CYBER CRIME AND CYBER LAWS IN INDIA

IQBAL SINGH

Assistant Professor, A.S.B.A.S.J.S. Memorial College, Bela, Ropar(Punjab).

Abstract

Internet is fastest emergent industry in modern world. People of all ages depend on Internet. Cyber crime refers to any criminal action on internet, like online frauds, thieving confidential information, harming other computers. Cyber laws control these criminals to evade the crimes. This Paper aims to introduce to the cyber crime from the streets to the networked super-highways of cyberspace unlike normal criminals.

Keywords: Hacking, Security, Threat, Vulnerability, Cybercrime, Cyber laws.

The introduction

Cyber crime is the use of internet to achieve illegal actions such as spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Over the past two decades or so, computers and the internet have become an essential part of everyday lives. Almost every aspect of life has become digital, be it bank transactions or product purchase. It is high on accessibility, and convenience. Unfortunately, this also makes it a hotspot for criminal activity. To stop these criminal activities, Government makes laws known as "cyber laws".

1. Cyber crime

Any illegal activity committed using a computer and/or the internet can be called a cyber crime. Furthermore, cyber crime also includes traditional crimes conducted through the Internet. New technology creates new avenues for crime.

2. The Effects of Cyber Crime

2.1. Cyber crime against people:

It includes a broad range of offenses. Online harassment or cyber bullying is a common occurrence on internet. Yet another type of unwanted engagement is cyber stalking –having every action online followed as and when it happens. In some of the more serious cases, the internet is used as a intermediate to trace

individuals, engage them in conversation, invite them over for a personal meeting and then once the perpetrators meet the victim commit serious crimes.

2.2. Cyber crime against property:

It basically involves the penetration of computers with malicious software through websites, emails or personal chats. These malware attacks could be just to destroy someone's computer or to steal information from them. These attacks deny the user access to his/her information while supplying the perpetrators with crucial details about the victim. Theft of bandwidth, that is gaining unauthorized contact to an internet connection, is also treated as a cyber crime.

2.3. Cyber crime against businesses:

These happen when the Criminals impersonate sites to get sensitive information hack into the systems of the companies. Most businesses store their sensitive information on servers. Hackers who can get access into the systems of these companies get access to all the information available in these files. Hackers can select to destroy or leak them, or where money is concerned transfer funds from an organization to someone else's account. The customers of that particular company lose faith in the organization such cases and thus, businesses can lose a significant number of customers based on incidents such as these.

2.4. Cyber crime against governments:

Cyber criminals can attack government organizations. The secure database of a government agency can be hacked with the intention to misuse sensitive information and the term "cyber-terrorism" is often used in this context. Basically, any individual or group gaining access to any sensitive information pertaining to the government and using it to cause disharmony, are cyber-terrorists.

3. Types of Cyber Crime

3.1. Hacking

Hacking is an act committed by person by accessing computer system and network without permission. Hackers are basically computer programmers, who have an advanced understanding of computers and misuse this knowledge for hacking the computer systems. They usually have expert-level skills in one particular software program or language. Hacking can be done in following ways:-

3.1.1. Vulnerability Scanning:

Every network or operating system will have some vulnerability. These vulnerabilities are crucial for a successful hack. There are a number of vulnerability scanners available to scan the host for known vulnerabilities. Some of such vulnerability scanners include:-

1. Shadow Security Scanner
2. Stealth HTTP Scanner
3. Nessus
4. Wireshark
5. Nessus Remote Security Scanner
6. NMAP
7. Nikto
8. SuperScan

3.1.2. SQL Injections:

SQL injection is a common attack that uses malicious SQL code for backend database exploitation to access information that was not intended to be displayed. This information may include any number of items, including sensitive company data, user lists or private customer details. An SQL injection is a technique that allows hackers to play upon the security vulnerabilities of the software that runs a web site. It can be used to attack any type of unprotected or improperly protected SQL database. This process involves entering portions of SQL code into a web form entry field – most commonly usernames and passwords – to give the hacker further access to the site backend, or to a particular user's account.

3.1.3. Cross-site scripting:

It is also known as XSS, is a very easy way of circumventing a security system. Cross-site scripting is a hard-to-find loophole in a web site, making it vulnerable to attack. In a typical XSS attack, the hacker infects a web page with a malicious client-side script or program. When user visits this web page, the script is automatically downloaded to browser and executed. Typically, attackers inject HTML, JavaScript, VBScript, ActiveX or Flash into a vulnerable application to deceive user and gather confidential information.

3.2. Virus Attacks

Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. Viruses disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether.

3.2.1. Types of Virus:-

3.2.1.1. Worms

"Worms" unlike viruses don't need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term "worm" is sometimes used to mean self-replicating "malware".

