*Monthly Multidisciplinary
Research Journal*

Review Of

Research Journal

Chief Editors

Ashok Yakkaldevi
A R Burla College, India

Flávio de São Pedro Filho
Federal University of Rondonia, Brazil

Ecaterina Patrascu
Spiru Haret University, Bucharest

Kamani Perera
Regional Centre For Strategic Studies,
Sri Lanka

Review Of Research

A RESEARCH STUDY ON CYBER CRIME IN THE SOCIAL MEDIA :CHALLENGES AND SOLUTIONS

S. S. Solanke[1] , G. K. Chalindrawar[2] and Patange V. N.[3]
[1]Department of commerce , Sunderrao Solanke Mahavidyalaya majalgaon , Maharashtra.
[2]Department of commerce , Sunderrao Solanke Mahavidyalaya majalgaon , Maharashtra.
[3]Assit.Prof. ,Department of computer science , Sunderrao Solanke Mahavidyalaya majalgaon , Maharashtra.

ABSTRACT

In the old age of the world, peoples has using some code to share language ,after some time humans life style has been changed forever and forever & to use some particular language for the communication. They have used some language for exchanging message to each other. As per changed the life style and country chin has invented the paper and hand written text has became in front of the world. The knowledge has improved between all the areas .Literature of Greek has been popular and except religion the knowledge has becoming more and more powerful so the technology and science has became in front of world. This knowledge has used to improve in the radio, television education. Due to Internet knowledge of word has getting instantly on one click. The difficult work done has become too easy by using the smart devices and smart phones. An attractive data plan, cheap electronic devices has advantages that all having to use it , spreads it and becoming a popular. The user of social media has been grown and grows day to day rapidly due to such type of reasons. All peoples used laptop, notepad instead of notebook, diary for their storage purpose and used the face book, Twitter, what's app for transferring the messages in the groups. The peoples having online friends, so face to face discussion have now in history. This paper describes the facts for using social media and its crime occurred using the social media.

KEYWORDS:Face book, Cyber crime, Twitter, What's App, Smart phone etc.

.

1.INTRODUCTION:

Social media, a concept that has given people a common platform for sharing their news, views and opinions regarding the happenings around them. Not only this, social media is also being used by the advertisers and companies for their promotions, professionals for searching and recruiting,

students for internships, parents and educators as social learning tools, etc Internet is a very essential part of life from shopping to electronic mails and education, internet is very important. It is a very large community which is using internet for pure education but unfortunately we have also a very large number of people including majority of youth .using Internet only for social networks. Internet is very big evolution of technology but when we talk about the social networks it is extremely dangerous for youth and become enormously common and widespread in past few years M. Trusov et.al. (2009). Social media are computer mediated tools that allows people to create, share or exchange information, career interests, ideas, and pictures, videos in virtual communication networks. Social media is defined as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content."Furthermore, social media depend on mobile and web-based technologies to create highly interactive platforms through which individuals and communities share, co-create, discuss, and modify user-generated content. Social media operate in a dialogic transmission system. This is in contrast to traditional media that operates under a monologist transmission model. "Social media has been broadly defined to refer to 'the many relatively inexpensive and widely accessible electronic tools that enable anyone to publish and access information, collaborate on a common effort, or build relationships.' There are many effects that system from Internet usage. According to Nielsen, Internet users continue to spend more time with social media sites than any other type of site. At the same time, the total time spent on social media in the U.S. across PC and mobile devices increased by 99 percent to 121 billion minutes in July 2012 compared to 66 billion minutes in July 2011.the list number of social media are available today in the market of internet like google, twitter, facbook, whatsapp, friendstore,myspace, linkedin etc.

1.1 ADVANTAGES OF SOCIAL MEDIA
1 Technological literacy
2 Bringing people together
3 Attracts attention
4 Breadth of knowledge
5 Opportunity to widen business
6 Worldwide connectivity
7 Real time information sharing
8 Increased news cycle speeds

1.2 DISADVANTAGES OF SOCIAL MEDIA
1 Distraction
2 Health problems
3 Relationship problems
4 Illegal crimes, virus attacks
5 Negative effects on worker productivity
6 Face to face connections are endangered
7 Risk of fraud

