academic Press,2011: Pp. 5-19.
7. Farmer, Dan. & Charles, Mann C. Surveillance nation. Technology Review; Vol. 106, No. 4, 2003: Pp. 46.
8. Harrison, A. Privacy group critical of release of carnivore data Computer world; Vol. 34, No. 41, 2006: Pp. 24.
9. Tipton, Harold F. & Krause, Micki. Information security management handbook (5th ed.). London: Taylor & Francis e-Library, 2005: Pp. 320-386.
10. Whitman, Michael E. & Mattord, Herbert J. Principles of information security (2nd ed.). Boston: Thomson Course Technology, 2005: Pp. 205-249.

Author

Er. Navneet kaur was born in mugal majra in Punjab, India 1987. She did her M.Tech (CSE) from Shri Guru Granth Sahib World University. She is working as an assistant professor at college ASIAN. She has written 03 research paper.

© 2014- 18, IRJCS- All Rights Reserved