Cyber Crime

Dr. JATINDER KUMAR
Assistant Professor
A.S. College, Khanna. Punjab (INDIA)
PG Department of Computer Science and Applications

Abstract

The risk of cyber crime has become a global issue affecting almost all countries in the world. It is a criminal activity involving any computing device and the communication networks. Internet is a "double edge" sword providing many opportunities for individual and organizations to grow both financially and geographically, but at the same time has bought with it new opportunities to commit crime. The main goal of cyber crime to gain unauthorized access to sensitive information of any organization or an individual. This paper throws light on the term cyber crime, its various categories and the precautionary measures which can be taken to prevent these crimes. The primary objective of this paper is to raise awareness regarding legal loopholes and enabling technologies, which facilitate acts of cyber crime.

Keywords: Cyber crime, hacking, cyber fraud, unauthorized access.

Introduction

With the advent of IT and ITeS, where the use of IT has increased many fold, along with that the abuse has also increased. Use and abuse are the two issues of the same coin. Technical experts, police, lawyers, criminologists, and national security experts understand the concept of 'cyber crime' differently. It is unclear that whether cyber crime refers to legal, sociological, technological, or legal aspects of crime and a universal definition remains elusive. The abuse of ICTs by criminals is interchangeably referred to as cyber crime, computer crime, computer misuse, computer related crime, high technology crime, e-crime, technology-enabled crime, amongst others. Cyber crime refers to the act of performing a criminal act using computer or cyberspace (the Internet network), as the communication vehicle. Following this definition, cyber crime is merely *a sub-set of conventional crime where ICTs are used as a vehicle or tool to commit traditional criminal offences*. Though there is no technical definition by any statutory body for Cyber crime, it is broadly defined by the Computer Crime Research Center as - "Crimes committed on the internet using the computer either as a tool or a targeted victim." All types of cyber crimes involve both the computer and the person behind it as victims; it just depends on which of the two is the main target. Broadly, the word cyber crime includes the following features:

• The conduct is facilitated *by information and communications technology;*

• The conduct is motivated by *intent* to commit *harm* against a *person* or *organization;*

• The perpetrated or intended harm encompasses conduct amounting to *interference* or *damage* to either *tangible* or *intangible property* owned by a *person* or *organization;* and

• The conduct concerned is *criminalized* within either the *jurisdiction of the victim* or the *jurisdiction of the accused.*

Categories of Cyber Crime: The cyber crime can be divided into the following categories:

1. **Fake websites**: Fake websites are generating billions of dollars in fraudulent revenue at the expenses of unsuspecting internet users. The growth of these sites is due to several factors including their authentic appearance, lack of user awareness. A spoof site is an imitation of existing commercial site. A variation of take website is fraudulent email selection where sender sends an email claims an association with some reputed organization. Email says your email is selected in a lucky draw of worth some large amount and the email proceeded to ask for the potential victims' personal information and some advance money to transfer the funds to their accounts.

2. **Money Laundering**: Money laundering is an activity of transferring illegally acquired cash through financial or other system so that it appears as it is acquired legally.

3. **Bank Fraud:** In banking sector criminal acts often linked to financial aspects. There are many cases of illegal loan sanctioned to an investor. The investors are deceired into investing money in a financial project that is said to be producing a high profit. When the loan is sanctioned by the bank authority, offer some time investor loose their money because no investment actually takes place and no actual project exits that money is divided between the investor and the various middleman.
4. **E-Mail Spoofing**: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates. SMS Spoofing: Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals

identity of another person in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual. Carding: It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account. There is always unauthorized use of ATM cards in this type of cyber crimes.

5. **Cyber pornography**: Online environment has a potential for misuse and has generated societal concerns. Today, there is a big concern for children because internet provides anonymity to predators. Screening video and photographs of sexual exploitation of children and women. Making pornographic video, m clipping or distributing such clipping through internet using mobile or any other computing device falls under this category.

a. ***Phishing:*** The Phishing is a form of online identity theft that lures consumers into divulging their personal financial information to take websites also known as spoofed websites. How this is done? It starts with an email; the phiser sends an email to an unsuspected victim instructing him to click on the given link to a bank's website to confirm his account information. The customer provides the information, thereby enabling the phisher to steal his personal account info or financial info. Now the phisher then use this information to withdraw the money from victims' account or commit other forms of identity theft.

b. ***Pharming:*** It is similar to Phishing but more complex and sophisticated in its operation. Pharmer also sends an email. The consumer compromises his personal information or financial information simply by opening this email message actually this email contains a Trojan Horse that installs a small software program on user's computer. When the customer tries to open the official site, the phasmers' fake version of the website. In this way the pharmer is able to capture the personal financial information.

c. ***Password Sniffers***: Password Sniffers are malicious programs that monitor and record the username and password of internet users also log on to network. This program work by collecting bytes typed by the user and send this information to installer of that program.

d. ***Cyber bullying***: In this Cybercrime the offender sends the threatening messages, altering images and distributing them with the intent to harasses or intimidate.

e. ***Cyber Terrorism***: It is violence spread across the specific area using digital media or internet which is commonly politically motivated, committed against a civilian or a specific community by sending some objectionable content over the internet.

f. ***Denial of Service***: It involves flooding computer resources with more requests then it can handle. Which causes to crash thereby unavailability of that particular resource? E.g. If a customer, intending to buy something online, tries to connect to a company's website at 10:00 and web browser displays into message "website temporarily unavailable", he might back at 10:45 am and still receives the same message then the customer will go to a competitor to buy the product. For one company, an online bookstore, the attack resulted in lost revenue.

g. ***Software Privacy***: It is an illegal reproduction or distribution of software for individual, business, industrial or scientific use. It is considered as a violation of copyright and license agreement rule.

h. ***Forgery:*** Counterfeit currency notes, revenue and postage stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners.

i. ***Cyber Stalking:*** The meaning of cyber stalking is pursuing stealthily. It involves following a persons' activity across the internet by posting messages (threatening), on the chat room, or bulletin board used by the victim.