2 CYBER CRIME
Cyber criminals may use computer technology to access personal information, business trade secrets, or use the Internet for malicious purposes. Criminals can also use computers for communication and document or data storage. Criminals who perform these illegal activities are often

referred to as hackers. Cyber crime makes big challenges in the universe police department that has increased the use of Internet. India country is on the 11 th number as compared to the To this cyber crime of Australia,Macksico ,Japan country. In India above 50 laks people are attaché with the cyber crime. 20 percentage people are involved with the mobile cyber crime. So that to find out the misuse of the Internet government has increased facility regarding these cases. The investigation department of India makes more than 13 applications for to the Google Company in case of cyber crime and after the America country India is the first mot demanded country about the cyber crime. Government of India has appointed some organization to stop the crime in each district level area. One of the organizations is the TATA INSTITUTE OF SOCIAL SCINCE that having to arrange the conference, workshop to provide knowledge to the universe regarding the social Medias and cyber crime. Reliable sources report that during the year 2014, 179 cases were registered under the I.T. Act as compared to 68 cases during the previous year, reporting the significant increase of 163% in 2014 over 2015 Klovdahl AS et.al.(1994)

2.1 HISTORY

The first recorded cyber crime took place in the year 1820 which is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B.C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage. In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This was the first recorded cyber crime.

2.2 CATEGORIES OF CYBER CRIME
Cybercrime can be basically divided into four major categories Hundey and Elizabeth (2012)
1 Cyber crimes against persons
2 Cyber crimes against property
3 Cyber crimes against government
4 Cyber crimes against society at large

1 Cyber crimes against persons

Cyber crimes committed against persons include various crimes like transmission of child-pornography, cyber porn, harassment of a person using a computer such as through e-mail, fake escrow scams. The trafficking, distribution, posting and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cyber crimes known today. The potential harm of such a crime to humanity can hardly be explained. Cyber-harassment is a distinct Cyber crime. Various kinds of harassment can and do occur in cyberspace, or through the use of cyberspace. Different types of harassment can be sexual, racial, religious, or other. Persons perpetuating such harassment are also guilty of cyber crimes. Cyber harassment as a crime also brings us to another related area of violation of privacy of citizens. Violation of privacy of online citizens is a Cyber crime of a grave nature. No one likes any other person invading the invaluable and extremely touchy area of his or her own privacy which the medium of internet grants to the citizen. There are certain offences which affect the personality of individuals can be defined as:

Harassment via E-Mails: This is very common type of harassment through sending letters, attachments

of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter, Orkut etc. increasing day by day.

Cyber-Stalking: It is expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.

Defamation: It involves any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

Hacking: It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs. Hackers usually hacks telecommunication and mobile network.

Cracking: It is act of breaking into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

E-Mail Spoofing: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.

SMS Spoofing: Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another person in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual. Carding: It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account. There is always unauthorized use of ATM cards in this type of cyber crimes.

Cheating & Fraud: It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.

Child Pornography: In this cyber crime defaulters create, distribute, or access materials that sexually exploit underage children.

Assault by Threat: It refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

2. Cyber crimes against property.
The second category of Cyber-crimes is that of Cyber crimes against all forms of property. These crimes include computer vandalism (destruction of others' property) and transmission of harmful viruses or programs. A Mumbai-based upstart engineering company lost a say and much money in the business when the rival company, an industry major, stole the technical database from their computers with the help of a corporate cyber spy software. There are certain offences which affects persons property which are as follows:

Intellectual Property Crimes: Intellectual property consists of a bunch of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an crime. The most common type of

IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc. Cyber Squatting: It involves two persons claiming for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously. For example two similar names i.e. www.yahoo.com and www.yahhoo.com.

Cyber Vandalism: Vandalism means deliberately damaging property of another. Thus cyber vandalism means destroying or damaging the data or information stored in computer when a network service is stopped or disrupted. It may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral or a device attached to the computer.

Hacking Computer System: Hackers attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Due to the hacking activity there will be loss of data as well as computer system. Also research especially indicates that those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company. As in April, 2013 MMM India attacked by hackers.

Transmitting Virus: Viruses are programs written by programmers that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They mainly affect the data on a computer, either by altering or deleting it. Worm attacks plays major major role in affecting the computer system of the individuals .

Cyber Trespass: It means to access someone's computer or network without the right authorization of the owner and disturb, alter, misuse, or damage data or system by using wireless internet connection. Internet Time Thefts: Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge. You can identify time theft if your Internet time has to be recharged often, despite infrequent usage.

3. Cyber crimes against government.

The third category of Cyber-crimes relates to Cyber crimes against Government. Cyber terrorism is one distinct kind of crime in this category. The growth of internet has shown that the medium of Cyberspace is being used by individuals and groups to threaten the international governments as also to threaten the citizens of a country. This crime manifests itself into terrorism when an individual "cracks" into a government or military maintained website. The Parliament attack in Delhi and the recent Mumbai attack fall under this category. India had enacted its first Cyber Law through IT Act 2000. It has been amended and now in 2008 the revised version is under implementation.

