IMPACT: Journal of Modern Developments in Applied Engineering & Technology Research (IMPACT: JMDAETR)
Vol. 1, Issue 2, Dec 2017, 51-58
© Impact Journals

CYBER SECURITY AND ETHICS ON SOCIAL MEDIA

MUDASSIR KHAN & SHAMEEMUL HAQUE

Research Scholar, Department of Computer Science College of Science & Arts Tanumah King Khalid University, Saudi Arabia

ABSTRACT

Cyber security becomes an important field in the information technology. Securing the individual and organization information become the biggest challenges in the present era. Nowadays peoples all over the world are dependent on social media. Social media is very useful in our life but social media is also effected by cyber crimes and increasing day by day.

Different social media websites are giving their best services in spite of that cyber crimes are increasing day by day. Still cyber security is a big concern for many in the present day. Nowadays peoples all over the world are addicted towards social media. Social media becomes the part of their life. The main concern is “how to protect social media from cyber crime”. The cyber security is very important for using the social media without and cyber crime but it becomes very difficult task “how to ensure 100% cyber security in the real world”. It also based on cyber security techniques used to solve the cyber crime related problems. It also emphases on ethics and trends changing the face of cyber security.

KEYWORDS: Cyber Security, Social Media, Cyber Ethics and Crimes

INTRODUCTION

Nowadays peoples all over the world can communicate with one click by using social media.

They can share audio, video, text and many more over the Internet. Life becomes very easy rather than old days. Today all over the world life of peoples are surrounded by social media and Internet. They need social media and Internet in their personnel life. For running the life smoothly after using social media over the Internet, they need cyber security. Today cyber security becomes the main issue. Whenever we are transmitting information over social media to other person” how securely data being transmitted or sent to the other person without any leakage of information”? The answer is “cyber security is not 100% data or information can be stolen or hacked by the cyber criminals”.

Today Internet is fastest and growing technology in the daily life of human being. In this technological era, we are having new technologies and different social media’s proving that our sites and apps are secure and reliable. But the real world scenario is different. Cyber security becomes the main issue in the everyday life. Now the main issue is that “how to overcome this cyber security problem”.

Even all the latest technologies like E-commerce, Mobile computing, cloud and grid computing and Net banking needs high level of security. All over the world government is giving main focus on cyber security and they are giving awareness to peoples how to use different latest technologies and social media. According to current survey in this real world we have million of cyber crimes daily.

CYBER SECURITY

The security and privacy of data is primary focus of any organization. Nowadays all over the world all peoples want to keep their data or information in digital form or cyber form. In these cases cyber criminals focused on social media websites, Net banking and many more personal uses. The following survey indicates the various cyber crime incidents occur over the past years.

Table: 1

Event	Year 2016	% Difference
Fraud	One in 10 peoples	Inc- 37%
Spam	One in 13 peoples	Inc-41%
Personal	One in 47 peoples	Inc- 75%
Denial of Services	One in 11 peoples	Inc-43%
Vulnerability reports	One in 17 peoples	Inc- 37%
Cyber attacks	One in 10 peoples	Inc-10%
Malicious Frauds	One in 20 peoples	Inc-10%

CYBER CRIME

Cyber crime is a form of crime where the internet or computers are used as a medium to commit crime.

According to the last year survey over 6 millions offences are committed last year, means out of ten peoples one is victim of cyber crime. The increasing number of cyber crimes day by day because the peoples are dependent on new technologies and social media. Fraud has become the most prevalent crime in the countries all over the world with peoples ten times more likely to become victim then they are to suffer a theft.

The Major Types of Cyber Crimes Seen are as Follows:

Phishing:

The main aim here is to trick people into handing their credit/debit card details or access to protected system. The emails sent out that contained the links or attachments that either takes you to the desired website that looks like your bank's page or install unwanted malware in to your computer. One of the survey showed that approximately 27% peoples all over the world open phishing emails on their systems.

