ANALYTICAL STUDY OF CYBER THREATS IN SOCIAL NETWORKING

Seema D. Trivedi,  
MEFGI, Rajkot  
Gujarat, India

Ms. Chandani Kathad,  
AITS, Rajkot, Gujarat,  
India

Ms. Tosal Bhalodiya,  
AITS, Rajkot, Gujarat,  
India

Ms. Tanvi Pandya,  
AITS, Rajkot, Gujarat,  
India

Abstract:

A social networking service (SNS) or Social networking site is a platform to build social networks and social relations among people who share similar interest, activities or other real-time connections. A cyber threat is referred as unauthorized access to the system or network using communication pathway. Cyber threat can be either intentional or unintentional. Such threats to control system can come from numerous sources such as intruders, terrorist group, unsatisfied employees etc. To protect such threats, it is necessary to create cyber-barrier. In this paper we investigate the cyber threats in social networking. We go through history of when social networking website started and classify their category, possible threats related to social network and ways to prevent such threats.

Keywords:  
Social networking website, security

1. Introduction

Now a days millions of people visit so many social networking site to have in touch with their friends, share their photos, videos & even to discuss their day-to-day life. The first E-mail was sent in 1971 by Raymond Samuel Tomlinson, who was programmer on the ARPANET. In 1987, bulletin board system exchanged data over phone lines with other users. The first social media site incorporated in 1995, as theglobe.com which created community of registered users with the freedom to personalize their online experience, publishing their own content and interacting with people of similar interests. In 1997, AOL (America on Line) Instant Messenger was launched. In 2002, Friendster was launched and just in time span of 3 months, more than 3 Millions of people were using it. Skype was launched Orkut was launched in January 22, 2004. Facebook was launched in February 4, 2004. Twitter was launched in march 21, 2006.

![Figure 1: Social Network Site Usage](image-url)
Social network has its positive and negative impact. Many people waste their most of the time on such social network sites. Which may cause losing their job, social lives and families. Many people are using it in positive way as well.

Commonly, users of social network site make many mistakes while using it. People post unauthorized data, most of the people even post their private pics and videos etc. as public which can be accessed by anybody. Intruders may gain such data and can misuse such sensitive information.

No. of users of social network site is increasing day by day. And due to that attacks are also increasing to gain access over sensitive information of other users. Hacked information can be used in so many ways. Many people just view the information to have constant watch in other’s personal life. They don’t damage the data neither use it in other way. Which is known as passive attack. Whereas if data is used to harm person such as stealing someone’s account password and use it for robbery comes under type of active attack. The purpose of this paper is to study current possible attacks and take countermeasures to prevent the information.

2. Privacy and Threats of social networking

The popularity of social networking is increasing day by day since 1997 and now millions of people using social networking site to be in contact with their friends, to share their thoughts, photos, videos and daily life.

Article [6] security breaches and attitude behavior of social networking site users.

3. Classification of social network

A social networking service (SNS) or Social networking site is a platform to build social networks and social relations among people who share similar interest, activities or other real-time connections. Such social networking sites are Friendster, orkut, facebook, skype, twitter, myspace, linkedin, flicker etc.

Top five social website

<table>
<thead>
<tr>
<th>Web site name</th>
<th>Monthly Visitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>900,000,000</td>
</tr>
<tr>
<td>Twitter</td>
<td>310,000,000</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>255,000,000</td>
</tr>
<tr>
<td>Pinterest</td>
<td>255,000,000</td>
</tr>
<tr>
<td>Google Plus+</td>
<td>120,000,000</td>
</tr>
</tbody>
</table>

4. Cyber Threats in Social Networking

4.1 Privacy Related Threats:

The information provided to social networking site ranges from sharing their contact detail, personal photos, e-mail, employment etc. which increase security breach and privacy. Social engineering is generally used by hackers to gain access over sensitive information using phishing, malware, key logger, and masquerader to steal vulnerable details and use it when and where required.

4.2 Traditional Network Threats:

There are two types of threats: 1. Security of person & 2. Security of computer which people use to store
their data. Hackers may gain the data and can harm an individual or use their sensitive information to harm an individual to injure persona dignity.

![Figure 2: Threat possibilities in different social networking site](image)

5. Anti-Threats Strategies:

In this section I discuss about different type of security threat in social networking and found that most of the security breaches causes due to the factors listed below:

a. People are not concern about the importance of the personal information disclosure which makes security breach in security.

b. Users who are not aware of threats, chose wrong security settings.

c. The security policy is not well fortified to deal with threats which increases day by day with more challenges and technologies.

d. Lack of authentication mechanism to handle different privacy policies.

6. Risk Prevention and Threats Vulnerability:

In this section, I discuss about countermeasures which can help users of social networking to stay safe by applying the following:

a. Password always must have strong combination of numbers, letters and special characters and it must be enough long which can’t be easily cracked.

b. Reducing providing personal information on social network as much as you can.

c. Change the password on regular basis which may stay away hackers to gain access over the password by
guessable password techniques even if people know you very closely.

d. Don’t trust strangers and don’t answer question asked by unknown people.

e. Be very much careful about making friends online if you don’t know them.

f. Have strong privacy settings and be sure about unknown e-mails and links sent by users.

g. Don’t share everything what you do on social networking site

7. Conclusion:

Social networking site provides an advantage of connecting and interacting with people from anywhere and anytime. It also increase the chances of security breach. In this paper, I have briefly described the usage of social networking website, security breaches and countermeasures to prevent vulnerabilities.

We think social networking site as advancement tool to be connected with people but it comes with risk for malicious actions using phishing, keylogger, malware, Trojan horse, viruses etc.

References:


[7] https://www.google.co.in/?gfe_rd=cr&ei=MIROVqj5ILDGg7HgDw&gws_rd=ssl#q=traditional+network+threats+in+social+networking+websites


