Asian Journal of Applied Science and Technology (AJAST)
(Peer Reviewed Quarterly International Journal) Volume 3, Issue 3, Pages 146-150, July-September 2019

Social Networking Crimes: A Conceptual Analysis on the Rising Problem

Dr. N. Saranya Devi

Assistant Professor, School of Management Studies, Tamil Nadu Open University, Chennai. Email: saranyan19@gmail.com

Article Received: 29 January 2019 Article Accepted: 23 May 2019 Article Published: 13 August 2019

ABSTRACT

The present article discusses about the issues of social networking which is the major threat in present scenario. It also highlights the reason for which the cyber criminals prefer the social networking sites. Social networking scams which are the threat to reveal the users private details that is mostly unnoticed by the user which leads to slip into the cyber criminals are discussed. As network attacks other network and also target population, hence proper measures of safety need to be adopted to remain secured in social networking sites such safety measures are enumerated.

Introduction

Online Social networking is a type of virtual communication that allows people to connect with each other. This concept arises from basic need of human beings to stay together in groups forming a community. Social networking sites, email, instant messaging, video- and photo- sharing sites and comment posting are all tools that help people to communicate and socialize with each other (Mooney, 2009). A well-known use for the fresh technology is social networking among businesses. Organizations had find that social networking sites like Facebook and Twitter are good traditions to develop their product icon. As per Nimetz (2007), writer of Marketing Jive, there are five main uses for businesses and social media are (i) to develop product wakefulness, (ii) as an online status management tool, (iii) for hiring, (iv) to find out about fresh technologies and opponent, and (v) as a main generation tool to interrupt possible prediction. These organizations are capable to take crowd to their self online sites as cheering their customers and users by planning on how to progress or modify products or services.

Issues of Social Networking Sites

1. Privacy

Once the details are posted to a social networking website, it is no longer personal. The more details the user posts, the more at risk he or she might get into. Even whenever making use of high security settings, associates or sites might unintentionally pour out user's information. Confidentiality on social networking sites could be undermined by many aspects. For instance, users can include private details but sites might not get sufficient actions to guard individual's privacy, and third parties recurrently make use of details submitted on social networks for lots of reasons. Many social networking websites provide an API (Application Programming Interface) for third party developers to create applications that can run on its site. These third party applications are very trendy among social network users. Once users add and permit third party applications to access their information, these applications can access user's data automatically. It is also capable of posting on users' space or user's friend's space, or may access other user's information without user's knowledge.

2. Data mining

By data mining, organizations are able to improve their sales and productivity. Using this information, organizations develop user's profiles which include user's demographics and online performance. Business

players, hackers, predators, and overseas actors' sprite use the social networking websites for seeking details of individuals to allege for misuse. Details obtained from social networking websites may be utilized to design a precise assault which does not approach by way of the social networking website.

3. Access to information

Various social networking services offer the individual with an option to whomever they may allow to see their profile. This avoids illegal individuals from accessing their details.

4. Compromising User Account

Cyber criminals use different methods such as Social Engineering, Spam mails, Malwares, Cross Site Scripting and stealing cookies, to take control of an user account which may lead to the disclosure of sensitive information resulting in the compromise of the of the user account along with the details of the individual user along with the information about the others including his office.

5. Hazards for child security

People and government are anxious on child and teenagers for the misuse of social networking sites particularly relative to online sexual predators. Uncontrolled use of social networking might build children towards gloominess and fretfulness. Then the paedophile cultivates a friendly online relationship that which the law enforcement agency calls it as "grooming." It could continue for days or weeks before the paedophile begins bringing up sexual topics, asking for explicit pictures or for a personal meeting. By that time a touching relationship has been made. Even if an actual meeting never takes place, it is important to note that youngsters can be victimized by such sexually explicit online contact.

6. Cyber bullying

Cyber-bullying is comparatively familiar event and it may be out as a poignant shock for the fatality. Dependent on the networking opening, nearly 39% of users are admitted to being "cyber-bullied".

Evolution of Cyber Crime in Social Networking Sites

A social media offers users a well-organized method to interact in a network with one another on an unprecedented scale and at rates unseen in traditional media. A social networking site offers a virtual society for people to intermingle. People are pushed towards identity-exposure by others which significantly have an effect on privacy. Those records include individual details of the account owner. Even though a latest confidentiality setting includes private details, such as person's name, sex, address, date of birth etc. Regarding to the previously completed privacy settings, which was not sufficient. Illegal activators may simply receive benefit of this undeleted information from record container would be digamous through many ways!

Social Networking Sites are favourite location for Cyber criminals

The major reason for the attraction of social networking sites by the cyber criminal are as follows.

- ➢ Increasing social networking popularity.

- The addiction or lure towards social networking.
- Social networking becoming an ideal place for crime as it takes more time to find the offender.
- The enormous transition from emails to social media.
- Growing usage of social networking over smart phones.

Threats of Social Networking Sites

Social networking sites are becoming more well-known due to the joy, advantages and fun linked with it. One thing that user do not observe is the threat involved in revealing users private details. Users must be pretty cautious as social networking websites are largely fall prey on to cybercrimes. Some of the most general social networking scams are:

Fake identity: It is fairly simple to set up a fake identity on the huge social networking sites and it benefits the offenders. As a result user believing people blindly as well as think prior to accepting friend requests.

