Review on various Cyber Crime, Hacker, and Authorities

Miss. Divya Sharma
Assistant Professor, Panjab University Swami Sarvanand Giri Regional Centre, Hoshairpur, India
Hoshairpur, India

Abstract
With the growth of the Internet and the number of users who are well acquainted to the Internet have also grown these user either use, misuse or try to damage (it can be update, modify, delete, etc) such information (here information is basically personal, private details or banking details of a user). These users can either have intentional or non intentional motive of doing so. This paper consist of a study of the various types of hacker, the various kinds of cyber crimes practices or faced now days and authorities that check and take measures to prevent any of these cyber crimes.

Keywords: Hacker, Phishing, Vishing, IP spoofing, Click Jacking.

1 INTRODUCTION
A crime in which computer is used can be called as a cyber crime. Cyber crime is a growing issue in today’s world where every single detail about an individual can be easily found on the Internet like our email, social networking site, shopping sites, marriage, jobs and even our family history of income are online such crime have increased. All these websites have become necessary and are important to everybody. In this age of Internet we are faced with many crimes done on the Internet such as hacking, which can be done by Script Kiddies” (i.e. children), Skilled crackers, Foreign nationals (well funded), Competitors or their agents these are all external attacker who have no real ton to the user of the information while internal attacks are done by Disgruntled employees (these are those people who have worked with the person or organization that is being attacked and bear a grunt against them due to there past experience), Contractors, vendors(these are those people who have sold you the software), etc. The attack done on a particular system are common now days and most of the time people who have hacked have no idea about it. Other than just losing valuable information such as account password for a particular bank account a hacker can also can also destroy information present on a system.

Due to the growth in internet technology we are all at the risk of losing our valuable information to attack such as hacking or cracking whether intentional or unintentional.

2. THREATS
Any natural disaster and attack due to which the secrecy and privacy of data present on a computer system is called a threat to the computer system.

There are two types of computer data threats:

2.1 Unintentional Threats: These threats are not caused by any individual or organization and cannot be prevented. Such threats are natural or accidental (like fire, etc). Types of unintentional threats are as follows:

2.1.1 Natural disaster: These threats cannot be predicted and are nature born such as floods, earthquake, volcano eruption, etc.

2.1.2 Software error or hardware malfunction: Software errors are caused by downloading software which consists of malware, Trojan horse, etc which can cause computer system to crash. Hardware malfunction is caused due to wear and tear of computer hardware over the time of use of the hardware.

2.2 Intentional Threats: These are those threats that have intentional motives of harming an organization or user just for the sheer means of fun or destroying or changing existing information about an organization or user. Intentional threats can be caused by one organization to another just to slow down the productivity or steal internal secret of a particular organization. These threats can be against organization to any group or individual who is regarded as an imminent threat by the organization or can be from user to user just to harness some revenge. Types of unintentional threats:

2.2.1 Active Threats: In such types of attacks data residing on computer system is altered.

2.2.2 Passive Threats: In these attacks the attacker tries to make use of the data stored on a computer system without altering it.

3 CYBER CRIMES
Crimes committed using the Internet are called cyber crimes. With the age of the Internet there has been an increase in number of cyber crimes.

3.1 Types of cyber crimes
The various types of cyber crime that occur now days are as mentioned below:

3.1.1 Phishing
In phishing an attacker tries to get private information from a user to commit frauds in future use. These attacks occur through email, fake websites which often look like the original website or fake websites which often redirected from the original website.

3.1.2 Internet scams
These scams often try to cheat their victim directly by using tricks rather than false promises.
3.1.3 Malware
These are illegal software which on being installed run another program in parallel to the original software which had been installed on a computer system they collect information such as email id, password, etc and transfer them to the creator of the software accordingly.

3.1.4 IP Spoofing
According to section 66A of IT act 2000 spoofing means sending offensive messages through communication medium which causes annoyance to somebody.

3.1.5 Privacy violation
In accordance to section 66E of IT ACT 2000 publishing or transmitting private areas of any person without his or her consent, etc, this is punishable to imprisonment of 3 years or 2 lakh rupees fine or both.

3.1.6 Cyber terrorism
In accordance to section 66F of IT ACT 2000 it intent to threaten the unity, integrity, security or sovrenity of a nation.

