CAPITAL UNIVERSITY OF SCIENCE AND
TECHNOLOGY, ISLAMABAD

A Technique for Identification of Information Severity Levels for Facebook User Profiles

by

Hamza Masood

A thesis submitted in partial fulfillment for the
degree of Master of Science

in the

Faculty of Computing
Department of Computer Science

2022

Copyright © 2022 by Hamza Masood

All rights reserved. No part of this thesis may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, by any information storage and retrieval system without the prior written permission of the author.

This work of research is dedicated to my family members and my dear teachers, who helped and supported me through the times of hardship.

CERTIFICATE OF APPROVAL

A Technique for Identification of Information Severity Levels for Facebook User Profiles

by

Hamza Masood

(MCS183031)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Raja Habib	UoL, Islamabad
(b)	Internal Examiner	Dr. Amir Qayyum	CUST, Islamabad
(c)	Supervisor	Dr. Qamar Mehmood	CUST, Islamabad

Dr. Qamar Mehmood
Thesis Supervisor
June, 2022

Dr. Nayyer Masood
Head
Dept. of Computer Science
June, 2022

Dr. M. Abdul Qadir
Dean
Faculty of Computing
June, 2022

Author's Declaration

I, **Hamza Masood** hereby state that my MS thesis titled "**A Technique for Identification of Information Severity Levels for Facebook User Profiles**" is my own work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad.

At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my MS Degree.

(Hamza Masood)

Registration No: MCS183031

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "**A Technique for Identification of Information Severity Levels for Facebook User Profiles**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS Degree, the University reserves the right to withdraw/revoke my MS degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

(Hamza Masood)
Registration No: MCS183031

Acknowledgement

I am grateful to the Almighty ALLAH(SWT), by the blessings of Whom i could accomplish my goals. Whatever the difficulty I have faced in my life, ALLAH provided me with the strengths to overcome that difficulty and achieve the goal. Secondly, I am Thankful to my parents for always being supportive in my whole educational and professional career. Further, I would like to thank those who helped me in achieving this goal and completing this task. I would like to thank my thesis supervisor Dr. Qamar Mehmood who supported me throughout the period and pointed me in the right directions, whenever I got stuck. I am grateful to him for helping and guidance. His suggestions and guidance helped me in completing the thesis.

(Hamza Masood)

Abstract

In the present era, social media platforms play an important role in connecting people from all around the world. People share their daily life routine, and their personal information with others by posting it on their profile. Where these platform provide such facility to connect and share your thoughts and beliefs with the rest of world, there is also a dark side. With this much personal information, present online and easily accessible to different groups of people, the social media becomes a information repository for the hackers and stalkers. Many hackers use social media platforms to gather personal information about their victim and then launch a cyber-attack such as phishing attack. People can easily become a victim of social engineering attack on a social media because of oversharing of their personal information and not setting the proper privacy configuration. This study highlights the problem with oversharing of publicly accessible personal information on social media platform such as Facebook. It focuses on, how a person can become a victim of social engineering attack just by oversharing the publicly accessible information. This study proposed a system to calculate the severity of publicly available information on Facebook user profile, with respect to cyber-attacks. It also provides a scale for the severity assessment of different types of information found publicly on a Facebook user profile. for comparison, field experts are also engaged to assign a severity score according to their understanding. For instance, the contact information that is usually found on Facebook user's profile, is rated to be highly critical by 50% of the experts. After collection of the results from the experts, the scores were compared with the results generated by the proposed system. It is found that, there is only 12% difference in the severity score of contact information that is generated by the system and assigned by the experts. In the end, an implementation of the idea is also proposed using android development environment.

Contents

Author's Declaration iv

Plagiarism Undertaking v

Acknowledgement vi

Abstract vii

List of Figures xi

List of Tables xii

1 Introduction 1
- 1.1 Introduction to Domain . . . 1
  - 1.1.1 Social Media Platforms . . . 1
  - 1.1.2 Social Activism and Hacktivism . . . 2
  - 1.1.3 Impacts of Social Media on Politics . . . 2
  - 1.1.4 Impacts of Social Media on Society . . . 3
  - 1.1.5 Facebook: Privacy and Security . . . 3
  - 1.1.6 Scraping Facebook Profile Information . . . 4
  - 1.1.7 Social Engineering Attack . . . 4
- 1.2 Motivation of Research . . . 5
- 1.3 Profile Information Leakage . . . 5
- 1.4 Social Engineers . . . 6
- 1.5 Sufficiency of Research Topic to Qualify as MS Thesis . . . 7
- 1.6 Severity of Publicly Available Information . . . 7
- 1.7 Problem Statement . . . 8
- 1.8 Research Questions . . . 8
- 1.9 Methodology . . . 9
- 1.10 Major Contributions . . . 9
- 1.11 Thesis Organization . . . 9

