# Social Network Security Issues

Sulabh Negi

Shubham Verma

Birjesh Kothari

**ABSTRACT**

**Purpose-**The purpose is to find the risk related to social sites and help the organisation to handle the security related to their social media more efficiently

- A survey on the security issues on social media that affect every user.
- Risk arises when we share data on social media.
- Solution discussion on the risk associated with risk related to social media.
- How we can reduce the risk on social media by implementing new techniques.

**Methodology-**In this paper we have mention the better way of handling security risk by studying various data from net, book .

**Finding-** security techniques of most of the organisation are not strong enough to prevent user data.

**Keywords-**user, risk, social media, techniques, security.

## I.INTRODUCTION

A social media is web service that allow people to connect on the internet and share their thought, personal details and other things.

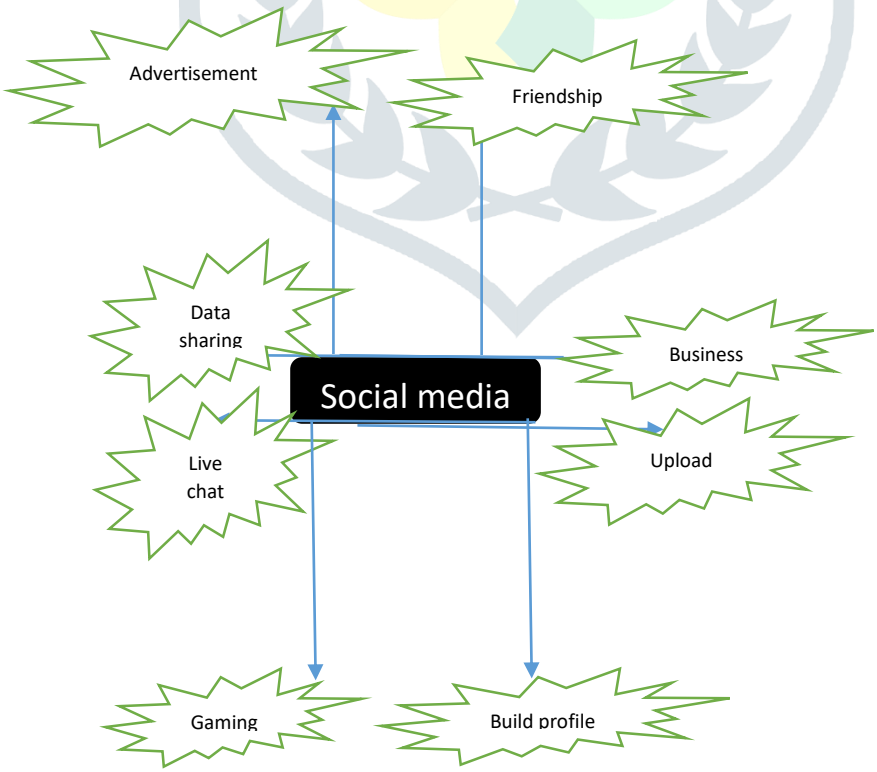


**Fig 1-** features of social media

- Data sharing is the most important feature of social media.
- In many SNSs, such as Facebook, mainly multimedia data is produced and shared.
- This statistic shows a timeline with the worldwide number of monthly active Facebook users from 2008 to 2018. As of the third quarter of 2018, Facebook had 2.27 billion monthly active users

