ISSN: 2249-7196
IJMRR/April 2019/ Volume 9/Issue 3/Article No-1/01-09
Padmaavathy PA / International Journal of Management Research & Review

CYBER CRIMES: A THREAT TO THE BANKING INDUSTRY

Padmaavathy PA*[1]

Asst. Prof, Dept. of Management, Karpagam Academy of Higher Education (Deemed to be University), Coimbatore, Tamil Nadu, India.

ABSTRACT

Cyber crimes can be defined as the unlawful acts where the computer is used either as a tool or a target or both. It covers crimes like phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, spam and so on. Cyber crime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It also covers the traditional crimes in which computers or networks are used to enable the illicit activity. As cyber attacks continue to plague businesses, it is banks who are under the greatest scrutiny from the increasing threat. Criminals can send phishing emails or set up fake websites that dupe consumers into giving away sensitive financial data. They can also leverage information from social media sites to socially engineer their way into accounts via customer service. Compared to today, the secure bank of the future will use more machine-learning technology and systems to proactively prevent potential breaches and data loss.

Keywords: Threats, Security, Phishing, Internet, Crime.

INTRODUCTION

Consumers want the confidence that their financial information will be protected, regardless of how it’s accessed. The banks have reputation, brand and highly sensitive personal data to protect, and in the main, they take that very seriously. Even though banks are a popular target for hackers, they also are among the most sophisticated enterprises in the world from a security perspective. This is largely because security and online banking go hand-in-hand. Compared to today, the secure bank of the future will use more machine-learning technology and systems to proactively prevent potential breaches and data loss.

DEFINITION

Cyber crimes can be defined as the unlawful acts where the computer is used either as a tool or a target or both. The term is a general term that covers crimes like phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, spam and so on.

Cyber crime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything

*Corresponding Author

from electronic cracking to denial of service attacks. It also covers the traditional crimes in which computers or networks are used to enable the illicit activity.

Cyber Crimes can be categorized in two ways:

1. The crimes in which the computer is the target. Examples of such crimes are hacking, virus attacks, DOS attack etc.

2. The crimes in which the computer is used as a weapon. These types of crimes include cyber terrorism, IPR violations, credit card frauds, EFT frauds, pornography etc.

DIFFERENT KINDS OF CYBER CRIMES

The different kinds of cyber crimes are:

1. Unauthorized Access and Hacking: Unauthorized access means any kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. Government websites are the most targeted sites for the hackers.

2. Web Hijacking: Web hijacking means taking forceful control of another person’s website. In this case the owner of the website loses control over his website and its content.
3. Pornography: Pornography means showing sexual acts in order to cause sexual excitement. The definition of pornography also includes pornographic websites, pornographic magazines produced using computer and the internet pornography delivered over mobile phones.

4. Child Pornography: The Internet is being highly used as a medium to sexually abuse children. The children are viable victim to the cyber crime. Computers and internet having become a necessity of every household, the children have got an easy access to the internet. There is an easy access to the pornographic contents on the internet.

5. Cyber Stalking: In general terms, stalking can be termed as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim. Cyber Stalking means repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using internet services. Both kind of Stalkers i.e., Online & Offline – have desire to control the victims life.

How do Cyber Stalkers operate?

a. They collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. If the stalker is one of the acquaintances of the victim he can easily get this information. If stalker is a stranger to victim, he collects the information from the internet resources such as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website.

b. The stalker may post this information on any website related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have sexual services. Stalker even uses very filthy and obscene language to invite the interested persons.

c. People of all kind from nook and corner of the World, who come across this information, start calling the victim at her residence and/or work place, asking for sexual services or relationships.

d. Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and sex sites, because of which victim starts receiving such kind of unsolicited e-mails.

e. Some stalkers keep on sending repeated e-mails asking for various kinds of favors or threaten the victim.

f. In online stalking the stalker can make third party to harass the victim.

g. Follow their victim from board to board. They “hangout” on the same BB’s as their victim, many times posting notes to the victim, making sure the victim is aware that he/she is being followed. Many times they will “flame” their victim (becoming argumentative, insulting) to get their attention.

h. Stalkers will almost always make contact with their victims through email. The letters may be loving, threatening, or sexually explicit. He will many times use multiple names when contacting the victim.

i. Contact victim via telephone. If the stalker is able to access the victim’s telephone, he will many times make calls to the victim to threaten, harass, or intimidate them.

j. Track the victim to his/her home.

