International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

Cyber Security - Importance, Effects and Prevention

Shivali Gautam

Student, Master of Computer Applications, ABES Engineering College

Abstract: ***Cyber law is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues. Digitalization and networking provide number of benefits to us in different fields like e-commerce, banking, communication but due to cybercrime, a new criminal methodology also arises. To stop these cybercrimes, proper knowledge and awareness of cyber laws is necessary among people. The objective of this paper is to aware people with cybercrimes, cyber security, Cyber Laws in India and the Precautions which we take to secure our self from these cybercrimes.***

Keywords: Cyber law, Cyber space, Cybercrimes, Cyber Security

1. Introduction

The entry of computer in human life have made it easier to human to use it for various purposes even the small to large organizations rely on computers and online services for their work, transactions and documentation.

Now a days, computers are used all over the world and as we all know each and everything have its pros and cons. The major problem arises with technology and computer is Cybercrimes. Cybercrimes include data interpretation, phishing etc. To control these cybercrimes various Cyber Laws are being introduced to safeguard the organization from being prey of these cybercrimes. Cyber laws are the laws that regulates the cyber space.

Cyber security is now a trending field work to control cybercrimes by implementation some cyber laws which provides facilities like digital signature, data encryptions. The world 1st computer specific law was enacted in the year 1970 by the German State of Hesse in the form of 'Data Protection Act, 1970' with the advancement of cyber technology. Since then cyber laws are used to govern every online activity in India and in the World. In Indian "**INFORMATION TECHNOLOGY ACT, 2000**" was passed by the parliament on 17th October to have its exhaustive law to deal with the technology in the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cybercrimes.

2. Literature Review

1) Animesh Sarmah [1], in his research paper on A Brief Study on Cyber Crimes and Cyber Laws of India described about cybercrimes and cyber laws along with the evolution and classification of cybercrimes. He also gives a brief description about different sections to govern cybercrimes that comes under cyber laws.
2) G. Nikhita Reddy [2] describes about the challenges to cyber security and its emerging trends on latest technologies. She also provides a vast classification of trends with their importance.
3) Santosh Kumar Maurya [3] in his research paper describes about cyber security issues and challenges with a brief description of E- commerce and its tools. He also gives some of the recommendations to control cybercrimes.
4) Deepa T. P. [5] gives the reasons of increase in cybercrimes in India along with methods to avoid cybercrimes in India.
5) R. M. Kamble [6] describes the various cyber laws and information technology trends along with various IT acts to prevent cybercrimes.
6) Jigar Shah [7] suggests some methods to aware the youth of the country with cybercrimes and also highlights the importance of awareness about cyber laws for Indian youth and for the society. He also gives some methodology and suggestions to spread awareness regarding cyber laws.

3. Cyber Laws and Cybercrime

3.1 Cyberlaw

Cyber Law is the world of law that deals with the Internet's relationship to technological and electronic components, together with computers, software, hardware and knowledge systems (IS). Cyberlaw is additionally familiar as Cyber Law or Internet Law. Cyber law is vital as a result of it touches the majority aspects of transactions and activities and on involving the web, World Wide internet and Net. each action and reaction in Net have some legal and cyber legal angles.

3.2 Cyber Crime

Any offence or crime during which a pc is employed could be a law-breaking. curiously even a petty offence like stealing or pick-pocket is brought at intervals the broader ambit of law-breaking if the fundamental information or aid to such associate offence could be a pc or associate data hold on in a very pc used (or misused) by the fraudster. The I.T. Act defines a pc, network, data, data and every one alternative necessary ingredient that kind a part of a law-breaking, regarding that we'll currently be discussing thoroughly. in a very law-breaking, pc or the info itself the target or the thing of offence or a tool in committing another offence, providing the required inputs for that offence. All such acts of crime can come back beneath the broader definition of law-breaking.

4. Cyber Laws in India

Cybercrimes is essentially divided into three major classes being Cybercrimes against persons, property and Government.

4.1 Cybercrimes against Persons

Cybercrimes committed against persons embody numerous crimes like transmission of child-pornography, harassment of anybody with the utilization of a pc like e-mail, and cyber-stalking. The trafficking, distribution, posting, and dissemination of obscene material together with smut, infraction, and kiddie porn, constitutes one amongst the foremost necessary Cybercrimes familiar these days. The potential damage of such a criminal offense to humanity will hardly be overdone. this is often one law-breaking that threatens to undermine the expansion of the younger generation as additionally leave irreparable scars and injury on the younger generation, if not controlled.