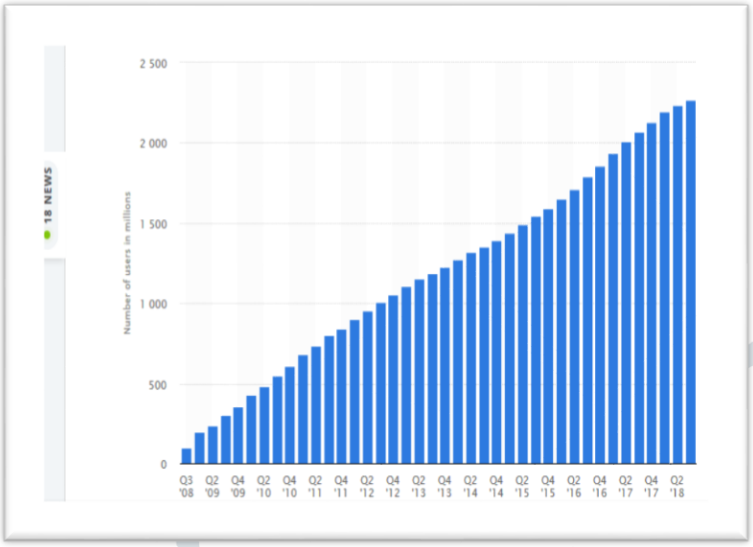


**Fig 2- number of active user in millions till 3rd quarter of 2018**

- There in increase in average viewing of data on social media every day. In 2018 8 billions of videos are viewed per day which is double of which are viewed in 2015.
- Huge amount of data availability on fb security risk are also very high.
- When a survey is conducted (in 2011), by Pew Internet Research, discussed in Lee Rainie and Barry Wellman's *Networked – The New Social Operating System*, illustrates that 'networked individuals' are engaged to a further extent regarding numbers of content creation activities and that the 'networked individuals' are increasing over a larger age span.
- Pew Internet Research conducted survey in (2015) shows that the Internet users among American adults who uses at least one social networking site has increased from 10% to 76% since 2005.
- List of the leading social networks shows the number of active users as of July 2018.[1]

| # | Network Name | Number of Users (in millions) |
|---|---|---|
| 1 | Facebook | 2,989 |
| 2 | YouTube | 1,900 |
| 3 | WhatsApp | 1,500 |
| 4 | Facebook Messenger | 1,300 |
| 5 | WeChat | 1,040 |
| 6 | Instagram | 1,000 |
| 7 | QQ | 806 |
| 8 | QZone | 563 |
| 9 | Tik Tok | 500 |
| 10 | Sina Weibo | 411 |
| 11 | Twitter | 336 |
| 12 | Reddit | 330 |
| 13 | Baidu Tiba | 300 |
| 14 | Skype | 300 |
| 15 | LinkedIn | 294 |
| 16 | Viber | 260 |
| 17 | Snapchat | 255 |
| 18 | Line | 203 |
| 19 | Pinterest | 200 |
| 20 | Telegram | 200 |
| 21 | Tinder | 100 |

Fig 3- number of users of most popular social media.

# II.RESEARCH METHODOLOGY

## Social media security issues

There are many security risks that target social media. For a little more information on how easy it is to create a social media security risk take a look at this article in The Next Web.To get more insight into this area, be sure to talk with your IT department. In fact, an IT representative should be on your Social Media Governance Team and should be bringing these to your attention.
Read more at https://www.business2community.com/cybersecurity/7-social-media-security-issues-business-faces-02024378.

## Some common social media security issues

- **Phishing & Brand Impersonation[2]**

  Phishing typically involves setting up a website that resembles that of the company whose customers are targeted as part of the phishing attack. The idea is to convince the individuals that the website belongs to the trusted company, such as the person's bank, so that the victim reveals sensitive information (such as login credentials, credit card information, etc.)

- **Forgetting to Log Out[3]**

  Increase the security of your social media account by always logging out when you step away from your laptop or computer. It's best to go one step further and close down the browser you were using to view your account. If you leave your account logged in, you set yourself up to be hacked because anyone who can get to your computer can access your account, change the password or even post items and communicate with your friends as if they are you. Logging out and shutting down the browser is even more important if you use a public computer.

- **Clicking on Enticing Ads[3]**

  Viruses and malware often find their way onto your computer through those annoying, but sometimes enticing ads. However, on the Web, just like in real life, if an offer seems too good to be true, then it probably is. Save yourself a potential security headache - don't click.

