Facebook Spoofing and Messenger Calling

Akash Shitole
Student at Ajeenkya D. Y. Patil University
Guided by: Sneha Ambhore, Inurture Education Solutions, Banglore, Karnataka

Abstract- The rapid growth of users on social network has created an opportunity for communicating worldwide. More than a billion users have come together to share their information with each other and effectively make new friends and connect all over the world. However, we find evidence of members misusing this social network website. We also find that users are concerned about their privacy over social network website and trust their ability to control the information they provide to the website. Facebook also provides two mobile applications to communicate efficiently which are Facebook and Messenger. Although some users are using this application for disturbing other user's privacy and intruding their personal space. Due to some of these users, other users tend to close their Facebook account or prefer to use it less and restrict their information to be provided to the community due to privacy concerns.

Keywords- Facebook, Social network, Messenger.

I. INTRODUCTION

Modern ways of communication have their own risk of having one's confidential information being stolen and having their privacy disturbed. In recent times, we have noticed that such risks have gone up several times more than usual. We have noticed that users are creating multiple accounts by entering fake information and manipulating other users. In 2011 Facebook came up with an instant messaging application called the Facebook Messenger. Since then Facebook Messenger has become one of the most used instant messaging mobile application in today's world. However, we have found evidence that users are using the Messenger application provided by Facebook for directly contacting unknown users and intruding their personal space by calling them.

II. LITERATURE SURVEY

Stephanie A.C. Schuckers [1] describes different researches happened at West Virginia University regarding spoofing and anti-spoofing measures. Different anti-spoofing measures can be developed and implemented to drastically decrease the chance of any spoof attacks. More testing and implementation of these measures needs to be done to check and increase the effectiveness against spoof attacks. Katharina Krombholz [2] conducted a social engineering experiment on Facebook to collect information about the success of integration of fake profile into an existing friend network. They demonstrated their work through conducting a survey by creating various fake accounts and getting mixed up with an existing friend network. After conducting the survey, they were able to conclude that most of the fake profiles are the ones that do not exhibit social activities and also high number of friends are identified to be fake profiles than that of those who manifest social activities and interactions with others. In addition to that, they were also able to analyze Facebook users' privacy considerations and establish a connection between a fake user and authenticate user.

In recent times there is a drastic increase in the number of fake profiles created over the website and a lot of attacks have been happened through those fake profiles. Due to rapid growth in technology newer ways of spoofing are coming into display. Although risk of such attacks can be analyzed using various tools.

III. FACEBOOK SPOOFING AND MESSENGER CALLING

a. FACEBOOK SPOOFING

Lately the number of cybercrimes committed have been increased drastically. Social networking websites play a huge role in these crimes. People often tend to use social network to gather information about various organizations through connecting with some inside people in that organization and manipulating them into giving away the information. One of the most happening attack over social network is Spoofing. In context of information security, spoofing attack is a situation in which a person or a program disguises as another by falsifying data, to obtain illicit data.

In this paper, we did survey analysis to study the various possibilities through which user data and privacy is compromised. We surveyed number of Facebook members at our local area. In particular, we looked for member who are having trouble over social networking website and also have concerns regarding security of their data. While conducting the survey we asked various people if they used Facebook and if they would like to use it to which their response was "Facebook? Is it safe? Is your data safe there? we have heard people use fake accounts to manipulate, is it true?". No one is pressurized to join Facebook or use Messenger or any social network website or application and most of them endorse, but not pressurize users to give some of their personal details

Facebook spoofing is one of the most happening attack in today's world. we often see users having multiple accounts and making it difficult to know which one is legitimate. Regardless of that the problem arises when these users create multiple accounts by falsifying their details and then engaging in social activities. These users contact other users which are completely unknown to them and manipulate them and steal their information. Users have no idea if the person he/she is talking to isn't the person he/she think they are. Through spoofing users can be easily hacked or targeted into something they haven't done.

b. MESSENGER CALLING

Video calling has become an essential part for communicating with our loved once no matter where they are. Many social networking websites and applications offer video calling feature. Messenger application is a one of the most used application worldwide for communicating worldwide with more than billion users actively communicating with each other but at the same time there are some users that are misusing this application.

We have verified that through Messenger users can make normal calls or video calls to random unknown users without adding them as friends. This is a huge problem regarding the privacy concerns of the users as random unknown people are calling them. This can lead to many cyber-attacks such as social engineering, phishing, eavesdropping, etc. which can cause many problems to the victim. Any user active on Messenger will receive calls these calls made by the attacker.

IV. PROPOSED SOLUTION

a. FACEBOOK SPOOFING

Spoofing has become a major problem over Facebook and many other social network websites. Users are unable to recognize real and fake accounts due to the accuracy of faking details. However, we have come up with a solution for this problem.

The solution is that every user should give some unique valid identification detail like passport number or driving license number. At the same time the website should be able to verify the details given by the user by connecting to the respective organization handling the information. Each identification detail provided can be used to access only one account. After providing the identification details, other details like name, date of birth, hometown should be auto-filled in order to prevent faking details and should not be editable.

