IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 3, Issue 6)
Available online at www.ijariit.com

Cyber Crime: A Potential Threat and Remedies

Dr Nitan S. Kotwal
Government Higher Secondary School Chinta Bhaderwah,
J&K, India
nitankotwal@hotmail.com

Abstract: Cybercrime is an illegal activity performed by an individual or by a group of experts in computer technology using the Internet. It ranges from stealing money online from an individual to big corporate using the internet. In the present era of information technology, the computer has made the life easy. People use computer or mobile to perform various jobs on the Internet. So it is necessary to know how to perform various transactions on the internet safely. Everyone is prone to the attack from the cyber criminals. One must be aware and should have knowledge of cybercrime.

***Keywords: Cybercrime, Hackers, Website, Cyber Attack, Emails, Online Transaction*.**

I. INTRODUCTION

A crime committed or facilitated through the Internet is a cybercrime. It is a criminal activity that involves computers and networks. It is emerging as a serious threat worldwide. In the current scenario, computer and Internet have become a parallel form of life. Anyone using computer and Internet can do things which were not imaginable a few years back. The growing dependence of people on the Internet made it an inseparable entity. Although Internet has provided a lot of facilities for the betterment of mankind like e-mails, online shopping, and online transactions and so on at the same time, it poses threat to the society. The availability of highly sophisticated technology tools made Internet vulnerable to criminals. The persons who do crime through the use of computer and Internet are known as Cybercriminals and the whole criminal activity is known as cybercrime. It includes fraud, unsolicited emails (spam), downloading illegal files, distant theft of government or corporate secrets, stealing millions of rupees online, creating viruses on others computers etc. It can cause a huge financial loss to an individual or an organization. Since India also become the third largest number of Internet users after USA and China. So anyone can become the victim of cybercrime so it is necessary to know what actually cybercrime means and how we can prevent it.

II. CLASSIFICATION OF CYBERCRIME

Cybercrime can be classified into a number of types. A number of Internet frauds range from phishing, usage of stolen Credit Cards / Debit Cards, unauthorized access to information system, transferring illegal items through the internet, fictitious offers of funds transfer, remittance towards participation in the lottery, money circulation schemes and other fictitious offers of cheap funds etc. A list of most common type's cyber-crimes is listed below:

1. **Spamming:** It is sending of the unsolicited bulk of emails through manual or automated techniques over the Internet. Most of the emails are commercial messages. Sometimes the intent is to disable to notice important message. Although it irritates but it is not illegal unless it causes damage such as overloading. In India Section 43, 66A, 66D (Compensation and punishment of three years) in IT Act, 2000 and Amendments deals with Spamming.

2. **Hacking:** It is an illegal access to the data stored in the computer systems or network resources without authorization. A hacker is an unauthorized user who attempts to or gains access to a computer system. Hacking is a crime even if there is no visible damage to the system because it is an invasion of the privacy of data. In India Section 70 (Punishment of ten years with fine) in IT Act, 2000 and Amendments deals with Hacking.

3. **Cyber Stalking:** It is the process of stealthily following a person by the use of the Internet or using other electronic communication, such as e-mail, posting a message on a website or a social networking site etc. It also involves online harassment, sending threatening messages, online abuse, altering images etc. The intent of all these things is to harass or intimidate someone. Normally, the majority of cyber stalkers are men and the majority of victims are women. In India Section 43 and 66 (Compensation and punishment of three years with fine) in IT Act, 2000 and Amendments deals with Cyber stalking.

4. **Cyber Pornography:** It is the act of publishing or transmitting obscene material or sexually explicit act over the Internet by using electronic media such as websites, social networking sites etc. Most of the victims of cyber pornography are children and women. Pedophiles target children by sending pornographic material over the Internet to sexually exploit them. In India Section 67A (Punishment of five years with fine) in IT Act, 2000 and Amendments deals with Cyber Pornography.

5. **Phishing:** It is the attempt to obtain sensitive information such username, passwords, and debit/credit card details by disguising as a trustworthy entity in an electronic communication. It uses social engineering techniques to deceive users and exploits weakness in current web security. India Section 43, 66, and 66C (Compensation and punishment of three years with fine) in IT Act, 2000 and Amendments deals with Phishing.