6. Denial of service Attack: This is an attack in which the criminal floods the bandwidth of the victim’s network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide. This kind of attack is designed to bring the network to crash by flooding it with useless traffic. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCp/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by Hacker.

7. Virus attacks: Viruses are the programs that have the capability to infect other programs and make copies of itself and spread into other program. Programs that multiply like viruses but spread from computer to computer are called as worms. These are malicious software that attach themselves to other software. Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious. Viruses usually affect the data on a computer, either by altering or deleting it. On the other hand worms merely make functional copies of themselves and do this repeatedly till they eat up all the available.

Trojan Horse is a program that acts like something useful but do the things that are quiet damping. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the Trojan. TCP/IP protocol is the usual protocol type used for communications, but some functions of the Trojans use the UDP protocol as well.

8. Software Piracy: Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. These kind of crimes also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc. Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws. Cyber squatters register domain name identical to popular service provider's name so as to attract their users and get benefit from them.

9. Salami attacks: These 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 the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

10. Phishing: Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. By spamming large groups of people, the phisher counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with legitimately.

11. Sale of illegal articles: This category of cyber crimes includes sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

12. Online gambling: There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Cases of hawala transactions and money laundering over the Internet have been reported.

13. Email spoofing: Email spoofing refers to email that appears to originate from one source but actually has been sent from another source. Email spoofing can also cause monetary damage.

14. Cyber Defamation: When a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends, it is termed as cyber defamation.

15. Forgery: Computers, printers and scanners are used to forge counterfeit currency notes, postage and revenue stamps, mark sheets etc. These are made using computers, and high quality scanners and printers.

16. Theft of information contained in electronic form: This includes theft of information stored in computer hard disks, removable storage media etc.

17. Email bombing: Email bombing refers to sending a large number of emails to the victim resulting in the victim’s email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

18. Data diddling: This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

19. Internet time theft: Internet time refers to usage by an unauthorized person of the Internet hours paid for by another person.

20. Theft of computer system: This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.

21. Physically damaging a computer system: This crime is committed by physically damaging a computer or its peripherals.

22. Breach of Privacy and Confidentiality: Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorized use or distribution or disclosure of personal information. Confidentiality means non disclosure of information to unauthorized or unwanted persons. In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected.

Generally for protecting secrecy of such information, parties while sharing information forms an agreement about he procedure of handling of information and to not to disclose such information to third parties or use it in such a way that it will be disclosed to third parties. Many times party or their employees leak such valuable information for monitory gains and causes breach of contract of confidentiality. Special techniques such as Social Engineering are commonly used to obtain confidential information.

23. Data diddling: Data diddling involves changing data prior or during input into a computer. The information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. It also include automatic changing the financial information for some time before processing and then restoring original information.

24. E-commerce/ Investment Frauds: An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

25. Cyber Terrorism: Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc. Cyber terrorism is an attractive option for modern terrorists for several reasons.

a. It is cheaper than traditional terrorist methods.

b. Cyber terrorism is more anonymous than traditional terrorist methods.

c. The variety and number of targets are enormous.

d. Cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists.

e. Cyber terrorism has the potential to affect directly a larger number of people.

The list of offenses given above is not exhaustive and would also include any other types of offenses that would be committed through a computer or against a computer in the future

CYBER LAWS

Cyber crimes are a new class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cyber crimes.

The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

1. Cyber crimes under the IT Act :

- Tampering with Computer source documents - Sec.65
- Hacking with Computer systems, Data alteration - Sec.66
- Publishing obscene information - Sec.67
- Un-authorised access to protected system Sec.70 Breach of Confidentiality and Privacy - Sec.72
- Publishing false digital signature certificates - Sec.73

2. Cyber Crimes under IPC and Special Laws :

- Sending threatening messages by email - Sec 503 IPC
- Sending defamatory messages by email - Sec 499 IPC
- Forgery of electronic records - Sec 463 IPC
- Bogus websites, cyber frauds - Sec 420 IPC

- Email spoofing - Sec 463 IPC
- Web-Jacking - Sec. 383 IPC
- E-Mail Abuse - Sec.500 IPC

3. Cyber Crimes under the Special Acts:

- Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act
- Online sale of Arms Arms Act

HOW TO FILE A COMPLAINT?