Identity theft: Other than acting as someone else, scammers could pilfer information through social networking sites too. Offenders might then attempt to create a phishing for user log-on passwords. Therefore user must keep boundaries to post too many details regarding themselves and be cautious for page asking users to login once more although the page was sent as a message by an online friend. The page might seem to be a fake page that asks you to login "again". In actuality users are providing their secret password to a scammer.

Social Network Spoofing: In this assault attackers set up a false Facebook page in support of light company. Users might join under the purpose of it being a real company. The users might have tricked on login in for discounts and in the bargain their personal info is theft. By this means they can let the uses to visit some malicious sites and implant malicious codes in to their computers.

Downloading Malware: So as to make the social networking sites pretty thrilling diverse user-generated software could be configured by associates on their profile pages. The problem is that there are so many of these applications that even website security people keep great effort to remove them. These acts as an entry for swindler who are mixing out spyware, Trojans and viruses where members inadvertently either download to their own system or post on their account pages. Therefore user could see that many cybercrimes are done by the means social networking sites as the spirit of online community is reliance. People believe others unknowingly and reveal their information online making thing simpler for cybercrime.

Cyber Crime of Social Networking Sites

Jamil and Khan (2011) while comparing the data protection act in India with that of European countries have concluded that the Indian cyber laws are very poor and it is very necessary to actually bring in the appropriate cyber law and awareness about them. There is not much of awareness regarding protecting the data. There is a continuous rise in cybercrime as there is huge population but lesser resources to manage the population and the cybercrimes that take place.

The main factor in cyber-crime increase is the Internet. By use of Internet, cybercriminals often appeal to images, codes or electronic communication in order to run malicious activities. Among the most important types of Internet crimes we can mention: identity theft, financial theft, espionage, pornography, or copyright infringement. The cyber-crimes can be divided into two categories: the crimes where a computer network attacks other computers networks – e.g. a code or a virus used to disable a system, and, the second category, crimes where a computer network attacks a target population – e.g. identity theft, fraud, intrusions Svensson, (2011).

Safety measures to remain secured in Social Networking Sites

Whether to use social networking site or not is an individual decision to many. But you must be aware of certain things when discussing your private life in public. These are some of the tips that can make you and your family safe on the networking sites.

1) Change the profile privacy now. Keep your information accessible only to people in your friend list.
2) Don't accept friendship request from strangers. Many often we judge a particular person online, by his/her profile picture and personal information. This is the first mistake that cyber criminals wanted us to do.
3) Don't post very personal information on the profile. It includes your email id, date of birth, contact number, home address and information about your family members.
4) Be cautious while posting your photo. Ensure your photo background doesn‟t show about your actual whereabouts.
5) Don't post your current location when on a tour. Posting this information on social networking site is just like inviting criminals.
6) Don't post negative things about your life. This is just like maligning your own image. Your friends are monitoring your activity and one such mistake can cause havoc in future.
7) Make distance from your ex's profile. This might seem you little cruel, but once you decide to quit a relationship there is no meaning again visiting your ex-partner‟s profile. If you want to have a good life in future, then unfriend your ex from friend list.
8) Don't substitute real friends with virtual friends. Facebook is a great tool to connect new people across world. But they can never be your real friends. You need real friends to enhance your social image and reduce stress and anxiety.
9) Avoid using Social networking sites in work hours. When you try to use social networking sites during work hour, it not only affects your work performance but also increases chances of getting fired.

Conclusion

The growth of social networking sites shows a significant change in the social and personal behavior of Internet users. SNS has become an essential medium of communication and entertainment among the young adults. Though it has started to affect the daily activities of normal human beings, the popularity of SNS is not going to reduce in

near future. Everything in this world can be used for a bad purpose as well as for good. It‟s us who can make the difference and utilize social networking sites wisely for the benefit of developing social bonds across the geographical borders. However, nefarious act of cyber criminals discussed in the article has to be brought to the fore and stringent measures should be taken to curb the menace. Cyber laws have to be fortified with advancement of rules as if violators cannot escape committing a crime, at the cost of societal values.

Reference

Biswajit Das, (2011). Social Networking Sites – A Critical Analysis of Its Impact on Personal and Social Life, International Journal of Business and Social Science, Vol. 2 No. 14, p-222.

Jamil D. and Khan M.N.A. (2011), Data Protection Act in India with Compared To the European Union Countries, International Journal of Electrical & Computer Sciences, Vol: 11 No: 06.

Jennifer Obbe, (2012). Social Networking, The Scarecrow press, UK, p-55-76.

Mooney, Carla. (2009). Online social networking. Gale Cengage Learning.

Peter K. Ryan, (2011). Social Networking, The Rosen publishing group, New York, p-7-23.

Svensson, P. (2011). Nasdaq hackers target service for corporate boards. Retrieved from http://news.yahoo.com/s/ap/20110205/ap_on_hi_te/us_nasdaq_hackers.