If a user wants to create more than one accounts the user will require another identification detail and the website should be able to connect to that respective organization handling the details as well. Even if the user is creating other account using some other identification, the user should be prompted with a message saying 'you already have an account with another identification detail. Would you still like to continue?". If the user says no, the page should redirect to login page and if user says yes, the rest of the details should be automatically filled. In addition to these features, if a user is creating a second account the first account should be visible in the second account as a friend and should be visible to other users at all times to let other users know if the user contacting them is a genuine one. The website should be able to cross-link between multiple identification details of each individual user.

b. MESSENGER CALLING

One of the most used instant messaging (IM) application in the world is Messenger. It has played a major role in connecting people to the other side of the world. However, as it has so many features, it has also a tiny flaw which is being misused by many users nowadays. The feature which is being misused is the calling feature. The calling feature is an undoubtedly important feature but at the same time this feature has a flaw which is any user across the globe can search your name in the messenger search bar and directly call you over the application despite not knowing each other and at the same time also not being friends on Facebook. We have come up with multiple solutions for this vulnerability of the application. The following solutions are:

a. The application should create a calling request bar similar to the message request bar where all the users who are not authorized to call you will be held on stand until the user accepts the calling request. Also, this feature should have option like 'accept calls' and 'ignore and block' or 'report'. If the user rejects the call request for more than three times the other user trying to call will be automatically blocked and reported for further actions to be taken.

b. For the other solution, the website can create an option similar to 'who can see your friend list' in the privacy setting. This option can be named as 'who can call you directly' and four options should be provided saying 'no one, friends, friends of friends and everyone'. This will help in controlling the number of users allowed to call you directly.

c. Both the above solution can also be combined to create a more effective and efficient security options that will help users in protecting their privacy and their personal time and space.

TABLE

In the second quarter of 2018, a number of media articles have published reports regarding the fake profiles on Facebook. After analyzing the data collected, we came to an approximate value of 2.25 billion monthly active users (MAUs) and an immense 1.49 billion daily active users (DAUs).

In the third quarter of 2018, New York times published an article saying that from October 2017 to March 2018, Facebook has deleted over 1.35 billion fake accounts. After doing the math we find that the number of fake profiles on Facebook is almost 60% of the total users active which leads to a total of 900 million MAUs and 894 million DAUs after removing the 60% fake profiles.

Note: values mentioned are approximate values.

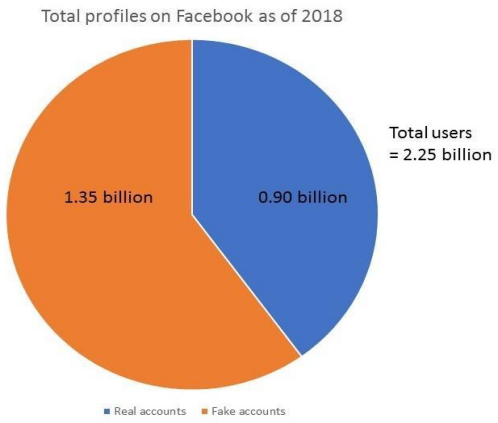

Fig.1:

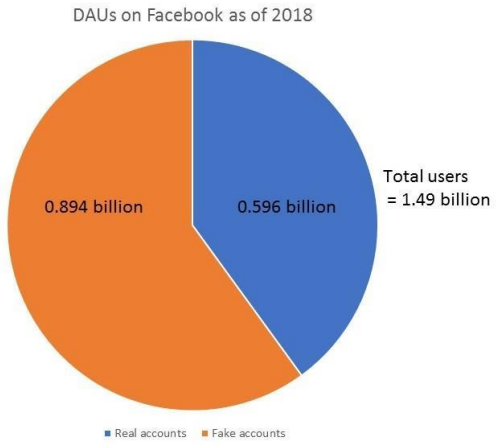

Fig.2:

V. CONCLUSION

We observed that there are various fake profiles over social networking websites. These fake accounts are usually less-active users or friends over a friendly network. These fake profiles use various social engineering methods to gain information about the victim and misuse them in many ways. We concluded that on Facebook 60% of the accounts back in third quarter of 2018 were fake accounts. We also proposed solution for this problem to make it difficult for attacker to perform spoof attacks over the website.

We conducted an experiment on Facebook Messenger application by random users being added in friend list. This problem leads to disturbance in Messenger application. We also provided multiple solutions for this problem to help increase the privacy of user over this application.

VI. REFERENCES

[1]. Stephanie A. C. Schuckers, Ph.D. Clarkson University and West Virginia University, "Spoofing and Anti-Spoofing Measures", Information Security Technical Report, Vol 7, No. 4 (2002) 56-62

[2]. Krombholz, K., Merkl, D., & Weippl, E. (2012). "Fake identities in social media: A case study on the sustainability of the Facebook business model". Journal of Service Science Research, 4(2), 175–212.doi:10.1007/s12927-012-0008-z.

Akash Shitole is pursuing his Bachelor's Degree in Computer Application that specializes in Cloud Technology and Information Security. He has interned with Hewlett Packard Enterprise (HPE) and Kyrion Technology for Artificial Intelligence and Ethical Hacking. His interest in technology helps him to work hard in the corresponding field.