The complaint regarding commission of cyber crime can be made to the in-charge of the cyber crime cells which are present almost in every city. To file a complaint alleging commission of a cyber crime the following documents must be provided:

1. In case of hacking the following information should be provided:

a. Server Logs

b. Copy of defaced web page in soft copy as well as hard copy format, if your website is defaced

c. If data is compromised on your server or computer or any other network equipment, soft copy of original data and soft copy of compromised data.

d. Access control mechanism details i.e.- who had what kind of the access to the compromised system

e. List of suspects – if the victim is having any suspicion on anyone.

f. All relevant information leading to the answers to following questions –

- what ? (what is compromised)
- who? (who might have compromised system)
- when?(when the system was compromised)
- why?(why the system might have been compromised)
- where?(where is the impact of attack-identifying the target system from the network)
- How many?(How many systems have been compromised by the attack)

2. In case of e-mail abuse, vulgar e-mail etc. the following information should be provided:

a. Extract the extended headers of offending e-mail and bring soft copy as well hard copy of offending e-mail.

b. Please do not delete the offending e-mail from your e-mail box.

c. Please save the copy of offending e-mail on your computers hard drive.

Is secure banking an unrealistic goal?

Even though banks are a popular target for hackers, they also are among the most sophisticated enterprises in the world from a security perspective. This is largely because security and online banking go hand-in-hand.

Consumers want the confidence that their financial information will be protected, regardless of how it's accessed. The banks have reputation, brand and highly sensitive personal data to protect, and in the main, they take that very seriously.

How will banks combat cyber crime in the future?

Compared to today, the secure bank of the future will use more machine-learning technology and systems to proactively prevent potential breaches and data loss.

In other words, we will see more 'attack as the best form of defence. They will also defend the sensitive data they hold at every potential access point, regardless of whether that is a mobile device, internal network, connected internet of things device, through a website, through an app etc. And of vital importance, they will all then add more protection to the databases themselves that hold the key to the information the criminals are after.

CONCLUSION

In the selected subject of work, we made a thorough study on the new forms of crimes. The criminals of this advanced age endeavor to commit these new crimes with the help of computers through Internet by exploiting cyber space. An estimated 95% of transactions in India are paid for in cash but with the growing penetration of computers and smartphones, and increasing access to the internet, Indians are taking to digital channels for their banking needs. Cybercrime is becoming a greater threat as a result

The cybercrime is a primarily example of cross-border crime. Since the jurisdiction in this area is a tricky and is still unclear, it is important that we recognize the need of the hour and stand for a serious cause, against cybercrimes and more so pertaining to the banking sector as the financial security of this sector defines the financial security and safety of the assets of our nation as a whole. India, being at its stage of development, we cannot risk the safety of such an essential unit. If we are able to curb these attacks, one by one, soon in the time to come, this move will help us accelerate the rate of overall growth and development and take further steps towards betterment.

REFERENCES

[1] http://www.cyberlawsindia.net/

[2] https://m.rediff.com/amp/business/report/perfin-if-you-are-a-victim-of-banking-fraud-heres-what-you-can-do/20150720.htm

[3] https://www.google.co.in/url?sa=t&source=web&rct=j&url=http://m.timesofindia.com/business/india- business/demonetisation-case-ed-files-first-chargesheet-involving-axis-bank-staff/amp_articleshow/56959891.cms&ved=0ahUKEwi4q

[4] https://www.google.co.in/url?sa=t&source=web&rct=j&url=https://m.economictimes.com /industry/banking/finance/ba nking/hdfc-bank-begins-probe-after-staff-held-in-money-

launderingcase/amp_articleshow/49365032.cms&ved=0ahUKEwilwZuOkcHYAhVLP48KHT4rC0kQFggnMAE&usg=AOvVaw 3RKUP0SVWnDDJWUy3OvmSZ&ampcf=1

[5] www.conferenceworld.in

[6] www.thehindubusinessline.com

[7] https://www.journalguide.com/journals/international-journal-of-cyber-criminology