CYBER CRIMES IN SOCIAL NETWORKING WEBSITES

Ms.REENA RAVEENDRAN, Research Scholar, Kerala University

Dr.D.MUHAMMAD NOORUL MUBARAK, Asst.Professor,

Dept.of Computer Science, Kerala University

Abstract: *The development in rising internet era and its extensive spread information finally ends up in safety trouble and cyber-crimes. Social Networking websites are used as a manner of conversation for interaction among humans the world over, although it have numerous advantages love it facilitates in connecting human being's lives, buy products, percentage information and so forth., however unluckily numerous threats also accompany those endless benefits. Although it seems that social media has got the sector closer, there's a flipside to it. Many offenders use it as a susceptible way to dedicate offences like identity theft, cyber terrorism, sending offensive messages and so forth. And many of us fall into such trap due to lack of awareness or overuse of social networking websites. The cause of paper is to offer glimpse of ways increase of Social Networking websites gives extra scope for cyber criminals to perform their unlawful activities and the cases regarding the cyber offences occurring on theses social networking web sites, which have were given the eye of public. The paper additionally covers the legal guidelines enacted beneath specific statues to modify cyber-crimes.*

Index phrases— *Internet, cyber criminals, cyber crimes, Social Media, Awareness, Cyber Laws*

I. INTRODUCTION

The extensive use of web offers platform to cyber criminals. Social media is a collection of web sites and programs constructed on concept of improving networking and sharing of facts on-line. The famous social media programs are fb, Whatsapp, twitter, Skype, Instagram, YouTube, and many others. In beyond few years social media has won popularity within the society. Regardless of the numerous benefits that social media presents globally, people want to be made aware of the threats accompany with social media. Unluckily, Social media has end up the five platforms for cyber criminals to hold their grimy activities. Cyber Criminals are people who perform criminal hobby through the laptop networks violating the rules and guidelines and legal guidelines that's known as cyber-crime. The common instance of cyber-crimes is robbery, damage, software piracy and so on. Cyber criminals encourage social media users to publish their private details like age, gender, address, telephone number, and many others. Social media offers platform to the cyber criminals to control non-public records and use that to dedicate crimes.

II. SOCIAL MEDIA

Social network is a committed website or software that allows customers to talk with each other with the aid of posting information, feedback, messages, photos and many others. Three social media is computer primarily based technology that allows the sharing of ideas, mind, and information via the constructing of digital networked and communities. Social media originated because the way to transport with friends and own family but became later followed through organizations that wished to attain out to clients via a famous new conversation approach. according to Forbes, there are approximately 1 billion social media accounts all over the global, these accounts makes almost all the nations of the world linked with every other. Social media is a completely commonplace in nowadays current international, social media is considered to be one of humanity's best achievements and accomplishments.[4]

III. CYBER-CRIMES

Cyber-crime is a risky crime related to computer systems or digital devices, for the duration of which a computer is both a goal of the crime, a tool of the crime or comprises evidence of the crime. Cyber-crime has grown to be one of the most complicated international problems within the criminal framework. Cyber-crime commonly outlines any criminal activity that occurs over net. . There are numerous examples consisting of fraud, malware together with viruses, identity theft and cyber stalking. Cyber-crimes are widely categorized into 3 companies which include crime against: five

- INDIVIDUAL: This sort of cyber-crime may be within the form of cyber stalking, distributing, trafficking and "grooming".
- PROPERTY: This kind of cyber-crime consists of stealing a person's bank information and drains off cash; misuse the credit card to create frequent purchases on-line; run a rip-off to induce naive people to provide their difficult-earned cash; use malicious package deal to comprehend access to an organization's web website or disrupt the structures of the organization. The malicious package can also harm software and hardware, a piece like vandals damage assets in the offline world.

GOVERNMENT: Crimes against government consists of cyber terrorism. If criminals are a success, it is able to purpose devastation and panic amongst the citizen. If criminals are a success, it can cause devastation and panic amongst the citizen. On this elegance, criminals hack authorities' web sites, military web sites or circulate propaganda.

IV. CRIMES ON SOCIAL MEDIA

- **Hacking**

Hacking usually refers to unauthorized intrusion right into a computer or a network. Cyber criminal use absolutely different assault strategies to induce access to focused customers' virtual devices. Cyber criminals send electronic mail or messages to the social media consumer's when customers click on thereon hyperlink get hacked by means of criminals. Hacking also can consult with non-malicious activities, generally concerning uncommon or improvised changes to device or strategies.