6. **Cyber Terrorism:** To exploit the one section of the civil population by misguiding them to take arms against other section or against the country by mongering hate speech and floating the same on social media by the use of the Internet. It is a form of violence to intimidate or coerce a government, any section or group to achieve its political or social objective.

7. **Spoofing:** It is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. It is an attempt by the intruder to gain unauthorized access to a user's system or information by pretending to be the user of that system. One of the best known spoofs is Email spoofing. The spoofed emails may request for personal information so that they can access the victim's bank account, password contact number etc.

8. **Personal Data Theft:** It is an attempt by criminals to steal the personal data such as name, address, contact number, Email address for malicious purposes.

9. **Money Laundering:** The process of moving illegal money through financial or other systems so that it appears legally acquired money. Cash is transported to such a country that has less stringent banking regulations and it is moved back by the way of loans. It was also possible prior to the internet but the use of computer technology made is easier and much successful.
10. **Destroying Data:** It is an activity of destroying valuable data or information from the Internet with an intention to deprive users of the information. It is done by installing malicious code such as viruses, worms.

11. **Human Trafficking:** It involves exploiting people for forced prostitution, forced labour, forced begging, forced marriage, forced organ removal etc. The target is selected by luring, soliciting by advertizing on the Internet. Most of the victims of this crime are children and women.

12. **Credit/Debit Card Fraud:** It is fraud in which someone uses your credit card or credit account and make unauthorized transactions. It can happen either you lose your credit card or someone has stolen it. Fraudsters can also obtain credit card number and pin to do unauthorized transactions.

13. **Web Jacking:** It refers to forcefully taking control of the website by cracking the password and then changing it. In this case, the actual owner of the website loses control of the website. The person who takes control of the website is known as a hacker. A website is hacked either for ransom or due to enmity between people, the enmity between countries. There are various techniques by which hacker may get to know the id the password. One of the most common techniques to crack the password is by using cracking software to guess the password. Password cracking is done by two types. First is Dictionary attack and second is a Brute force. In dictionary attack, the software attempts all the words contained in a predefined dictionary of words. While in brute force software tries to guess the password by trying out all the possible combinations of letters (uppercase, lowercase), numbers, and special character until the correct combination is found.

14. **Online Gambling:** Online gambling also comes under cyber crime, although it is legal in some countries.

III. CYBERCRIME PREVENTION STRATEGIES

Cyber criminals are like traditional criminals who want to make money as quick as possible through unfair means. A cyber attack can happen to anyone ranging from individuals to multinational companies to banks to government. Everyone is vulnerable to cyber attack. No one is immune to cyber attack. Sometimes it affects millions of people. Cybercrime prevention can be achieved by having little technical knowledge and common sense. It is just like protecting our home and office by locking them. The following strategies if adopted can prevent online fraud.

1. **By Keeping the Computer System up to Date:** The best way to avoid cyber attackers from damaging your system is to update the system regularly. Whenever patches and updates are available they should be incorporated into the system. If the system is not updated, the cyber attackers can take advantage of the vulnerabilities (software flaws) and can cause damage to the system. It is difficult for the hackers to gain access to an updated computer system. Recent versions of Microsoft Windows can be configured to download software patches and updates automatically. By keeping the system up to date cyber attackers may be thwarted.

2. **Computer System Should be Configured Securely:** The newly purchased computer may not have the right level of security so it is important that the newly purchased must be configured securely. Internet applications such as web browser are a most important application to be configured. The security settings in the web browser must be such that it does not frustrate the user with too many questions. The computers should be configured to a security level that is appropriate and comfortable to the user.

3. **Choose a Strong Password and Keep it Confidential:** In the present era of technology, the importance of passwords has become essential. In our day to day life, we use the Internet for everything from paying bills, recharging mobiles, booking a ticket, online payment for online purchases etc. For every online transaction, we are provided with a user id and password. The password must be strong enough and should consist of at least twelve characters and must have at least one lower case letter[a-z], one upper case letter[A-Z], one numeric character [0-9] and one special character. Using the same password for various sites should be avoided. Always memorize the password and never write a password and leave it. It is a good practice to change the password after every 100 days. Avoid using personal information in the password such as name, date of birth, mobile number and words that are found in the dictionary.