3.2.1.2. Trojan horses

"Trojan horses" are different from viruses in their manner of propagation. They masquerade as a legitimate flees, such as an email attachment from a supposed friend with a very believable name, and don't disseminate themselves. The user can also unknowingly install a Trojan-infected program via drive-by downloads when visiting a web site, playing online games or using internet-driven applications. A Trojan horse can cause damage similar to other viruses, such as steal information or hamper/disrupt the functioning of computer systems.

3.3. Logic bombs

A logic bomb, also known as "slag code", is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It's not a virus, although it usually behaves in a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met. Malicious software such as viruses and worms often contain logic bombs which are triggered at a specific payload or at a predefined time. The payload of a logic bomb is unknown to the user of the software, and the task that it executes unwanted. Program codes that are scheduled to execute at a particular time are known as "time-bombs".

3.4. Denial-of-service attack

A Denial-of-Service (DoS) attack is an explicit attempt by attackers to deny service to intended users of that service. It involves hooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload. This causes the resource to crash or slow down

significantly so that no one can access it. Using this technique, the attacker can render a web site inoperable by sending massive amounts of traffic to the targeted site. A site may temporarily malfunction or crash completely, in any case resulting in inability of the system to communicate adequately.

3.5. Phishing

This is a technique of extracting private information such as credit card numbers and username password combos by masquerading as a legitimate enterprise. Phishing is typically carried out by email spoofing. The malware would have installed itself on computer and stolen private information. Cyber-criminals use social engineering to trick users into downloading malware off the internet.

3.6. Web jacking

Web jacking derives its name from "hijacking". Here, the hackers have power over of a web site fraudulently. Hacker may change the content of the original site or even redirect the user to another fake alike looking page controlled by hacker. The owner of the web site has no more control and the attacker may use the web site for malicious function.

3.7. Data Diddling

Data Diddling is unauthorized changing of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track. In other words, the original information to be entered is changed, either by a person typing in the data, a virus that's programmed to change the data, the programmer of the database or application, or anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data.

3.8. Identity Theft and Credit Card fraud

Identity theft occurs when someone steals identity and pretends to be access resources such as credit cards, bank accounts and other benefits. The imposter may also use identity to commit other crimes. "Credit card fraud" is a wide ranging term for crimes involving identity theft where the criminal uses credit card to fund transactions. Credit card fraud is identity theft in its simplest form. The most common case of credit card fraud is pre-approved card falling into someone else's hands. It can be use to buy anything until report to the authorities and get card blocked.

3.9. Software Piracy

Thanks to the internet and torrents, Users can find almost any movie, software or song from any origin for free. Internet piracy is an integral part of lives which knowingly or unknowingly all contribute to. This way, the profits of the resource developers are being cut down. It's not just about using someone else's intellectual property illegally but also passing it on to people further reducing the revenue. Software piracy is the unauthorized use and distribution of computer software.

3.9.1. The following constitute software piracy:

1.Loading unlicensed computer code on pc

2. Victimization Single-licensed computer code on multiple computers

3.Using a key generator to bypass copy protection

4. Distributing a commissioned or unlicensed ("cracked") version of computer code over the Internet and offline.

4. Cyber laws

Cyber law or Internet law is a word that encapsulates the legal issues associated to use of the Internet. It is less a distinct field of law than intellectual assets or agreement law, as it is a field covering many areas of law and regulation. Cyber laws, same as any other branch of law, help define what is legal and illegal, and stipulate mechanisms to detect convict and punish offenders, and protect electronic property and its rightful use. Cyber laws pertain to diverse aspects of the electronic world such as:

1. Software licenses, copyright and fair use
2. Unauthorized access, data privacy and spamming
3. Export of hardware and software
4. Censorship
5. Computerized voting

4.1. Indian Cyber Crime Laws

In India, cyber laws are contained in the Information Technology Act, 2000 (IT Act) which came into force on October 17, 2000. The major principle of the Act is to provide legal identification to electronic business and to make possible filing of electronic records with the Government.

4.1.1. IT act, 2000

The IT Act, 2000 consists of 90 sections spread over 13 chapters [Sections 91, 92, 93 and 94 of the principal Act were omitted by the Information Technology (Amendment) Act 2008 and has 2 schedules.[Schedules III and IV were omitted by the Information Technology (Amendment) Act 2008].

4.1.2. Salient features of the Information Technology (Amendment) Act, 2008

1. The term 'digital signature' has been replaced with Page 2 of 9 'electronic signature' to make the Act more technology neutral.

2. A new section has been inserted to define 'communication device' to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text video, audio or image.