Identify theft:

According to fraud protection agency Cifas, the number of victims rose by 31 per cent to 32,058 in the first three months of 2015. Criminals use online 'fraud forums' to buy and sell credit cards email addresses and collect data or personal information from social media sites.

Hacking:

In a survey of security frauds there were hundreds of millions data exposures, which works out to about 10 records exposed every second. 27% of these attacks were executed internally within organizations.

It is estimated that 91% of all data records that were used in a crime was a result of hackers employed by organized crime.

Online Harassment:

In the current world almost half of the teenagers have been persecute online, We can say that overall around 73% of adult users have seen few are strained in the online activities and more than 40% of peoples have an idea for this.

The Following List of Cyber Crimes under an IT Act:

- Hacking with computer systems
- Publishing obscene information
- Unauthorized access to protected system
- Breach of confidentiality and privacy
- Sending threatening information by email
- Forgery of electric records
- Bogus websites, cyber frauds
- Email spoofing
- Web jacking
- Social websites hacking
- Email abuse
- Misuse of social media

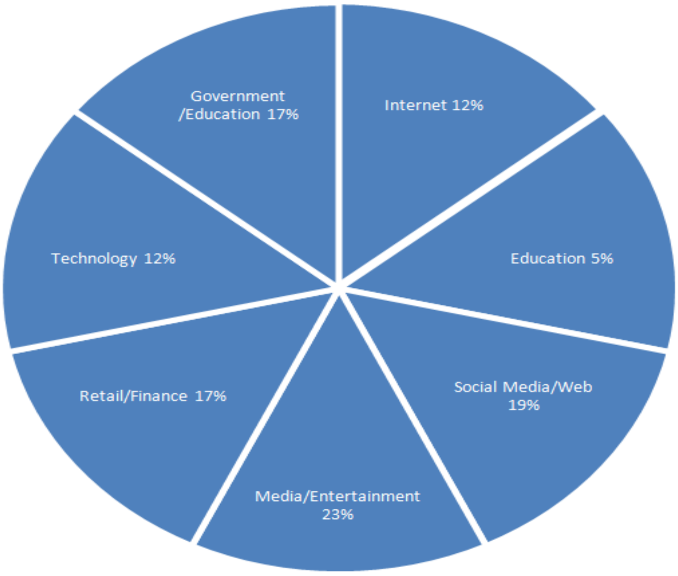

Figure 1: Cyber Crime Trends and Targets

SOCIAL MEDIA

Social media are online communications that allows individuals to creating and sharing of information via virtual communities and networks.

Websites and applications dedicated to forums, micro blogging, social networking, social bookmarking, social curation, and wikis are among the different types of social media.

The Following Prominent Examples of Social Media:

- Face-book- is a free and very popular social networking website that allows the users to keep in touch with family and friends. Face-book also allows the users to upload photos and videos, in addition send messages, share posts, add location, live videos and many more lasts features are there.
- Twitter- is a micro blogging social networking site that allows registered users/members to broadcast small posts that called tweets. Tweets can be done through multiple platforms and devices.
- Google (+) - It is also a social networking site that allows designing and reproducing the internet user interaction.
- Linked-in- is also a social networking site that is designed for professional interaction worldwide and especially for business community. The main goal for this social networking is to provide professional and business network globally.

SOCIAL MEDIA POLICY AND SECURITY:

- The explanation for the responsibilities of the employees of the company, who are responsible for the company confidential information. To describe, how the employees or staff of the company should convince that do not have the friend's, who are trustworthy towards the company policy.
- The clear information should be given to the employees, what are the requirements by them to help safeguard information that should be start from screen locks to the timely password changes.
- Regular periodic check for the privacy settings on social media sites access from the company or workplace and teach the employees about these types of settings.
- All the employees should know about any external or internal attacks on the company confidential data or information social media.
- The regular training sessions should be given to the employees for security and privacy of company data or information.