3.1.7 Child pornography
Depicting children engaging in sexual activity over the Internet is a crime. Whether these depiction are in the form of images, photographs or video.

3.1.8 Cyber stalking
It means intervening in somebody personal life so as to harass him or her and abuse online.

3.1.9 Cyber bulling
This includes sending threatening messages altering images and then using these images to create nuisance for others.

3.1.10 Cyber squatting
Cyber squatting is the practice of is registering, selling domain name which are authentic and selling them to those individuals for gaining profit or money from the buyer.

3.1.11 Spam email
These are junk email sent without the consent of the receiver creating lots of problems for the receiver who receiver these unwanted emails.

3.1.12 IRC related
Three main ways to attack IRC are: "verbal attacks, clone attacks, and flood attacks.

3.1.13 Money Laundering
Using Internet to convert money collected either through terrorist activities or other cyber crime into legitimate money.

3.1.14 Denial of service
Denial of service attack is a resistance used by hacker on banking websites and business, it also used in reference to CPU resource management. In this attack the computer resources of the user being attacked are flooded with requests so that it becomes busy while abstaining it from doing what it was intended to do. Here the network traffic is increased so that the speed of network is slowed down so as to make it unavailable to the user therefore no service of communication media is available. This is done so as stop the user or computer system from doing what it is intended to do on being attacked.

3.1.15 Computer vandalism
It is kind software or malware which destroys data present on computer or use it according to their needs or even makes them useless for any future use.

3.1.16 Click jacking
Here the user access a website may be tricked into clicking on to such links which they may perceive to be something else and sharing personal information on these links. Here the user is tricked into think that he or she may be clicking onto an original website while they might be on fake one.

3.1.17 Salami attack
Salami attack is also called penny shaving in this attack small amount of money is stolen from bank customer by taking advantages of the rounding or money to the nearest paisa. This type of attack is designed by the programmer of the banking website at the time of coding. Salami attack can even go undetected.

3.1.18 Key logger
This is used by organization to keep check on their employees and monitor their activities on the Internet. They can also be used as surveillance software by the organization where they monitor the websites an employee access. A keylogger records every stroke made on the keyboard by the employee and can even record every key pressed on the keyboard by the employee or employees.

3.1.19 E-mail Bombing
Email bombing is sending meaningless email to a specific email id so as to block or utilized all the resources of a particular email. These emails can appear to be from different email ids and can be totally unrelated.

3.1.20 E-mail Spamming
Here a single email message is sent too many email ids these emails are mostly junk mail and to some they may seem to be authentic while in actual they are not.

3.1.21 Cyber Defamation
Cyber defamation is defamation conducted on the Internet. This can be done intentional or unintentional. The targets
of cyber defamation can be website or user having an account on the Internet.

3.1.22 Web Jacking
This is a kind of phishing attack in which a user can be redirected to an unauthentic website which might seem authentic through the actual website by just clicking on the hyperlink specified on the original website.

3.1.23 Logic Bomb
A logic bomb is a malware inserted into the authentic software which is inserted into the program by a programmer at the time of coding. This bomb starts working when certain condition is met and steals secrets from a computer system or destroys data present on a computer system or database.

3.1.24 Data Diddling
It is the process in which cyber criminals change the data during the start of the program and after the program has completed or ended the data may seem unchanged or will be changed back to what it was at the start of processing of the program.

3.1.25 Vishing
It is the practice of using voice over IP to gain personal, private and financial information about any individual. In this type of crime information like credit card details are stolen by fake caller and later used for stealing money from user account.

3.1.26 Password Sniffers
It is a program that remembers your user name and password for a particular website as a user log in at a site. The sniffer can impersonate to be an authorized user and log in to access information which can be restricted documents.

3.2 Measure that can be taken to avoid such kinds of attacks:
Some measures must be taken by users while surfing the Internet and sharing personal or credit information with any third party on the Internet. Few of these measures are listed below:

3.2.1. Antivirus: User should install a good antivirus program on the system and update it accordingly to requirement.

3.2.2. Firewall: User should keep the firewall of the computer system on at all time.

3.2.3. Password protection: user should apply password on a computer system. The password should be strong and should not relate to people or date of birth. For protecting the password the password should be changed periodically. The user should not share password with anyone.

