International Research Journal of Human Resources and Social Sciences
Vol. 4, Issue 3, March 2017 Impact Factor- 5.414
ISSN(O): (2349-4085) ISSN(P): (2394-4218)
© Associated Asia Research Foundation (AARF)
Website: www.aarf.asia Email : editor@aarf.asia , editoraarf@gmail.com

SPAM A CYBER CRIME USING A KNOWLEDGE TRICK

Ajay Singh,
Assistant Professor Northern India Institute of Fashion Technology,
Mohali (Govt. of Punjab), India.

ABSTRACT

Spamming is a very common form of cybercrime. Spam is basically unwanted emails and message. Cyber Crime is a social engineering attack that scares every internet user, banks, companies and many other organizations. Cyber crimes are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime. Additionally, cyber crime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet. Internet fraudsters imitate a website or business to trick the people into giving out their personal, banking, and other credential information. Genuine businesses never ask anybody to send sensitive information through insecure channels.

Due to lack of awareness and knowledge, cyber crimes are increasing dramatically, resulting financial and emotional loss and it also affects psychologically. However, today more and more ways are trying to be found and new technologies are being devised to deal with the cyber crime attacks. This is being achieved through the use of various legislations and cyber laws along with training people how to detect and deal with such attacks. In this paper the best available detection and prevention techniques are being proposed to prevent from becoming the victim of cyber crime/hacking or a malware/Spam attack.

Keywords: Spam, Cyber laws, Internet fraud, Cyber attack, hacking, internet fraud

I. Introduction

From business, industry, government to not-for-profit organizations, the internet has simplified business processes such as sorting, summarizing, coding, editing, customized and generic report generation in a real-time processing mode. However, it has also brought unintended consequences such as criminal activities, spamming, credit card frauds, ATM frauds, phishing, identity theft is highly disturbing. Over the past twenty years, immoral cyberspace users have continued to use the internet to commit crimes; this has evoked mixed feelings of admiration and fear in the general public along with a growing unease about the state of cyber and personal security. The best way to someone can protect himself from spamming is to avoid supplying personal information to an email request.

In order to avoid being victim, user should take proper security precautions every time he/she on the Web. Virus protectors and firewalls do not catch most spams because they do not contain suspect code, while spam filters let them pass because they appears to come from legitimate sources. The most common way that cyber criminals attempt to gain access to the sensitive information is by creating "look- a-like" websites that resembles like the original websites or by sending an email or instant message to the Internet or mobile users. Recipients of these fake e-mails are requested to click on these links and to provide their personal and credential information. After getting the enough personal information from victim, cyber criminals then can commit a variety of fraudulent and other criminal activities in the victim's name. Cyber Crime is a global problem now and number of anti-phishing activities and awareness camps are going on to reduce its graph.

II. How Spam-Cyber Crime Works in Modern Society

Today, criminals that indulge in cyber crimes are not driven by ego or expertise. Instead, they want to use their knowledge to gain benefits quickly. They are using their expertise to steal, deceive and exploit people as they find it easy to earn money without having to do an honest day's work.

Spams have become a real threat today and are quite different from old-school crimes, such as robbing, mugging or stealing. Unlike these crimes, cyber crimes can be committed single handled and does not require the physical presence of the criminals. The crimes can be

committed from a remote location and the criminals need not worry about the law enforcement agencies in the country where they are committing crimes. The same systems that have made it easier for people to conduct e-commerce and online transactions are now being exploited by cyber criminals. With increase and expansion of technology cybercrime has also increased and expanded. These types of offenses are rapidly replacing existing styles as the number one crime. This situation imposes a drastic effect upon society. The focus and funding of law enforcement is being stretched thin. This leaves less attention and financial means to enforce against serious crimes such as theft, drugs, and murder.

SPAM, has become one of the biggest problems facing the Internet today. In fact Spam and the "patchwork" attempts to reduce Spam have turned email into an unreliable Internet tool today. If you talk to some end users they don't see much difference between Spam and the ordinary junk mail that mail carriers have delivered for years. They may say "all you have to do is hit delete". Obviously these people have never had hundreds of Spam messages hit their inbox in a very short period. Additionally they have never run a network or email gateway. The cost to corporations in bandwidth, delayed email, and employee productivity has become a tremendous problem for anyone who provides email services. Many customers think their Internet Service Provider (ISP) should be able to fix the problem. But Spam is a world-wide problem, and email systems around the world are not setup in a consistent manner. Cybercrime is a heavy burden on society. It is estimated that these types of crimes result in damages over a half of a billion dollars annually. Companies are becoming so frustrated that recently Microsoft offered a quarter of a million dollar reward for the capture of the individuals responsible for the MSBlast worm and the SoBig.F virus. One of the most successful software companies in the United States has had to resort to posting a bounty for cybercriminals. This seems very similar to the anti-crime tactics of the billboards located in inner city neighborhoods that offer reward money for information leading to the arrest of individuals involved in violent crimes.