CYBER ETHICS

Cyber ethics is the research of virtuous, legitimate and social issues arises in the cyber technology. After the research impact cyber technology is surrounded by four social, moral and legal systems. It has been discovered that the social networking polices and principles and legitimate laws have been framed. The issues and crimes in the cyber technology are generated by the development.

The Ethical issues in the Information Technology system have been adopted new urgency by the growth of internet e-commerce. The Internet and the digital technologies make it easier to integrate, shuffle and distribute information. The appropriate customer information, the protection and personnel privacy should be protected.

The old computer era has many ethical issues that are raised by the information system. The quality of the system and standard should be followed to protect the data. The information systems, it is very urgent to ask" What are the ethical and socially responsibilities work of action". Social media is a social interaction through technology based on tools, which are based on internet. The social media exhibits unique characteristics over tradition media forum. The scope of social media means that the content is published and it is available instantaneously to the global audience. The social media tools are available free or at very low cost globally and do not require as much technical knowledge as other tools. This tends to allow individuals to publish materials than with traditional media forums. These unique characteristics of social media its challenges effects on real life.

ETHICAL RESPONSIBILITIES

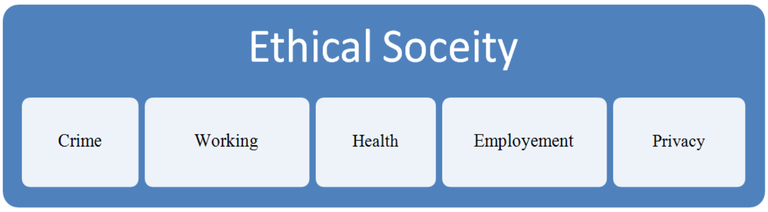

Figure 2: Ethical Society

Safety and Security

To understand the risk and authenticity, the problems imposed by the applications and other latest technologies like the viruses and phishing.

Digital Proficiency

Learning digital proficiency is based on the current information technology concepts. The skills build on the system traditional reading and writing.

Ethical Society

The ethical behaviors in the society are based on the digital environments. This area includes the digital environment those are responsible citizens of the society to communicate in which the society participate, from the social networks and civil forums.

Boundary Violation

The growth of social media and networking options has been phenomenal.The constantly changing in the technologies of the area of Computer Science becoming one of the most difficult to access a specific collection of moral codes. It is necessary that the ethics to be considered in the area of decision making. The technology creates overall an advance set of ethical problems and unique. So the technologies used by the citizens and professionals should not cross the boundaries. They should work under the current technology boundary set by the organizations for the propose of security and privacy.