3.2.4. Not share personal information: user should not share their personal information such as credit card number, e-banking name, email id, password, etc. with any third party or website nor should a user respond to unknown emails. User should be aware of fraud websites and should not share important information related to banking details with any of these websites.

3.2.5. Review financial information regularly: user should regularly review his or her financial details so as to notice any changes or fraud.

3.2.6. Turn computer off: user should turn off the system because of high speed internet connectivity any hacker can hack into the system and change the details or modify the contents present on a system or steal personal details present on your computer system.

3.2.7. Buying recognized hardware and software or Software privacy: User should always buy authentic hardware and software so as to secure the computer system from unauthorized attacks. Any malware software Trojan horse or viruses if installed will prove harmful for your computer.

3.2.8. Not to share information over Voice calls: user should not share personal, private, and financial information over voice calls as a fake caller might be trying to lure you into sharing credit details, or information for the sake of identity theft.

3.2.9. Saving details for future analysis: a user should save details about the attack after it has occurred so that those details can be used as E-evidence for reporting against such crime to the police or appropriate authority.

3.2.10. Parental guidance: Parents should monitor their children who surf the internet. They should guide their children about the benefits and limitations of internet and educate them on cyber crime as well.

3.2.11. Fraud Emails: user should not respond to any fraud email claiming to provide free goods and services, lottery, etc.

3.2.12. Never arrange meetings with strangers: many people on chat with stranger over the internet and viewing their picture on their social networking sites arrange a meeting with strangers which is not healthy as many people online lie about their identity and their true intentions might be to hurt you. Making friends online can be harmful and parental guidance should be observed in such cases.

3.2.13. Don’t believe everything you read or see online: Information hosted on a website may be misleading as because of non trusted source. Many websites and email contain information which is misleading and can be plain lie. In many cases parental guidance should be asked.

3.2.14. Don’t post inappropriate content: user should not post inappropriate information on the internet as the internet has no boundaries and any information posted on the internet will stay there forever. As some user have a habit of might save pages so that they can view or read them later.

3.2.15. Don’t be bullied into fights: people may say bad things to you over the internet just so that you respond to it. Instead user should block such people and should discontinue any future communication.
4. Hacking or Cracking

Hacking or cracking is illegally gaining access to somebody’s personal or banking data or information stored by the user on their computer system.

4.1 Types of Hackers

The various kinds of hacker are as follows:

4.1.1 White hat

This type of hacker hacks a system just to check how strong or how weak a system is against actual attacks. These types of hacker are often called ethical hacker since they work to increase the security of a particular system. Such hackers are often hired by organization so as to test how strong their software or websites are under an actual attack.

4.1.2 Black hat hackers

These hackers hack a system just for the motive of destroying, stealing information, or modifying the already exiting contents for their own gain or for an organization.

4.1.3 Gray hat hackers

These hackers are a combination of white hat and black hat. These hackers hack a system or user account without their knowledge or permission just to tell them that there system is not secure or they are facing some security defect and may offer to correct them as well.

4.1.4 Elite hacker

Elite is used to describe the most skilled hacker and mostly are a group of hackers. They are a high level of hackers who have vast experience of hacking.

4.1.5 Script kiddies

This kind of hacker lack skills for hacking and used pre-designed tools designed by hacker to hack into somebody computer system. Script kiddies may use borrowed programs or tools available online so as to deface a website and make a name for them.

4.1.6 Neophyte

These hackers are new in hacking and have no experience about hacking.

4.1.7 Hacktivist

These hackers promote religion and work for a cause. This hacker uses computer and internet to promote politics or any specific religion.

4.1.8 Blue hat

These are hacker working within an organization who checks a system just before its launch to test how secure is the designed system against an actual attack.

4.1.9 State Sponsored Hackers

These hackers are hired by government or government agencies just to monitor any hacking being done against them or hack other country website in order to check for attacks.

4.1.10 Spy hackers

These kind of hackers may be working in an organization just for the means of stealing information about the organization so as to sell it to its competitors’. These kinds of hackers are hired by an organization to steal secret information about other organization.

4.2 Hacking

Hacking is without the permission of the authorized personal accessing the personnel information of an individual/organization and modifying it or removing it.