Cyber Scams illustration:-

a) A very popular e-mail scam received by almost every e-mail user is Lottery scam. You might receive messages that claim that you have won the lottery of $80,000. These messages might even look like they come from a legitimate source.

So if ever you receive these kinds of e-mails, delete themimmediately. A demonstration of such type of e-mail is given below.

THE LOTTERY DEPARTMENT BMW Automobiles
22 Garden Close, Stamford, Lincs, PE9 2YP, London
United Kingdom

Dear Winner,

This is to inform you that you have been selected as a winner for a cash prize of £350,000.00 (Three hundred and fifty thousand Great British Pounds) and a brand new BMW 5 Series Car from International programs held on the 9th of 2010 in London Uk. Description of prize vehicle is given below;

Year: 2009, Model: 530iA, Colour (exterior/interior): Back Sapphire

Metallic/Black Leather, Mileage: 5, Transmission: Automatic 6 speed

The selection process was carried out through random selection in our computerized email selection ballot system from a database of over 250,000 email addresses from which you and nine others were selected as the winners. To begin the processing of your prize you are to contact our fiduciary claims agent for more information as regards procedures to claim your prize.

BMW LOTTERY DEPARTMENT UK
7 DOCK WAY, SEFTON BUSINESS PARK
LONDON, T40 4RT United Kingdom

Contact him by please providing him with your secret pin code x7pwyz2005 and your Reference Number BMW: 2551256003/23.You are also advised to provide him with the under listed information as soon as possible:

1. Name:

2. Address:

3. Contact number:

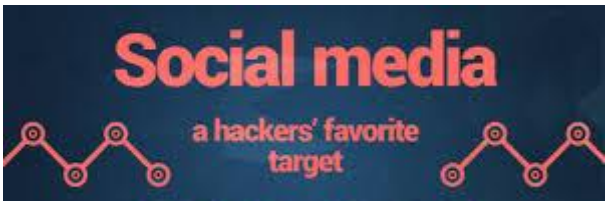
4. Name of Bank:

5. Bank account number:

6. Netbanking password:

III. Types of Spam-Cyber Crime

a) Hacking- Hacking or Cracking is a major cyber crime committed today. Hacker makes use of the weaknesses and loop holes in



operating systems to destroy data and steal important information from victim's computer. Cracking is normally done through the use of a backdoor program installed on your machine. A lot of crackers also try to gain access to resources through the use of password cracking soft wares. Hackers can also monitor what u do on your computer and can also import files on your computer. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal information such as passwords and credit card information. Important data of a company can also be hacked to get the secret information of the future plans of the company.

b) Viruses and worms- Viruses and worms is a very major threat to normal users and companies. Viruses are computer programs that are designed to damage computers. It is named virus because it spreads from one computer to another like a biological virus. A virus must be attached to some other program or documents through which it enters the computer. A worm usually exploits loop holes in software's or the operating system.

Trojan horse is dicey. It appears to do one thing but does something else. The system may accept it as one thing. Upon execution, it may release a virus, worm or logic bomb. A logic bomb is an attack triggered by an event, like computer clock reaching a certain date. Chernobyl and Melissa viruses are the recent examples.

c) c) Software Piracy-Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. Retail revenue losses worldwide are ever increasing. This crime can be done in various ways such as end user copying, hard disk loading, Counterfeiting, Illegal downloads from the internet etc.

d) d) Credit Card Fraud-The user need to type credit card number into www page off the vendor for online transaction. If electronic transactions are not secured the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner.

e) e) Cyber Stalking-The Criminal follows the victim by sending emails, entering the chat rooms frequently.

IV. Prevention of Spam-Cyber Crime

f) Keep your computer secure – Activate your firewall which is your first line of defense against unauthorized access to your computer. Also be sure to install anti-virus/malware and anti-spyware software which prevent, detect, and remove malicious software, spyware programs, worms, Trojans, adware, and viruses. Keep up with any software updates.

g) Choose strong passwords – A good password is one that cannot be guessed easily. They typically have over eight characters and contain a combination of numbers, letters, and symbols (e.g., $, #, &), as well as a mix of upper- and lowercase letters. Use uncommon words. Use different passwords for different sites, and choose especially secure passwords for your online banking sites.