Social Media Ethics Framework

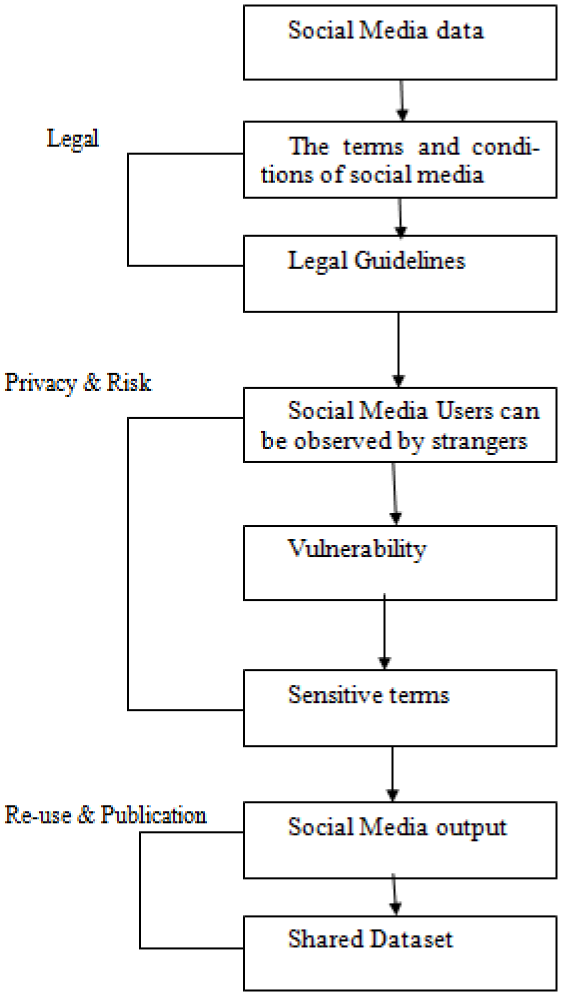

Figure: 3

CONCLUSIONS

It is very difficult to say that hackers from all over the world are making security breaches but in reality, 80% of data loss is caused by insiders. To design a pure security model for achieving protection of data in all the organizations must understand the security mechanism relevant to its business process. The scope of the security in different organization must be achieved at advance level to protect data loss from external and internal intruders. A business is using IT tools heavily, depends on providing services to the users to access the information in a way that is controlled and secure. In addition to deploying standards bases, flexible and interoperable systems, the technology must provide assurance of the security provided in the products. As technology developed and secure information systems are deployed, companies will be better positioned to manage the risks associated with companies can access the market directly for accessing the data or information. Overall this is possible to develop ethical guidelines on an ongoing basis to keep changes in the issues. The codes of ethics are varies from one professional organization to the other organization.

REFERENCES

1. Bynum, Terrell Ward, A very short history of computer ethics, Southern Connecticut State University, 2008.
2. Computer Security Institute and US FBI, Computer Security Issues & Trends, CSI 2000.
3. Forester, T. and Morrison, P. Computer thics, MIT Press, Cambridge, Mass., 1990. http://www.acm.org/about/code-of-ethics.
4. IEEE code of ethics. http://ieee.org.
5. ISO/IEC 17799 Code of practice for Information Security Management, International Organization for Standardization.
6. Kling, R., Computer abuse and computer crime as organizational activities, Computers and Law J. 2 (Spring 1980).
7. Mason, R.O., Four ethical issues of the information age, MIS Quarterly, 10, 1 (1986),5–12.
8. Praveen Dalal, ICT Trends in India, 2006
9. Altman I (1975) The environment and social behavior: privacy, personal space, territory, crowding. Cole Publishing Company, Monterey, CA
10. Baker DJ (2008) Constitutionalizing the harm principle. Criminal Justice Ethics 27:3–28, Summer/ Fall 2008
11. Bennett CJ, Raab CD (2006) The Governance of Privacy: Policy Instruments in Global Perspective.Cambridge, MA, London: MIT Press, 2 ed.
12. Bowie NE, Jamal K (2006) Privacy rights on the internet: self-regulation or government regulation?Bus Ethics Q 16(3):323–342
13. Boyd d (2008) Facebook’s privacy trainwreck: exposure, invasion, and social convergence.Convergence: The International Journal of Research into Media Technologies 14(1):13–20
14. Mediat Commun 13:210–230.http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html. Accessed 12 Jan 2011
15. Hornung G, Schnabel C (2009) Data protection in Germany I: the population census decision and the right to informational self-determination. Comput Law Security Review 25:84–88
16. Hoy MG, Milne G (2010) Gender differences in privacy-related measures for young adult facebook users. J Interactive Advertising 10(2):28–45
17. Ibrahim Y (2008) The new risk communities: social networking sites and risk. Int J Media Cult Polit 4(2):245–253
18. Jonas H (1984a) The imperative of responsibility: in search of ethics for the technological age. University of Chicago Press, Chicago
19. Jonas H (1984b) Warum wir heute eine Ethik der Selbstbeschr€ankung brauchen. In: Str€oker E (ed) Ethik der Wissenschaften? Philosophische Fragen. Wilhelm Fink Verlag, M€unchen, Paderborn, Wien, Z€urich, pp 75–86