➢ Identity theft

Identification theft is a critical crime that has unfavorable and comprehensive impact for its victims. On-line identification theft is the maximum common cyber-crime. Identification theft is dedicated to steal any individual's identity without user's permission to steal cash or to dedicate fraud. Identity thieves more and more use technology to get humans' non-public records for identity fraud. The cyber criminals use social media to accumulate focused customers statistics. Criminals use stolen information to commit unlawful activities.

➢ Phishing

It is widely known that email messages, texts and phone calls are strategies generally employed via criminals to people with the aim of committing cash or identity fraud. Social media phishing attack is a preliminary desire amongst cyber criminals. Phishing is a common chance on the social media during which the offender creates and controls fake websites that looks the actual ones to trap sufferers to show the non-public records. Usually, customers get hold of links on social networking web sites and after they tap on that hyperlink perpetrator collect all of the users' information.

➢ Cyber bullying and Cyber Stalking

Some of the common threats associated with social networking web sites are cyber bullying and cyber stalking. Cyber bullying is using technology like internet, emails, and social networking web sites to annoy, threaten, embarrass, or target a character. Cyber bullying or any kind of bullying is towards regulation. It can have terrible outcomes. Cyber Stalking has been outlined as a person who follows or contacts a woman, despite the clean indication of disinterest through the woman or monitoring the usage of internet or electronic verbal exchange of lady. Each of those crimes has legal effects and conjointly includes imprisonment.

➢ Posting videos of criminal activity

As Smartphone and social media technology preserve improve hand in hand, a variety of and more criminals are posting videos in their crimes on social media. Whereas this sounds particularly atrocious, it very is in reality quick-sighted as a variety of and extra police departments and prosecutors are capable of rely on these films to arrest and convict those criminals.

V. CASE LAWS

I. Google India private ltd. v. Visaka Industries limited

Visaka industry ltd, a production materials enterprise filed a case towards Google India for criminal conspiracy, and publishing fake defamatory content approximately the company in 2011 alleging that a blogger named Gopal Krishna used Google's Blogspot.com to unfold the content material which stated that, the organization had reference to congress celebration and consequently the enterprise could manufacture asbestos. The A.P excessive court held Google India to be dependable and consequently it filed the attraction in S.C which remains pending.

II. Suhas Katti v. Tamil Nadu10

It becomes the first case in India wherein a conviction becomes handed down in reference to the posting of obscene messages on the internet under the controversial section 67 of IT Act, 2000. Within the case, a woman complained to the police about a man who became sending her obscene messages in a Yahoo message organization. The accused also forwarded the emails obtained in a fake account opened by him inside the sufferer's name. The victim also received cell phone calls by means of human beings who assumed she turned into a prostitute.

III. Janhit Manch & Ors. v. UOI[11]

The petition sought a blanket ban on pornographic websites. The NGO had argued that web sites showing sexually explicit content had a negative influence, main young people on a delinquent course.

IV. JNU MMS SCANDAL case,

In this instance a pornographic MMS clip become apparently made inside the campus and transmitted outside the college. The 2 scholar to begin with attempted to extort money from the lady within the video but when failed the culprits placed the video out on mobile telephones, net, social networking web sites. They have been punished below sec 66E of IT Act, 2000.

VI. DIFFERENT LEGAL ACTS AGAINST CYBER CRIME

It is the duty of the government to ensure that its laws cope with the development of science and technology, and fully participate in the legislative enactment

- The India Information Technology Act of 2000.
- The Philippines Electronic Commerce Act No 8792 of 2000
- The Philippines Cybercrime Prevention Act of 2012 No. 10175
- USA Cyber Intelligence Sharing and Protection Act of 2011 (CISPA).

- USA Cyber Security Enhancement Act of 2009 (S.773).

VII. USE OF SOCIAL MEDIA AND CYBER CRIME AND THE REGULATION IN INDIA:

Each sixth cybercrime in India is committed through social media, Alok Mittal, the chief of the national investigation agency (NIA) has said. As we recognize that India has enacted the first I.T.Act, 2000 based totally on the UNCIRAL version advocated by using the overall meeting of the United Nations. bankruptcy XI of this Act offers with offences/crimes alongside certain other provisions scattered on this Acts .The various offences which are provided underneath this chapter are shown within the following table: -

OFFENCE	**SECTION UNDER I.T. ACT**
Tampering with Computer source documents	Sec,65
Hacking with Computer systems, Data alteration	Sec.66
Publishing obscene information	Sec.67
Un-authorized access to protected system	Sec.70
Breach of Confidentiality and Privacy	Sec.72
Publishing false digital signature certificates	Sec.73