4.2 Cybercrimes against Property

The second class of Cybercrimes is that of Cybercrimes against all types of property. These crimes embody unauthorized pc invasive through Net, pc destruction, transmission of harmful programs, and unauthorized possession of processed data.

4.3 Cybercrimes against Government

The third class of Cybercrimes relate to Cybercrimes against Government. Cyber act of terrorism is one distinct quite crime during this class. the expansion of net has shown that the medium of Net is getting used by people and teams to threaten the international governments as additionally to terrorise the voters of a rustic. This crime manifests itself into act of terrorism once a personal &"cracks&" into a government or military maintained web site.

5. Sections of Cyber Laws in India

To regulate such activities that violate the rights of an online user, the Indian government has the data Technology Act, 2000, in place. Here square measure a number of its sections that empower net users and conceive to safeguard the Net.

5.1 Section 65 – Meddling with pc supply Documents

A person United Nations agency on purpose conceals, destroys or alters any pc ASCII text file (such as programmes, pc commands, style and layout), once it's needed to be maintained by law commits associate offence and may be penalized with three years' imprisonment or a fine of two lakhs.

5.2 Section 66 - Victimisation word of another person

If an individual fraudulently uses the word, digital signature or alternative distinctive identification of another person, he/she will face imprisonment up to three years or/and a fine of one hundred thousand Bureau of Intelligence and Research.

5.3 Section 66D - Cheating victimisation pc resource

If an individual cheats somebody employing a pc resource or a communication device, he/she may face imprisonment up to three years or/and fine up to one hundred thousand Bureau of Intelligence and Research

5.4 Section 66E - Business enterprise non-public pictures of Others

If an individual captures, transmits or publishes pictures of a person's sex organ while not his/her consent or data, the person is entitled to imprisonment up to three years of fine up to a pair of Lakhs Bureau of Intelligence and Research or each

5.5 Section 66F - Acts of cyber act of terrorism

A person will face imprisonment if he/she denies a certified person the access to resource or tries to penetrate/access a computer resource while not authorization, with associate aim to threaten the unity, integrity, security or sovereignty of the state. this is often a non-bailable offence.

5.6 Section 67 - Business enterprise kid porno or predating youngsters on-line

If an individual captures, publishes or transmits pictures of a toddler in a very sexually express act or induces anyone beneath the age of eighteen into a sexual act, then the person will face imprisonment up to seven years or fine up to ten lakhs.

5.7 Section 69 - Govt.'s Power to dam websites

If the govt feel it necessary within the interest of sovereignty and integrity of India, it will intercept, monitor or rewrite any data generated, transmitted, received or hold on in any pc resource. The ability is subject to compliance of procedure. Beneath section 69A, the central government may also block any data from public access.

5.8 Section 43A - Information protection at company level

If a body company is negligent in implementing cheap security practices that causes wrongful loss or gain to anyone, such body company shall be susceptible to pay damages to the love person.

6. Why will we ought to Fight with Cyber Crimes

We all should keep in mind that computer network may be a common heritage of ours that we've hereditary in our life time from the advantages of ever-growing technologies. This computer network is that the lifeline of the complete universe and given its irreversible position nowadays, it's the duty of each netizen to contribute toward creating the aforesaid computer network freed from any bother or law-breaking.

7. Precautions to be taken from cyber crimes

7.1 Use a full-service net security suite

For instance, Norton Security provides period of time protection against existing and rising malware as well as ransomware and viruses, and helps defend your non-public and money data after you log on.

7.2 Use sturdy passwords

Don't repeat your passwords on completely different sites, and alter your passwords frequently. create them complicated. meaning employing a combination of a minimum of ten letters, numbers, and symbols. A password management application can assist you to stay your passwords latched down.

7.3Keep your code updated

This is particularly vital along with your operative systems and net security code. Cybercriminals oft use noted exploits, or flaws, in your code to achieve access to your system. fixture those exploits and flaws will create it less probably that you'll become a law-breaking target.