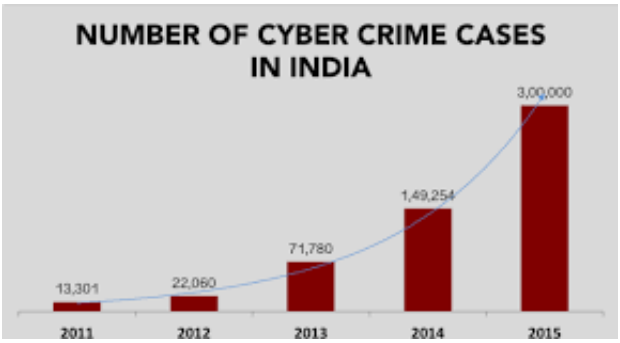
h) Protect your personal information – Sharing personal information such as your name, phone number, address, or credit card information is inevitable if you are making online purchases. Do business with companies that have websites that begin with “https:” – the “s” stands for secure – and look for a “lock” icon on the status bar of your Internet browser. Enable privacy settings when accessing social media sites and do not over share

information about yourself online. Cybercriminals use that type of personal information to answer "challenge" questions on online banking and other websites.

i) Fight phishing – Cybercriminals often using "phishing" as a way to scam people into sharing personal information. They send fraudulent emails or set up fake websites that look like legitimate businesses. To avoid phishing scams, never respond to spam, communicate personal information only through a phone or a secure website, and do not click on links or download files from unknown senders. Verify that a website is the official website before sharing any personal information.

j) Watch your wireless network – Properly secure your Wi-Fi networks at home so that cybercriminals can't hack into your computers. Here are tips on how to do this.

V. Cyber Crime-Facts and Figures



There were more than 314,000 cyber crime reports in 2011, with about 116,000 reporting a loss, according to the Internet Crime Complaint Center. The center states that the top five cyber crime complaints were FBI-related scams, identity theft, advance fee fraud, non-delivery of merchandise fraud and overpayment fraud. The average cyber crime loss was estimated at $1,500, and the total annual loss was more than $485 million. According to Cyber Crime Watch magazine, about 75 million scam email messages are sent every day, victimizing about 2,000 people. The majority of Internet hackers -- 66 percent -- are American. According to the magazine, Americans have discouraging views on cyber crime. While it's estimated that about 25 percent of all cyber crimes go unsolved, 78 percent of Americans believe most criminals won't be caught, and only 2 percent believe they won't experience cyber crime at some point in their life.

VI. Cyber Offences and Laws

In India the Information Technology Act 2000 was passed to provide legal recognition for transactions carried out by means of electronic communication. The Act deals with the law relating to Digital Contracts, Digital Property, and Digital Rights Any violation of these laws constitutes a crime. The Act prescribes very high punishments for such crimes. Anyone who

destroys deletes or alters any information by any means with intent to cause damage to the public or private system commits cybercrime The Information Technology (amendment) Act, 2008(Act 10 of 2009) , has further enhanced the punishments. Life imprisonment and fine up to rupees ten lakhs may be given for certain classes of cyber crimes.

VII. Conclusion

Cyber crime poses a big threat to both national and international security. The cyber crime is a new invention of crimes made by a class of intellectual, sophisticated criminals. The country need to establish its laws and establishment of these laws alone is not enough, educating the masses against cyber crime and strict enforcement of these laws is also necessary. The software's are easily available for download should be restricted by the Government by appropriate actions. New amendment should be including to the IT Act, 2000 to make it efficient and active against the crimes. The training and public awareness programs should be organized in the Companies as well as in common sectors. The number of the cyber cops in India should be increased. Technology makes the things easier but a user has to be aware of the threats and dangers that can be paused by the misuse of technology and hence cause financial and other loses. Awareness among users is must and they should put a cross to their curiosity factor that makes them open the phishing mails and hence become victim of these attacks. If somehow users have been trapped in this technology trap, awareness regarding the necessary actions and reporting to the Cyber organizations should be clear and followed. Technology like network is a boon for the users, but lack of awareness can turn it to a curse. So be aware for these kinds of attacks and surf the net safely.

References

[1] Cybercrime: A Reference Handbook, Bernadette Hlubik Schell, Clemens Martin ABC-CLIO, 2004

[2] Corporate Hacking and Technology-driven Crime , Bernadette H. Schell, published:

[3] "Technical trends in cyber crime" by Jason Milletary.

[4] "Threats and Solutions: Phishing" by Trend Micros's.

[5] "The Perpetration and Prevention of Cybercrimes" by Stanley Kratchman, Jacob Lawrence Smith and Murphy Smith.

[6] "Impact of Cybercrime on Virtual banking" by Subramoniam Arumuga Perumal.

[7] “Privacy and the information technology act in India” by Prashant lyengar.

[8] “A Review of the Economics of Information Security Literature” by Mike Hammock.

[9]“www.wikipedia.com” An online encyclopaedia.

[10] “Strategies for Securing the Cyber Safety Net for Terrorists: A Multi- Disciplinary approach” by Doris Estelle Long.