V. COMPUTER RELATED CRIMES COVERED UNDER IPC AND SPECIAL LAWS

OFFENCE	**SECTION**
Sending threatening messages by email	Sec. 503 IPC
Sending defamatory messages by email	Sec.499 IPC
Forgery of electronic records	Sec.463 IPC
Bogus websites, cyber frauds	Sec.420 IPC
Email spoofing	Sec.463 IPC
Web-Jacking	Sec.383 IPC
E-Mail Abuse	Sec.500 IPC
Online sale of Drugs	NDPS Act
Online sale of Arms	Arms Act

VI. CONCLUSION

The internet may be very effective tool and powerful means of communication but it is susceptible similar to something else. Internet has been a boon and curse for absolutely everyone. On one hand the whole lot has turn out to be so clean and handy, and however this has made cyber offenders to take advantage of the scenario. Cyber criminals are greater interested in social because of the outrageous sort of customers and lack of understanding amongst many people using social networking web sites. We are able to reduce the threat of cyber-assault or cyber-crime via getting a little conscious and conscious while using social media systems. It is viable to make sure the safety of your private information of these social media systems with a totally minimal effort. Do now not percentage your password with any of your friends or colleagues or even on any on-line shape. It's also counseled fending off proportion information about your debit or credit card over these social media networks which will avoid credit/debit card fraud, as nicely.

BIBLIOGRAPHY

[1]. W.Ghari and M. Shaabi"Cyber Threats in Social Networking Websites," International Journal of Distributed and Parallel Systems, 2012.

[2]. R. Jabee and M. Afshar, "Issues and Challenges of Cyber Security for Social Networking Sites (Facebook)," International Journal of Computer Applications, 2016.

[3]. V. L. Yisa, O. Osho, and I. Soje, "Online Social Networks: A Survey of Usage and Risks Experience among University Students in North-Central Nigeria," International Conference on Information and Communication Technology and Its Applications, 2016.

[4]. A. Singh, D. Bansal, and S. Sofat, "Privacy Preserving Techniques in Social Networks Data Publishing - A Review," International Journal of Computer Applications, 2014.

[5]. M. Fire, R. Goldschmidt, and Y. Elovici, "Online Social Networks: Threats and Solutions," IEEE Communications Surveys & Tutorials, 2014.

[6]. Y. Najaflou, B. Jedari, F. Xia, L. T. Yang and M. S. Obaidat, "Safety Challenges and Solutions in Mobile Social Networks," inIEEE Systems Journal, 2015.

[7]. D. Hiatt and Y. B., "Role of Security in Social Networking," International Journal of Advanced Computer Science and Applications, 2016.

[8]. L. Dehigaspege, U. Hamy, H. Shehan and D. Dhammearatchi, "Secure Authentication: Defending Social Networks from Cyber Attacks Using Voice Recognition," International Journal of Scientific and Research Publications, 2016.

[9]. M. Prasanthi, "Cyber Crime: Prevention & Detection," International Journal of Advanced Research in Computer and Communication Engineering, 2015.

[10]. R. Chouhan, "Cyber Crime: A Changing Threat Scenario in the State Of Art," International Journal of Engineering Research and General Science, 2015.

[11]. A. Kumar, S. Kumar Gupta, S. Sinha and A. Kumar Rai, "Social Networking Sites and Their Security Issues," International Journal of Scientific and Research Publications, 2013.

[12]. S. D. Trivedi, M. Chandani, M. Tosal and T. Pandya, "ANALYTICAL STUDY OF CYBER THREATS IN SOCIAL NETWORKING," International Conference on Computer Science Networks and Information Technology, 2016.

[13]. R. Chandramouli, "Emerging social media threats: Technology and policy perspectives,"2011 Second Worldwide Cybersecurity Summit (WCS), London, 2011

[14]. A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," Procedia Economics and Finance, 2015.

[15]. M. Carter, "Third Party Observers Witnessing Cyber Bullying on Social Media Sites," Procedia - Social and Behavioral Sciences, 2013.

WEBLIOGRAPHY

[1] http://en.wikipedia.org/ wiki/Security

[2] http://en.wikipedia.org/wiki/Data_ security

[3] http://en.wikipedia.org/wiki/Information_security

[4] http://en.wikipedia.org/wiki/Computer_ security

[5] http://www.cyberlawclinic.org/casestudy. Asp

[6] http://www.cyberlawsindia. Net/cases.html