2 Literature Review 11
- 2.1 Survey of Existing Techniques . . . 11
- 2.2 Conclusions from Literature Review . . . 18

2.3 Comparative Analysis and Survey of Existing Techniques 19
2.3.1 Methodology and Dataset 19
2.3.2 Information Type 20
2.3.3 Results 21
2.3.4 Limitations 24
2.4 Identified Research Gaps 25

3 Proposed System **26**
3.1 Introduction to the System 26
3.2 ENISA Methodology to Calculate Personal Data Breach Severity . 27
3.2.1 Recommendations for Scoring the Equation Parameters . . . 28
3.2.2 Data Processing Context (DPC) 28
3.2.3 Ease of Identification (EI) 28
3.2.4 Circumstances of Breach (CB) 29
3.3 Research Methodology 30
3.3.1 Experimental Methodology 30
3.4 Information Collection from Facebook Profiles and Legal Concerns . 31
3.5 Architecture Diagram 32
3.6 Assigning Information Severity Scores by Field Experts 33
3.7 Methodology Diagram 34

4 Experiment and Results **37**
4.1 Experimental Setup 37
4.1.1 Choosing the Appropriate Social Media Platform 38
4.1.2 Proxy Settings of Profile Information on Facebook User Profile 38
4.1.3 Public 38
4.1.4 Friends 39
4.1.5 Friends Except 39
4.1.6 Specific Friends 39
4.1.7 Only Me 39
4.2 Information Types and Presence on Facebook User Profiles 39
4.3 Severity Scores of Information by Field Experts 40
4.4 Severity Scores of Information by Public 41
4.5 Questionnaire Contents 41
4.6 Scoring the Information Using the Proposed System 42
4.6.1 Information Presence Check 43
4.6.2 Information Categorization 43
4.6.3 Ease of Identification Scoring 44
4.6.4 Scoring Circumstances of Breach 44
4.6.5 Calculating the Final Score for Each Information Type . . . 46
4.6.6 Results of Proposed solution 47
4.6.7 Comparison of the Scores with Expert Scores 47
4.7 Results of Questionnaire 48
4.7.1 Average of Severity Scores from Experts 55

4.8 Scoring of the Information Types by General Public 56
4.8.1 Average of Scores Assigned by Public 57
4.9 Comparison of Proposed System Results with Experts' Results . . . 63
4.9.1 Percent Difference 63
4.10 Inter-rater Agreement 65
4.11 Recommendations 66

5 Implementation of the Proposed System **69**
5.1 Introduction 69
5.2 Implementation Technology 69
5.2.1 Android Studio 70
5.2.2 JAVA 70
5.2.3 XML 70
5.3 FACEBOOK Graph API 70
5.4 Interfaces of the Application 71
5.4.1 Login Screen 71
5.4.2 Information Screen 72
5.5 Further Working of the Application 73

6 Conclusion and Future Work **74**

A Questionnaire Design for Experts **76**

B Questionnaire Design for Public **81**

Bibliography **82**

List of Figures

1.1 Causes of Phishing attacks 5

3.1 Architecture diagram of proposed system 32
3.2 Methodology Diagram for Expert's Scoring 34
3.3 Methodology diagram of proposed system 35

4.1 Q1: for Expert 51
4.2 Q2: for Expert 51
4.3 Q3: for Expert 51
4.4 Q4: for Expert 52
4.5 Q5: for Expert 52
4.6 Q6: for Expert 52
4.7 Q7: for Expert 53
4.8 Q8: for Expert 53
4.9 Q9: for Expert 53
4.10 Q10: for Expert 54
4.11 Q11: for Expert 54
4.12 Q12: for Expert 54
4.13 Q1: for Public 59
4.14 Q2: for Public 59
4.15 Q3: for Public 59
4.16 Q4: for Public 60
4.17 Q5: for Public 60
4.18 Q6: for Public 60
4.19 Q7: for Public 61
4.20 Q8: for Public 61
4.21 Q9: for Public 61
4.22 Q10: for Public 62
4.23 Q11: for Public 62
4.24 Q12: for Public 62
4.25 Percentage difference of the two results 64
4.26 Inter-Rater Agreement of the experts 66

