Social and Security influence of Social Networks

Report by

**Utkarsh Kaushik, PCE20CS191**

**Prachi Khandelwal, PCE20CS119**

**Sanya Gupta, PCE20CS120**

**Siddharth Kothari, PCE20CS181**

**Bachelor of Technology in Computer Engineering - II Year**

Under the guidance of

## Mr. Animesh Srivastava



(Session 2021-22) **Department of Computer Engineering Poornima College of Engineering**

ISI-6, RIICO Institutional Area, Sitapura, Jaipur – 302022

# Table of content

* Abstract
* Introduction
* Problem Statement & Objective
* Literature Review Paper[1-12]
* Comparison Table
* Proposed Approach
* Conclusion
* Future Scope
* Reference

**Abstract**

Our study analyses possibilities of misusing social network sites due to irresponsible behaviour of users. Recent surveys show that problems of social network are more often to occur, due to openness as one of the key features of these sites. Social engineering can be misused by attackers concerning on social network with the purpose of gaining sensitive information. There is a conflict between users’ security awareness and their actual behaviour, so called privacy paradox. We were interested in amount of information people are willing to reveal in their profiles. We have found out users’ behaviour which leads to insufficient protection of published information. These sensitive information are suitable for all kinds of phishing and other similar attacks. In our study we compared two groups of fictive profiles (personal profiles of users having no friends and profiles of users with fictive friends) and studied their success in creating new links in social network. We also considered tools for protecting sensitive information in social network

**Introduction**

Enabling social interactions among individuals is a critical requirement for many network applications. Boosted by the availability of ubiquitous connectivity, the internet is even more an internet of people ,rather than a simple internet work of hosts .This paradigm has also accounted for the huge success of Web 2.0, which enables to create and share contents with an increased degree of social connectivity.

Although, such features were already present in the original web vision. Specifically, the Social Web Incubator Group within the World Wide Web Consortium (W3C) put effort in the definition of a social web, where “people can create networks of relationships overlapped with the entire web, while controlling their own privacy and data”. Unfortunately, as today, social services are not based on standardised architectures.

Online social networks (OSNs) are the archetype of this new wave of applications counting millions of active users worldwide . Even if a definition is absent, an informal one can be as follows: ‘an OSN enables the interaction among participants according to some relationship basis’. Such links can be very mixed, since they can be based on friendship, business partnership, or common interests. As a consequence, OSNs are highly specialised, e.g., there are general-purpose services for dealing with specific topics, such as books and travelling. To make some examples, we mention Facebook, Google+ and Twitter. Facebook and Google+ offer a rich set of functionalities, ranging from text and multimedia sharing, to AV communications. Instead, Twitter is limited to 140 character long text messages.

**Problem Statement and Objective**

During our experiment we addressed 40 persons (20 males and 20 females) and asked them for adding to their group of friends in order to get to their personal information. Our request was successful in 47.5%, 19 persons agreed to become our friends.

We analysed obtained data and the results show that users are not aware of danger following from publishing personal information on social networks.

We also compared successfulness in creating new contacts with profiles without friends and profiles with friendships.

We wanted to check whether number of friends influences successful rate in creating new contacts.

**Literature Review**

**Paper 01:**

**A study of cyber security challenges and its emergent trends on latest technologies**

By: G.Nikhita Reddy , G.J.Ugander Reddy

B.E, CSE second year at Chaitanya Bharathi Institute of Technology, Osmania University, Hyderabad., India

B.E, M.B.A. and Founder Director - Peridot Technologies, Hyderabad, India

Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day.

As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats.

Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data. In a world where we’re quick to give up our personal information, companies have to ensure they’re just as quick in identifying threats, responding in real time, and avoiding a breach of any kind.

Since people are easily attracted by these social media the hackers use them as a bait to get the information and the data they require. Hence people must take appropriate measures especially in dealing with social media in order to prevent the loss of their information. The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. The rapid spread of false information through social media is among the emerging risks identified in Global Risks 2013 report.

