Journal of Forensic Research
ISSN: 2157-7145

Sarawagi and Srivastava, J Forensic Res 2016, 7:2
DOI: 10.4172/2157-7145.1000326

Research Article Open Access

Forensic Examination of Cyber Crime in Special Reference of Social Networking Sites

Ketan Sarawagi[1*] **and Dr. Ankit Srivastava**[2]

[1]*Dr. APJ. Abdul Kalam Institute of Forensic Science & Criminology, Bundelkhand University, Jhansi (UP), India*

[2]*Assistant Professor, Dr. APJ. Abdul Kalam Institute of Forensic Science & Criminology, Bundelkhand University, Jhansi (UP), India*

[*]**Corresponding author:** Ketan Sarawagi, Dr. APJ. Abdul Kalam Institute of Forensic Science and Criminology Bundelkhand University, Jhansi (U.P.), India, E-mail: mailme.ketansarawagi@gmail.com

Received date: Dec 02, 2015, **Accepted date:** May 20, 2016, **Published date:** May 30, 2016

Abstract

This paper provides an overview of the growing cybercrime problem and reviews the disadvantages of over uses of social networking sites. This paper also categories some types of cybercrimes that may cause victimization by these social networking sites. It includes few case studies showing how the personal information is stolen if someone's profile is already registered on any social networking sites for either monetary gain or antihuman activities like money laundering and terrorist activity respectively. Certain suggestion and preventions are also mentioned in full paper.

Keywords: Social engineering; Foot printing; Dumpster diving; Encryption; Decryption; Cracker; Hacker

Introduction

The predecessor of today's internet ARPANET was designed as a communication system that would allow researchers to access information from other computers around the country, therefore allowing information to flow more freely [1]. Later this expanded over the limits and reached to each and every point on glob and now a day's computer and the internet have become intertwined into our daily lives. The use of the internet is very essential because they can gather and share information with other individuals as well as the decreasing cost and size of computers no matter where individuals are located on the globe. Thus facilitates business at domestic to global level. However this new technology has brought with it much advancement which makes our lives easier but unfortunately it has also led to advancements in crime [1-3].

The growth of the internet has also resulted in the creation and growth of cybercrime due to ease of availability and connections through world web. Cybercrime is a major issue facing society today, requiring law makers and law enforcement agencies to take action. This issue can have a major impact on governments, businesses, and individuals and thus deserves the attention of researchers [4].

Some examples of cybercrime are: financial theft through e-banking, pornography, data stealing, data manipulation, hacking, cracking etc. [5]. The purpose of this paper is to take a look at areas related to cybercrime which may occur through social networking sites and to review criminological theories that have been applied to the study of cases of cybercrime and also suggested some tools and techniques to protect ourselves from these threats. The hacker and crackers are the individuals who get access into a system or into a network without any authorization. Mainly used techniques by the scammers involve reconnaissance in other word one can say foot printing (gathering information about the targeted person is called foot printing). It involves three techniques dumpster diving in this technique scammer uses to go through the victim's garbage and tries to gather useful information about the victim. The second technique is social engineering it is an art of convincing people to reveal sensitive information. The third is shoulder surfing it is a technique in which attacker spies over the victim's shoulder and try to steal sensitive data of the victim which is displayed on the screen of the victim [6,7].

Social Networking

A social networking service is a platform to build social networks or social relation among people who, for example, share interests, activities, backgrounds, or real-life connections. Network service consists of a representation of each user that is called profile, his/her social links, and a variety of additional services. Social networking sites allow users to share ideas, pictures, posts, activities, events, and interests with people in their network. Some social networking sites are Facebook, Twitter, Gmail, yahoo, Indyarocks, Orkut etc.

Social Networking based Application: An Alert

The applications used by the smart phone users like whatsapp, line, viber, we chat, true caller etc. are also very dangerous since the administration of that server can easily find the exact location of any contact number present in the phone of the user of any such application.

Results and Discussion

Case study: 1

An officer of a steel plant named Akash shrivastava of Jabalpur was browsing on his personal computer in his office a popup of 'Facebook notification' came. He eagerly clicked on that link to join the chat or see the new post in his profile but he found that it is an advertisement of another social networking site he refused it and went to lunch room to take his lunch. When he came back he found that his all deals and

all data related to company working and marketing strategies are deleted and in this way he was in loss of Rs 5, 00,000.