5.1 Screen 1: Login Screen 71
5.2 Screen 2: Information Screen 72
5.3 Screen 3: Information with scores 73

List of Tables

2.1 Methodology and Dataset of previous researches 20
2.2 Information type 21
2.3 experiment results of Pinchot [14] 22
2.4 Percentage of people who revealed the Information 23
2.5 Results of Baatarjav [34] 23
2.6 results of Farahbakhsh et al. [21] 24

4.1 Categories of Information type 43
4.2 Consequences of data breach 45
4.3 Scores of proposed solution 47
4.4 Professions of Field Experts 48
4.5 Field of Work of Experts 49
4.6 Scores of experts 50
4.7 Average of scores of experts 55
4.8 Scores of public 57
4.9 Average of scores of public 58
4.10 Average of scores of public 63
4.11 Inter-rater agreement of experts over each information type 65

Chapter 1

Introduction

1.1 Introduction to Domain

With every passing day, more and more people are connecting to internet with the help of their personal devices i.e., smartphones, PC etc. Now as the internet has become the biggest source of information, it has also provided many new facilities and innovative technologies to the end user such as electronic mail, video calling and instant messaging etc. Among these new facilities one of the most innovative facility that has become most popular is social networks.

1.1.1 Social Media Platforms

Social networks also known as social media platforms allow people to manage and establish relationships with others including their own family and friends. World has become a global village where thousands of people sitting in far places meet and greet each other using the social networks on daily basis, as if they are sitting near to each other. It also allows people to know each other and make new friends. Since the release of these social platforms, many new features are added in it day by day such as managing online businesses and having group chats etc. By the use of these features, social media has become more interesting and fun to use.

1.1.2 Social Activism and Hacktivism

Where the social media provides this much advantage in connecting and sharing knowledge with each other. It can also be used to spread false news and rumors to support and motivate any social or political agenda. The process of misusing the technology such as computer networks to spread and support a social and political cause is known as hacktivism. With the concept of hacktivism another concept named as social activism is linked. Social activism is the action or series of actions that could be taken promote and bring a social change. With the use of social media platforms, social activism has become more effective. When people share their thoughts on something using the social media, it is seen by almost all of the people connected and it leaves an impression on them.

1.1.3 Impacts of Social Media on Politics

During the period of political elections, different parties use their social media profiles to post about their success and future plans. They also use these profiles to post about the works their party members do in their region. Such type of information sharing can be used to build the image of different parties in people's mind. For example, people share the negativity happening in their surroundings and also spread love by sharing positive things happening in their surroundings. With these acts, almost everyone that uses social media gets to know the happening in the world, even if they are sitting in far places.

A study found that two in every ten U.S adults use social media to get their political news. And those people tend to be less-informed and are very likely to be exposed to claims that are not proven by anyone.

In history social media has played an important role in political elections. First, such incident happened in the elections of 2003 with "Howard Dean", then in the elections of 2008 [1] and then in the elections of "Donald J. Trump" which was almost driven by twitter. Same like this, There are many examples present in

[1] https://www.simplilearn.com/real-impact-social-media-article

literature, that show and demonstrate the use and role of social media platforms in society.

1.1.4 Impacts of Social Media on Society

According to a study nearly 80% of the U.S. population[2], who is on internet, are user of Facebook. As the social media causes people to interact with each other, their bonding and friendship becomes more powerful as long as they stay connected. Anyone who is on this platform is never alone. And when they find each other, they share knowledge, social issues, raise voice against wrong and promote the good. Even a little act of kindness is appreciated by almost everyone on the platform.

1.1.5 Facebook: Privacy and Security

Facebook is a social platforms that allows content sharing and making personal profile, where you can add your personal information such as name, contact, job and residence etc. This information helps to build the identity of a user so that people can know each other even better.

In addition to the personal information one can also share and exhibit the interests he/she has, such as music, movies, favorite singer and actor etc. While creating a profile in Facebook, one has to provide complete personal information. The personal information includes Full name, Date of birth and contact information etc. so it can be said that the profile of a person on Facebook reflects the actual personality of that person in real life. All the personality traits, that a person exhibits in real life, such as his liking disliking can be known from social media platforms.

Hundreds of people join Facebook on daily basis. Where it provides such great facilities and features, it can also be dangerous with respect to personal data privacy. In this era. Where privacy issues and cybercrimes are getting popular.