4.2.1 Website hacking: Here particular information hosted on a website can be modified, altered or rendered useless. Here hyper link leading to fake websites can be inserted on the original websites.

4.2.2 Email hacking: in such types of hacking an email id of a user will be hacked and important personal, banking information stored by the user on their e-mail is stolen by a hacker.

4.2.3 Network hacking: Here the speed of Internet of a particular user is slowed down or rendered useless by hacker either by over flooding the traffic on the network.

4.2.4 Password hacking: the credit detail of a user using services like net banking and credit card details of a user are stolen from a particular user either by click jacking or key logging.

4.2.5 Online banking hacking: hacker can create a fake website with proper website address by which a hacker can acquire password and details about a user who user that website.

4.2.6 Computer hacking: here information (like pictures, photographs, etc) saved on a computer system is stolen by a hacker. A hacker can also modify or alter information stored on a system according to their requirement.

5. Authority that keep checks on the cyber crimes

To keep check on cyber crime in India many acts have been formulated and added to IT ACT 2000 to keep a check on these crimes. The authorities that keep check against such crime and those that entertain complaints against cyber crime are mentioned below:

World intellectual property organization (WIPO) is a specialized united nation agency formed to protect intellectual property worldwide (Intellectual property such as trademarks, inventions, and copyrighted work).

Indian Computer Emergency Response Team (CERT-In): This agency determines threats such as hacking and phishing.

Cyber Appellate tribunal: Cyber Appellate tribunal or Cyber Regulations Appellate Tribunal (CRAT) was established by the Central Government in accordance with the provisions contained under Section 48(1) of the Information Technology Act, 2000.

Perry4Law it is the leading Techno-Legal Law Firm of India providing domain specific services on Corporate, IP and ICT matters such as Banking and Finance, Business Setup, Corporate and Commercial Advisory, Contract Management, Cyber Law, Cyber Forensics, Cyber Security, Digital Evidencing, Due Diligence, E-Commerce, E-Courts, E-Discovery, E-Governance, Electronic Services Delivery, Inbound-Outbound Investments, Intellectual Property Portfolio Management, Legal Enablement of ICT Systems in India, Mergers and Acquisitions, National E-Governance
Plan (NEGP), Online Dispute Resolution, Private Equity and Venture Capital, Resolution of Domain Disputes and Technology related disputes, and others. With the objective to spread Cyber Law Awareness and Cyber Security Awareness in India projects and policies like National Cyber Coordination Centre (NCCC) of India, National Critical Information Infrastructure Protection Centre (NCIPC) of India, Grid Security Expert System (GSES) of India, National Counter Terrorism Centre (NCTC) of India, Aadhaar Project of India, National Cyber Security Policy of India 2013 (NCSP 2013), Cyber Attacks Crisis Management Plan of India, Crisis Management Plan Of India For Cyber Attacks And Cyber Terrorism, Cyber Command For Armed Forces Of India, Tri Service Cyber Command for Armed Forces of India, Central Monitoring System (CMS) Project of India, National Intelligence Grid (Natgrid) Project of India, Internet Spy System Network And Traffic Analysis System (NETRA) of India, Crime and Criminal Tracking Network and Systems (CCTNS) Project of India, e-mail policy of India, etc were launched which are still in the initial stages.

For the convenience of common public a special department of police is available where report against cyber crimes can be registered and appropriate actions are taken accordingly. Few of these department are mentioned below: Special Task Force Office, CID, Cyber Crime West Bengal, Cyber Complaints Redressal Cell, Nodal Officer Cyber cell Agra, Cyber Crime Investigation Unit Police Station, Patna, Cyber Crime Police Station DSP Cyber Crime, S.A.S Nagar, Patiala, Punjab.

References

[2] Dr.B.Muthukumar “Cyber Crime Scenario In India”

AUTHOR
Miss. Divya Sharma received her M.Tech. Degree in Computer Science and Engineering from Rayat and Bahra Institute of Engineering and Technology in 2012 and B.Tech. Degree in Computer Science and Engineering from S.U.S.C.E.T. in 2009. From December 2012-till date, she is working as Assistant Professor at Panjab University Regional Center Hoshairpur in the Department of Information Technology.