While investigation it is found that the popup of 'Facebook chat' was containing a infected link that have a patch file hidden in it of a software called net bus through which the employee of the same company offended this crime, with the help of this software he hacked his boss's computer and committed this crime.

Elements of this case: fake link 'facebook', netbus tool.

In this case the interest of Mr. Akash Shrivastava in facebook which is a social networking site made him a victim, and so many social networking sites and their fake pages with popup are available on internet which may helpful to the crackers or hackers.

"Be aware from subordinates and friends in financial matter. "

Case study: 2

A business man activated internet banking on his account, after some days he found that all his account balance Rs. 7,50,000 has been transferred to an account through internet banking.

After the investigation offender confessed his offence when appeared in the court and told to the court that he was actually a friend of the victim. One day the victim's maid was dumping some paper pieces at dump yard through dumpster diving he found an envelope having information regarding the confirmation of activation of internet banking also mention that the new user ID and password has been sent to your registered e-mail account. That envelope was stolen by the accused. Through shoulder surfing he noticed that the victim use to save his all ID and passwords in his opera browser. In his first attempt to get the ID and password he found that the victim's laptop was protected with a password and a hint statement for that password, which was "add jay after your elder brother's best friend's name". Here he had taken advantage of social networking site called facebook; firstly he opened victim's profile then he gone to his elder brother's profile where he checked the list of close friends and found only one name 'Surya'. He attempted many times with different password like 'Suryajay, Surajjay, Prabhakarjay etc." at last he got the password as Sunjay from there he had stolen the mail id password and from there he transferred money by login in internet banking site of the bank and transferred all the money to another account.

Elements of this case: Dumpster diving, shoulder surfing, Facebook profiles, Hit and trial method.

As in above case social networking sites are also helpful to gather sensitive information like phone no., address, photos, friends etc. especially when victim is a female.

Case study 3

One day a MMS came to a girl namely Divya Kapoor, containing her vulgar photograph followed by a SMS within a minute. The accused was blackmailing the girl for money in lieu of publically displaying the photograph through web.

The investigating team found that the photo was edited by using tool trick photography and the photograph of that girl was downloaded from her unsecured facebook profile.

Elements of this case: Facebook profile, Photo editor software, Mobile phone.

Thus uploading her photograph on the internet especially in social networking sites made her victim.

Conclusion

From the above discussion it is clear that the social network services are meant good for society but often these are dangerous if not secured. Especially the adolescence and young ones should aware of the drawbacks of the frequently uses of social networking sites and should always be careful and secured in case of their confidential information. With the help of some tools, software and some techniques like encryption decryption mechanism, use of a Antivirus, Antitrozen horse, and net craft tool bar for browser which counterstrikes the phishing attacks, in cyber cafes check for the key loggers, check the network protocol written before the URL etc.

One should take precaution in using phone application specially VVIPs Intellectual brains which may be traced by GPS system by the servers and also prevent these individuals form anti-social or anti-terrorist activities.

Cybercrime research will be an important area of study for future criminologist as we move farther into the digital age, who knows, there may be a day in the far future when the number of cybercrimes committed outweighs the number of traditional crimes committed.

References

1. Tiwari RK, Sastry PK, Ravi Kumar KV (2002) Computer crime and computer forensics 1: 89-97, 113-116.
2. Dernadette SH, Clemens M (2004) Cybercrime (A reference handbook) 1:247.
3. Stephension P (1999) Investigating Computer related crime. CRC press, BocaRaton London, Newyork, Washington DC. Pp: 82-83.
4. Singh YK (2005) Cybercrime and law. Shree publisher and distributers 1: 1-2, 8-9, 28.
5. Mishra RC (2005) Cybercrime impact in the new millenniums. Authors press 1: 1-2, 57, 29.
6. Emmett Paize Jr. (1996) " The future of information technology. Defence issues.
7. Howard M and Le Blanc D. Writing secured codes, Microsoft press, Redmond Washington.