[2]https://www.simplilearn.com/real-impact-social-media-article

Many hackers on the internet use these social platforms to perform and land several types of attacks for the sake of their own good. For instance, a hacker can manipulate a person online to gain his/her trust. After gaining the trust of the victim the attacker could potentially blackmail the victim or maybe use the extracted information to perform password recovery attacks. People with malicious intents can extract the information given by people on their social media platform profiles to perform cybercrimes such as social engineering attacks.

1.1.6 Scraping Facebook Profile Information

Scraping Facebook refers to finding and collecting different types of information from Facebook. Now to perform some analysis on information found on Facebook, it is better to first find and collect that information from Facebook. Similarly, to find what type of information is publicly available on profiles of Facebook and to find the sensitiveness of that information. The problem with scrapping is that, it is now considered illegal, so an alternate is used that is discussed in section 3.4.

1.1.7 Social Engineering Attack

Social engineering attacks depend on social interaction between humans. In this type of attack people are reached and manipulated into disclosing their personal information. That information can later be used to perform damage to the people or organization they work in. Social engineering attack has many types, i.e., baiting, spear phishing and phishing attack etc. A type of attack in which hacker attempts to extract personal or sensitive information from his victim by luring the victim into a trap such as fraudulent email or phone call, is called phishing attack. Figure 1.1 shows the demonstration of causes of social engineering attack: phishing attack. Figure demonstrate, that phishing attacks can be launched by the use of imposter calls, emails, unsafe browsing and social media platforms. Once an attack is launched on a victim, the data can be stolen and leaked or even used in any malicious activity.

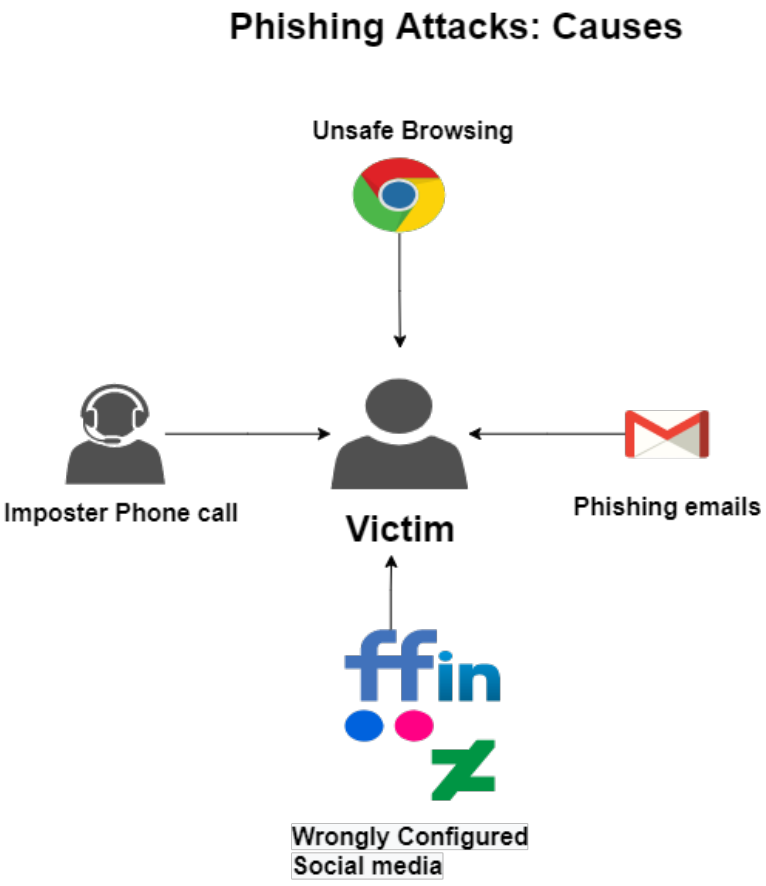


FIGURE 1.1: Causes of Phishing attacks

1.2 Motivation of Research

As discussed in the previous section Facebook has opened many doors to being attached with the rest of the world. People share a lot of information in daily basis on this platform. Because of the information being posted on daily basis, Hackers and attackers get attracted to this platform to perform many types of Cyber attacks such as social engineering attack for their personal benefit.

1.3 Profile Information Leakage

People using social platforms such as Facebook provide many types of information on their profiles (i.e., job location, job position, current city, check in etc.) that could lead them to be a victim of social engineering attacks.