WAYS TO PREVENT CYBER CRIME

Below mentioned security guidelines and good practices may be followed to minimize the security risk of Cyber crime:

Keep the computer system up to date:-Cyber criminals will use software loop holes to attack computer systems frequently. Most Windows based systems can be configured to automatically download software patches which nothing but some code to prevents attackers.

By protecting computer with antivirus and antimalware software:- Antivirus is a software to prevent malicious software programs from harming your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. In today's world of computers each day a new virus is introduced, so Failure to keep this software current is where a majority of the issues arise. The firewall monitors all data flowing in and out of the computer to the Internet, often blocking attacks from reaching the system.

By choosing strong passwords: username and passwords are used online for every identification over the internet. Always select a password that have at least eight characters and use a combination of letters, numbers, and symbols (e.g. # $ % ! ?). Avoid using easy password like name, city name etc. use non dictionary words. Using the same password for various sites or systems increases the risk of discovery and possible exploitation. Change passwords on a regular basis, at least every 90 days

Online offers that **seems too good to be true, it is:-** No one is going to receive a large sum of money from any person which you do not know, win a huge lottery from being "randomly selected from a database of email addresses". They actually want your personal and financial information for any criminal activity. Many of these crimes go unreported because the victim is too embarrassed to admit to law enforcement that they were duped.

Be Social-Media Savvy: Make sure social networking profiles (e.g. Facebook, Twitter, etc.) are set to private. Check security settings with in frequent intervals. Be careful what information post online.

Download Secure app for mobile Devices: Be aware that mobile device is vulnerable to viruses and hackers. Download applications from trusted sources.

Secure your wireless network with password: Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Avoid using public Wi-Fi spots.

Present Scenario of Cyber Crime in India

According to the latest report by National Crime Records Bureau (NCRB) for the previous year - 2013, 681 cyber crime related cases have been registered in Maharashtra, which has seen a 44.6 per cent rise in cyber crimes when compared to 2012. Andhra Pradesh with 635 cases registered in 2013 has also seen a 48 per cent rise when compared to 2012. Karnataka with 513 cases registered in 2013 has seen a 24.5 per cent rise when compared to 2012. Uttar Pradesh with 372 cases registered in 2013 is in the fourth place. It has seen a huge rise of 81.5 per cent in just one year. Kerala is in the 5th place with 349 cases registered in 2013. Among the bigger states Tamil Nadu and Bihar have very few cyber crime related cases. Just 54 cases have been registered in Tamil Nadu and just 23 cases have been registered in Bihar in 2013. Gujarat and Odisha have also registered just 61 and 63 cases respectively in 2013. In a positive development, the Northeastern states of Mizoram, Nagaland and Sikkim have not seen a single cyber crime related cases in 2013. Among the Union Territories, the national capital Delhi has registered 131 cyber crime related cases. It has seen a rise of 72.4 per cent when compared to 2012.

Lakshadweep, Dadra Nagar and Haveli have not seen a single case of cyber crime in 2013. There have been 4356 incidents of cyber crimes in the year - 2013. There is a rise of 51.5 per cent cases in just one year.

India's IT capital Bangalore has seen the highest number of cyber crime cases in 2013. The city has registered 399 cases in the same year. Visakhapatnam in Andhra Pradesh has registered 173 cases and Hyderabad has registered 159 cases. Jaipur has seen 110 such cases in the same year. Mumbai has seen just 40 such cases and another IT city Pune has seen 97 cyber crime related cases while 84 such cases have been registered in Kolkata. Chennai has seen just 5 such cases.

Conclusion: Cyber crime computer has a drastic effect on the world in which we live. It affects every individual irrespective of the nature of their work. Many hackers view the Internet as public space for everyone and do not see their actions as criminal. Hackers are as old as the Internet and many have been instrumental in making the Internet what it is now. The use of It has changed our life in a big way, but the need is to check its abuse . The use of computers should be checked, so that a balanace between use and enjoyment can be created . Governments worldwide have shown marked reluctance to scrutinize the effectiveness of state-controlled mechanisms for investigating and prosecuting serious instances of cyber crime offending, as the basic purpose of use of internet is openness, sharing and mobility. But still the governments have chalked out the plans for implementing measures to keep a check on the misuse of computer and is taking measures to control the cyber crime. But apart from the initiative taken by government, the need is to check the psychology of the users and their attitude towards the technology. It is high time for all of us to learn that this technology is a boon for us and it should not be converted into curse.

References:

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.

Cameron S. D. Brown, Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, International Journal of Cyber Criminology, Vol 9 Issue 1 January – June 2015

Pocar, F. (2004). Defining Cyber-Crimes in International Legislation. European Journal on

Criminal Policy and Research, 10, 27–37.

Goodman, M. D., & Brenner, S. W. (2002). The Emerging Consensus on Criminal

Conduct in Cyberspace. International Journal of Law and Information Technology, 10(2),

139-223.

Harpreet Singh Dalla, Geeta, Cyber Crime – A Threat to Persons, Property,Government and Societies International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013