4. **Network Firewall Should be turned on:** The first line of defense to your computer is a firewall. It controls who and what can communicate with your computer online. It is like a policeman that watches all the data attempting to flow out and flow in of your computer on the internet. It allows the communications that are safe and blocks those communications that it thinks are bad and can cause damage to the system.

5. **Antivirus should be installed on the system:** The next line of defense after the firewall is antivirus software. It monitors all the online activities like emails, web browsing, protects a computer system from viruses, worms, Trojan horse and other types of malicious programs. The antivirus software should be configured to update itself every time the computer system is connected to the internet. A number of antivirus software is available in the market such as Kaspersky antivirus, Norton antivirus etc.

6. **Personal Information Should be protected:** Nowadays many online services involve sharing of personal information such as name, phone address, location, and email address. So it is necessary to differentiate between the authentic and fraud service. By using common sense and some precautionary measures one can prevent from cybercrime. Avoid responding to messages that contain a misspelling, poor grammar, odd phrases, or web sites with strange extensions. When there is doubt in an email, call the organization telephonically to verify authenticity. Whenever visiting a website always type the address (URL) of the website in the address bar instead of clicking on a link. Furthermore always remember that any website with the financial transaction should have an “s” after the letters “http” (e.g., https://www.jkbankonline.com and not http://www.jkbankonline.com). The “s” stands for secure and should appear when you are in an area requesting you to login or provide other sensitive data. Another sign for a secure connection is a small icon of a lock in the status bar.

7. **Read the privacy policies on websites and in software:** Always read the privacy policies of various social networking sites and other web applications that involve photo and personal information sharing. Some websites retain information about the user even after the original has been deleted by the user. They can use this personal information for various purposes. They use this information for finding a potential victim. One should be careful while sharing his or her email address in social networking sites, newsgroups, blogs, discussion groups etc.

8. **Review Bank and Credit card statement regularly:** It is a good practice to review credit card and bank statements regularly to reduce the impact of identity theft and credit card fraud. Unusual shopping behavior should be brought in the notice to the customer by the bank.

9. **Online offers that look good are not always true:** Cyber criminals send a number of emails and messages on mobile number regarding winning a huge lottery to potential targets randomly. They ask for money transfer for the lottery amount. They continue to exploit the victims until they are exhausted with money. Majority of these crimes go unreported because the victim is too embarrassed to admit to law enforcement that he is duped.

10. **Be Alert on Social media:** Be sure that Social networking profiles (e.g. Facebook, Twitter, YouTube, MSN, etc.) are always set to private settings. Check the security settings. Always be careful what data or information you post online on these sites.

11. **Mobiles devices should be secured with passwords:** Always activate the built-in security features of mobile to avoid any unauthorized access to personal data and information. Avoid storing passwords, pin numbers or address on mobile.

12. **Be aware while using public Wi-Fi Hotspots:** Although everyone wants to use free Wi-Fi one should avoid any financial transactions on these networks.

13. **Turn off your computer:** Whenever not in use the computers should be shutdown properly to prevent them from possible attack from cyber criminals.

IV CONCLUSION

Due to advancement in technology criminals have found new means of cheating and stealing money online on the Internet. So we have to be careful while doing financial transactions on the Internet. The preventive measures must be adopted to get secured from the cyber attackers.

REFERENCES

1. Y. Joshi and A. Singh, “A Study on Cyber Crime and Security Scenario in INDIA”, *Int. J. of Engineering and Management Research*, India, vol. 3, No. 3, pp. 13-18, June 2013.
2. B. Muthukumaran, “Cyber Crime Scenario In India”, Gemini Communication Ltd., Criminal Investigation Department Review, India, Tech. Rep., pp 17-23, 2008.
3. H. Singh and Geeta, “Cyber Crime – A Threat to Persons, Property, Government, and Societies”, *Int. J. of Adv. Research in Comp. Science and Software Engineering*, India, vol. 3, No. 5, pp. 997-1002, May 2013.
4. S. Yadav, T. Shree, and Y. Arora, “Cyber Crime and Security”, *Int. J. of Scientific & Engineering Research*, India, vol. 4, No. 8, pp. 855-861, Aug. 2013.
5. [Online]. Available: https://www.ennia.com/en/preventionshop/prevention-tips/cybercrime-prevention-tips/
6. [Online]. Available: https://in.norton.com/cybercrime-prevention