7.4 Manage your social media settings

Keep your personal and personal data latched down. Social engineering cybercriminals will typically get your personal data with simply many knowledge points, that the less you share in public, the better. as an example, if you post your pet's name or reveal your mother's surname, you may expose the answers to 2 common security queries.

7.5 Strengthen your home network

It's an honest plan to start out with a powerful coding watchword also as a virtual non-public network. A VPN can encode all traffic exploit your devices till it arrives at its destination. If cybercriminals do manage to hack your communication line, they won't intercept something however encrypted knowledge. It's an honest plan to use a VPN whenever you a public Wi-Fi network, whether or not it's in a very library, café, hotel, or airport.

7.6 Talk over with your youngsters regarding the web

You can teach your youngsters regarding acceptable use of the web while not move down communication channels. confirm they understand that they'll return to you if they're experiencing any quite on-line harassment, stalking, or bullying.

7.7 Maintain thus far on major security breaches

If you are doing business with a businessperson or have Associate in Nursing account on a web site that's been wedged by a security breach, decide what data the hackers accessed and alter your watchword forthwith.

7.8 Take measures to assist defend yourself against fraud

Identity theft happens once somebody legally obtains your personal knowledge in a very method that involves fraud or deception, generally for economic gain. How? you may be tricked into giving personal data over the web, as an example, or a outlaw may steal your mail to access account data. That's why it's vital to protect your personal knowledge. A VPN may also facilitate to shield the info you send and receive on-line, particularly once accessing the web on public Wi-Fi.

7.9 Understand that fraud will happen anyplace

It's sensible to grasp the way to defend your identity even once travelling. There square measure plenty of belongings you will do to assist keep criminals from obtaining your non-public data on the road. These embody keeping your travel plans off social media and being employing a VPN once accessing the web over your hotel's Wi-Fi network.

7.10 Keep a watch on the youngsters

Just like you'll wish to speak to your youngsters regarding the web, you'll additionally wish to help defend them against fraud. Identity thieves typically target youngsters as a result of their Social Security variety and credit histories oft represent a tabula rasa. you'll be able to facilitate guard against fraud by being careful once sharing your child's personal data. It's additionally sensible to grasp what to seem for that may recommend your child's identity has been compromised.

7.11 Understand what to try and do if you become a victim

If you suspect that you've become a victim of a law-breaking, you would like to alert the native police and, in some cases, the FBI and the Federal Trade Commission. this is often vital although the crime appears minor. Your report could assist authorities within their investigations or could facilitate to thwart criminals from taking advantage of others in the future. If you think that cybercriminals have purloined your identity. These square measure among the steps you must contemplate.

7.11.1 Contact the businesses and banks wherever you recognize fraud occurred.

7.11.2 Place fraud alerts and find your credit reports.

7.11.3 Report fraud to the FTC.

8. Conclusion

Data security in the Indian power sector is largely seen as restricted to protection of customer's financial data. This needs to expand to protection of consumption records and mandatory disclosure of data loss and implementing punitive measures for data loss. To prevent any data loss cyber laws are to implemented strictly and every individual and organizations is to be made aware about cybercrimes and cyber laws in India.

References

[1] Animesh Sarmah, A brief study on Cyber Crime and Cyber Law's of India, International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 06
[2] Deepa.T.P., Survey on need for Cyber Security in India
[3] Manmohan Chaturvedi, Cyber Security Infrastructure in India: A Study,Article · January 2009
[4] R. M. Kamble CYBER LAW AND INFORMATION TECHNOLOGY, International Journal of Scientific & Engineering Research, Volume 4, Issue 5,
[5] Jigar Shah, A Study of Awareness About Cyber Laws for Indian Youth, International Journal of Trend in Scientific Research and Development, Volume 1(1)
[6] https://www.infosecawareness.in/cyber-laws-of-india
[7] http://www.cyberlawsindia.net/cyber-india.html
[8] https://en.wikipedia.org/wiki/Information_Technology_Act,_2000
[9] DOT (2008), Retrieved August, 2008 from http://www.dot.gov.in

Author Profile

Shivali Gautam completed graduation in Bachelors of Computer Applications from MDU, Faridabad in 2016 and now pursuing post-graduation in Masters of Computer Applications form ABES Engineering College, Ghaziabad.