- **Profile Cloning[4]**

  Profile cloning can be done manually or automatically. Manually means that someone copies all available information from another profile and then create a new profile. Automatic method requires a written script and that the social networking service allow scripts' execution. The latter is allowed in Facebook and LinkedIn.

- **SQL Injection [5]**

  SQL injection is a technique in which unauthenticated user manipulate database of some sites with the help of sql statements.

  This technique is mostly use for hacking websites.

---

SQL in web pages

In sql injection some malicious user enter some sql queries in the field in which were made to enter data such as username, passwords etc. And these code are running without developer of that website knowing it.

This following example which creates a SELECT statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):

**Example**

```
txtUserId = getRequestString("UserId");
txtSQL = "SELECT * FROM Users WHERE UserId = " + txtUserId;
```

## Techniques to reduce social media security risk

**1. Response Application Architecture should be used.**
It is an architecture in which to different database is used to store data of user and user can decide that whose request he want to accept or reject, And user have the authority that which portion of the information he will show to his friends.

**Benefits of architecture**

User can hide his information from unwanted user and he can customize his profile in different manner.

**Limitations**

Profile cloning cannot be prevented using this kind of architecture. So user should be careful to whom he is making his information visible.

We can prevent sql injection using prepared statements.[5]

**2. Prepared Statements and Bound Parameters**

As we know that most of the social media are developed using php language and uses database to save their user information so in order to prevent sql injection instead of using simple sql statement developer should use prepared statements and bound parameters to develop web applications.

A prepared statements are those which are similar to sql statement but are executed with high efficiency.

Prepared statements work like this

Prepare: An SQL statement template is created and sent to the database. Certain values are left unspecified, called parameters (labeled "?"). Example: INSERT INTO verma VALUES (?,?,?)

The database parses, compiles, and performs query optimization on the SQL statement template, and stores the result without executing it

Execute: At a later time, the application binds the values to the parameters, and the database executes the statement. The application may execute the statement as many times as it wants with different values

**Prepared statements have 3 advantages over sql statements:**

- Parsing time is reduced by using prepared statements.
- We have to only send parameter not the whole queries so the bandwidth to the server is minimized
- Prepared statements are very useful against SQL injections, Because If the original statement template is not derived from external input, SQL injection cannot occur.

- To prevent profile cloning on websites organisation should introduce a feature in which while creating your social media profile user have to attach their real identity card with account so that no other can clone the profile of original user. This will anyone to identify the real user and fake account cannot be made by introducing these features.

- Organisation should filter the advertisement and check them for any malware or viruses before they are attach to their sites so that there is no chance of account hacking even if user accidentally click the add. They should develop an application which can check for any embedded code of malware with any advertisement.

- An feature of automatically logout should be introduced if user closes the browser or there is not any activity by user on the particular sites this will help user when they forget to logout from their account.

## III.CONCLUSION

Social media is very helpful for an organisation as it help in communicating with the employee, customers etc. but this also increase the risk of publishing the confidential detail online and downloading malware. To reduce this risk a survey of all employees must be carried out and then the application is developed according to the usage behaviour of employees so that we can introduce security parameter according to employee mean what are the important feature which is necessary for user will only be included no additional features are added.

# IV.ACKNOWLEDGEMENT

We take this opportunity to express our sincere gratitude to all those who helped me in various capacities in undertaking this project and devising the report.

We are privileged to express our sense of gratitude to our respected teacher Mr **PARAG VERMA** whose unparalleled knowledge, moral fibre and judgment along with his knowhow, was an immense support in completing the project.

We are also grateful to

Mr **Sumit Chaudhary** the Head of Department,

Computer Science, for the brainwave and encouragement given


## V.References


[1] en.wikepedia.org

[2] Jane church (business2community.com/cybersecurity)

[3]Charlie R. Claywell Web Designer (https://socialnetworking.lovetoknow.com/Security_Issues_With_Social_Networking_Sites)

[4] Bolton, R.J. and Hand, D.J. 2002. Statistical Fraud Detection: A Review.

Statistical Science. 17, 3 (2002), 235–249.

[5] www.w3school.com