3. A new section has been added to define cyber cafe as any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.

4. New Section to address data protection and privacy –Section 43

5. Body corporate to implement best security practices-Sections 43A &72A

Table 1. Penalties and Offences

Cyber Crime	**Brief Description**	**Relevant Section in IT Act**	**Punishments**
Cyber Stalking	Stealthily following a person, tracking his internet chats.	43, 65, 66	3 years, or with fine up to 2 lakh

Cyber Pornography including child pornography	Publishing Obscene in Electronic Form involving children	67, 67 (2)	10 years and with fine may extends to 10 lakh
Intellectual Property Crimes	Source Code Tampering, piracy, copyright infringement etc.	65	3 years, or with fine up to 2 lakh
Cyber Terrorism	Protection against cyber terrorism	69	Imprisonment for a term, may extend to 7 years
Cyber Hacking	Destruction, deletion, alteration, etc in a computer resources	66	3 years, or with fine up to 2 lakh
Phishing	Bank Financial Frauds in Electronic Banking	43, 65, 66	3 years, or with fine up to 2 lakh
Privacy	Unauthorized access to computer	43, 66, 67, 69, 72	2 years, or with fine upto 1 lakh

5. How to Stay Safe on the Internet

5.1. Parental Guidance

A lot of cybercrimes revolve around unsuspecting teenagers and school children. Parents play a vital role in ensuring that children are safe on the internet and not vulnerable to hackers and identity theft. To start with, treat confidential information as confidential. Never reveal such sensitive data on the internet. It is always better to have a strong firewall installed in computer, especially armed with parental controls.

5.2. Be careful of Internet use

Always be careful each time using the internet. Never write down passwords. This rule also applies to other sensitive information – like social security number or credit card information. First step – keep computer updated. Switch off auto updates as most cybercriminals use such flaws in computer systems to attack machine while safely remaining anonymous. Choose passwords that are strong and protect it. Username, passwords and personal identification numbers (PIN) are quintessential for each and every online transaction.

5.3. Phishing

One of the most common forms of cybercrime, phishing is where criminals mail counterfeit email to the user, pretending to be a bank or a credit card merchant. Phishing is on the rise and is perhaps the largest form of identity theft in the internet. Luckily, the banks are now aware and are sending emails to customers, warn about phishing attacks and creating awareness among the general public. Keep away from websites which are suspicious and be careful with emails from any company requesting for personal or financial information. On a similar vein, don't ever click a link in a mail, even if mildest suspicion of the sites authenticity. Similarly, type out the URL of bank rather than clicking links. Check if the website is secure. Easy way to do this is by looking out for the padlock sign on the browser's toolbar. This means that the site is secure.

5.4. Secure Credit Cards

Credit cards are major sources of cybercrime and can be easily tampered. A stolen credit card can mean the end of the world. So, it is important that treat credit card as carefully as cash. Keep card details, like the card number and CVV confidential. While swiping card at stores, wait till the transaction has been completed. Check if the card returned that had given and has not been tampered with in any way. This way, such sensitive information won't get into the wrong hands.

5.5. Secure communication

Today is an era of supersonic communication. The mail is a place where millions of personal information is handled every day and is the commonest route to identity theft. Pay attention to email, especially the billing statements. Ensure that these statements are on time or better; opt for a paper-less statement through email id. It reduces the risk to cybercrime. Many identity thieves use complicated software to break into computer and elicit sensitive data like passwords. Most cybercriminals use spyware and other stealth mechanisms to steal data. The only way to fight this is by installing a strong firewall in computer.

5.6. Social media safety

While using public computers, never check the "Save Password" box. Many social media forums auto check this box – so keep eyes peeled for such possibilities. Signing up for social media could be done with full name. It prevents others from impersonating on the internet. The new scams on social media are done by emails that are similar to that of the social media provider. While getting such mails, assume the opposite – that it is a hoax. Social media is a double edged sword and has to be used carefully. Never give out travel plans on social media forums. This is the point where cybercriminals translate into real time threat. Most applications now have sign in options with social media. Never do that. This is just a great way to get access to personal information. Else, read the terms and conditions carefully before sign up.

Conclusion

While the internet is a wonderful device and has become an imperceptible part of lives, there's a lot out there that could cause serious trouble. The flip side is cybercrime and sadly, it is on the rise. The best thing to do is to be prepared. Follow these simple rules. Use common sense and act smart. Think before act and while conducting any online transactions, keep a wary eye. Being aware can help stay away from cybercrime.

References

1. https://www.tutorialspoint.com/information_security_cyber_law/introduction.htm

2.https://www.slideshare.net/bharadwajchetan/anintroduction-to-cyber-law-it-act-2000-india

3. https://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5-0374.pdf

4.http://searchsecurity.techtarget.com/definition/emailspoofing

5.http://www.helplinelaw.com/employment-criminaland-labour/CDII/cyber-defamation-in-india.html

6. http://ccasociety.com/what-is-irc-crime/

7.http://www.lawyersclubindia.com/articles/Classification-Of-CyberCrimes--1484.asp

8. http://catindia.gov.in/Default.aspx -Cyber Appellate Tribunal

9.http://www.cert-in.org.in/ -Indian Computer Emergency Response Team

10.http://cca.gov.in/rw/pages/index.en.do -Controller of Certifying Authorities

11.http://deity.gov.in/content/cyber-laws

12.http://www.cyberlawsindia.net/