**Paper 02:**

**On Privacy and Security in Social Media – A Comprehensive study**

By: Senthil Kumar N, Saravanakumar K, Deepa K

School of Information Technology and Engineering, VIT University, Vellore

In the larger context of data mining, a considerable measure of productive analyzing so as to learn can be found advanced records of human conduct in interpersonal organizations without breaching the users’ privacy. Thus, information ought to be made accessible in a manner that privacy should be safeguarded and protection is extremely scrutinized.

On the other hand, the suspicion that any outsider which is intrigued to break down information can be viewed as reliable is truth be told unlikely, because of the key point of preference that the usage of all information, including recognizing and delicate ones, may provide for these gatherings. Due to the specific instance of interpersonal organizations, the most grounded measure that can be received is to make unflinching quality of individual’s privacy who expresses the affiliation.

It has been observed that privacy concerns are very feeble in the social networking sites and the users endeavors to make the appropriate changes on their social media privacy is substantially lower than other mode of security operations.

Besides, many of the social media users have the dearth of technical makeovers and thus yield the low privacy concerns to their own content. In the statistics taken, we had identified many of the shortcomings and hiccups on the technical side of privacy and security measures are on the social media sites. Hence, we had given the possible root cause of the glitches and proposed the changes to take over for the privacy concerns of social networking site.

If we would go for enforcing a set of well defined policies for social media, like, a strong password, awareness of changing password often, awareness of information disclosure, purpose of antivirus or related software, and proprietary software etc, we would secure the social networks from further attacks and vulnerabilities

**Paper 03:**

**Privacy and Social networks**

By: Patrick Van Eecke, Maarten Truyens

In the context of social networks, the difference between data controllers and data processors is particularly vague, because both the social network operator and the users qualify simultaneously as data processor and data controller, as they both define the purpose and the means of the processing (although for different combinations of data flows and purposes).

For example, the structure and the technologies used on the social network are solely determined by the social network operator. However, the user himself also defines the purpose and the means of the processing when he chooses which social network he will use, why he will use this network (e.g. to stay in contact with friends or colleagues, or to boost his career), and which social network applications he will install (e.g. a birthday or event calendar). As a result, the network operator qualifies as a controller for the account data of the user (name, first name, alias, icon or photo, membership of specific groups, etc.) in the context of the performance of its contract with the user . When the consent of the user has been obtained of the Directive), the account data as well as all additional data that (only) relate to this user38dcan also be used for other purposes, for example to sell valuable commercial information to third parties. In this context, the user is a mere data subject towards the social network operator. Conversely, the user qualifies as a data controller for the personal data he publishes on the network about third parties.

**So On for all the papers….**

# Comparison Table

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No** | **Paper title** | **Author’s Name** | **Year** |
| 1 | A study of cyber security challenges and its emergent trends on latest technologies | G.Nikhita Reddy , G.J.Ugander Reddy | 2019 |
| 2 | On Privacy and Security in social media – A Comprehensive study | Senthil Kumar N, Saravanakumar K, Deepa K | 2015 |
| 3 | Privacy and Social networks | Patrick Van Eecke, Maarten Truyens | 2010 |

**Proposed approach**

* Provider established precautions
* Personal precautions
* Technical precautions
* Legislative precautions
* User’s precautions
* Facebook: example of security solutions

Recent solution on Facebook is not compliant with aforementioned requirements it is not enough fast and simple for the most users. Although there is a possibility to define who can see your profile, who can search for you, which information about your activities will be public, which information do you share with your friends, which information are available to Facebook applications etc., but only some users take time to adjust the security of their profile

**Conclusion and future scope**

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information.

The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

**References**

1. <https://citeseerx.ist.psu.edu/viewdoc/->Role of Security in Social Networking
2. <https://www.researchgate.net/-> A study of Cyber Security challenges and its

emerging trends on latest technologies

1. https://csc.sjtu.edu.cn/doc/- Influence Analysis on Social Networks
2. <https://ieeexplore.ieee.org/-> An analysis of Security in Social Networks