4. Cybercrimes Against Society at large:

An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences include: Child Pornography: In this act there is use of computer networks to create, distribute, or access materials that sexually exploit underage children. It also

includes activities concerning indecent exposure and obscenity. Cyber Trafficking: It involves trafficking in drugs, human beings, arms weapons etc. which affects large number of persons. Trafficking in the cybercrime is also a gravest crime. Online Gambling: Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. In India a lot of betting and gambling is done on the name of cricket through computer and internet. There are many cases that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc. Financial Crimes: This type of offence is common as there is huge growth in the users of networking sites and phone networking where culprit will try to attack by sending bogus mails or messages through internet. Ex: Using credit cards by obtaining password illegally. Forgery: It means to deceive large number of persons by sending threatening mails as online business transactions are becoming the habitual need of today's life style.

2.3 PREVENTION OF CYBER CRIME

Prevention is always better than cure. It is always better to take certain precautions while working on the net. One should make them a part of his cyber life. Sailesh Kumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber crime Cell, advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance N. Ellison et.al.(2007)

1 Identification of exposures through education will assist responsible companies and firms to meet these challenges.

2 One should avoid disclosing any personal information to strangers, the person whom they don't know, via e-mail or while chatting or any social networking site.

3 One must avoid sending any photograph to strangers by online as misusing or modification of photograph incidents increasing day by day.

 4 An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination. 5 A person should never send his credit card number or debit card number to any site that is not secured, to guard against frauds.

6 It is always the parents who have to keep a watch on the sites that their children are accessing, to prevent any kind of harassment or depravation in children.

7 Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber crimes as number of internet users are growing day by day.

8 Web servers running public sites must be physically separately protected from internal corporate network.

9 It is better to use a security programs by the body corporate to control information on sites.

10 Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens.

11 IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.

12 As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.

13 A complete justice must be provided to the victims of cyber crimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of

cyber crime.

3. CONCLUSION

This paper described all over the problems regarding the cyber crime as well as the social media. This is very useful paper for the students who are working the social media every day in full of time but aware of the knowledge. It is described the advantages and disadvantages and different types of social media and crimes.

REFERENCES
[1] M. Trusov, R. E. Bucklin, & K. Pauwels(2009), "Effects of Wordof-Mouth Versus Traditional Marketing: Findings from an Internet Social Networking Site", In Journal of Marketing,Vol. 73, Issue 5, page 90-102.

[2] Jayme, Waddington (2011),"Social Networking: The Unharnessed Educational Tool",Universityof shikago,Undergraduate Research Journal, Vol 4.1,Page No.22-29.

[3] Hundey, Elizabeth (2012), "Social media as an Educational Tool in University Level Geography,"Teaching Innovation Projects: Vol. 2, Iss. 1, Article 5.

[4] Cho, H., Gay, G., Davidson, B., & Ingraffea, A. (2007)," Social Networks, Communication Styles, and Learning Performance in a CSCL Community", Computers & Education.,Vol.No.49(2),Page No. 309-329.

[5] Boyd, D. M., & Ellison, N. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), article 11.

[6] Tiffany A. Pempek, Yevdokiya A. Yermolayeva, Sandra L.Calvert(2009), "College students' social networking experiences on Facebook", In Journal of Applied Developmental Psychology, Vol. 30, Issue 3, page 227–238.

[7] M. Trusov, R. E. Bucklin, & K. Pauwels(2009), "Effects of Wordof-Mouth Versus Traditional Marketing: Findings from anInternet Social Networking Site", In Journal of Marketing,Vol. 73, Issue 5, page 90-102.

[8] K. Williams, A. Boyd, S. Densten, R. Chin, D. Diamond, and C. Morgenthaler(2009), "Social Networking Privacy Behaviors andRisks", In Proceeding of CSIS Research Day, SeidenbergSchool of CSIS, Pace University.

[9] Klovdahl AS, Potterat JJ, Woodhouse DE(1994), "Social networks and infectious disease: the Colorado Springs study" In SocSci Med, Vol. 38, Issue 1, page 79–88.

[10] N. Ellison, C. Steinfield, and C. Lampe(2007), "The benefits of Facebook "friends:" Social capital and college students' useof online social network sites", In Journal of Computer- Mediated Communication, Vol. 12, Issue 4.

Publish Research Article
International Level Multidisciplinary Research Journal
For All Subjects

Dear Sir/Mam,
        We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Books Review for publication,you will be pleased to know that our journals are

Associated and Indexed,India

* Directory Of Research Journal Indexing
* International Scientific Journal Consortium Scientific
* OPEN J-GATE

Associated and Indexed,USA

* DOAJ
* EBSCO
* Crossref DOI
* Index Copernicus
* Publication Index
* Academic Journal Database
* Contemporary Research Index
* Academic Paper Databse
* Digital Journals Database
* Current Index to Scholarly Journals
* Elite Scientific Journal Archive
* Directory Of Academic Resources
* Scholar Journal Index
* Recent Science Index
* Scientific Resources Database