Attackers often use social platforms to extract some useful information regarding their target organization/person and to find the right person to start the attack with. There are many social engineering techniques available such as phishing emails, phone calling and instant messaging that can be useful in persuading a user to disclose his/her personal information. Anyone with no knowledge of social engineering can be tricked in disclosing the personal and sensitive information.

Now that this issue has become very important, and in recent years many updates done to Facebook have restricted their users to only provide real and valid information. So, the profile on the Facebook represents the actual personality of a user.

Social media platforms have become the most popular medium for communication among people. It attracts hundreds of users on daily basis and allows them to share their personal thoughts and express their feelings. People on social media can also share their photos, videos and personal information such as their liking and disliking etc.

1.4 Social Engineers

With this much popularity that these social networks have gained. They have also become a hunting ground for many cybercriminals. Among these criminals, social engineers are the ones who take the most advantage from these networks. Reason being the information richness of these networks. To land a successful phishing attack on a specific person, the attacker needs information about that person. If the victim has a profile on a social platform such as Facebook, there is a high chance that the victim has disclosed some of his personal information on his/her profile. So, the attacker can extract the required information and can land a direct phishing attack. This phenomenon is also known as the social media phishing. The following research will be done by keeping in mind the possible scenarios where social engineering attack can be launched by using the information which is available with public privacy settings on social media profiles.

1.5 Sufficiency of Research Topic to Qualify as MS Thesis

This research addresses the issue of confidential information privacy. Basically, when people trust too much on this social network and provide sensitive information such as their name, contact, job place, residence area, education and educational institute they become vulnerable to being a victim of cyber attack such as social engineering attack.

1.6 Severity of Publicly Available Information

Each type of information that is publicly available has its own importance with respect to social engineering attacks. For example, if an attacker wants to know the secrets and working of an organization, then in this case the information related to job and workplace of people is important. Because then it would be easy to find the employees of that organization . In case of an attacker that wants to target the specific person, then the aim of the attacker would be to find the friends and family or even the contact information of that individual and start the attack. So, calculating the information severity levels is a main task of this research.

If an attacker has to know about the infrastructure of an organization, the attacker needs information about how the organization manages and organizes the infrastructure. To get inside the system he needs information about that system and how it works. And no one knows that except the actual employees that work there.

So, the basic step, the attacker will take is to get in touch with someone from that specific organization. And as described earlier if anyone from that organization is on Facebook and he has given the information regarding his job and job place. He can be a victim in such a way that the attacker can pretend to be a kind person and over a period of time the attacker might gain enough trust, that the victim would not hesitate to disclose the organizations secrets and the working of

its system. And that specific information could be enough for the hacker/attacker to get inside the system of the organization.

Just like the example explained above, there can be many applications like targeting a person with the help of gaining the trust of someone from the victim's family or even find contact information and land a direct phishing attack.

In the light of above examples, the aim of this research is to find out the type of sensitive information that people disclose publicly on the social network, specifically on Facebook, that leads those users to being a victim of social engineering attacks. This research will also calculate the severity of information that is available on people's profile.

1.7 Problem Statement

People that use social media platforms often provide personal and sensitive information on their profile publicly. A hacker can access this information and use it perform a cyber attack such as social engineering attack.

1.8 Research Questions

The problem statement described above raises some important research questions, that should be answered. The research questions, raised by the problem statement are as follows:

Q1: How many people are aware of the severity of information that they make public on Social media on daily basis?

Q2: How publicly available information can be exploited to perform a social engineering attack against the users?

Q3: What are the severity levels of information found publicly on social media profiles that may cause the social engineering attack?

1.9 Methodology

To provide a solution of the problem discussed above an appropriate methodology is required. For this, the Experimental research methodology is chosen as the research methodology, where an experiment is performed and results are generated. The results are then further compared with the results that are provided by the field experts with the help of a questionnaire. Once the results from the questionnaire are collected, they will then be compared with the results that are generated by the proposed system and a final conclusion will be given.

1.10 Major Contributions

The major contributions of this thesis are:

1. A scale for calculating the severity of publicly available information on Facebook user profile is provided.
2. Understanding of experts regarding the severity scores of publicly available information, with respect to social engineering attacks is presented.
3. Similarly the understanding of general public is also provided.
4. Comparison of severity scores calculated by proposed system with the scores assigned by experts.
5. Development of android application of the idea to calculate the severity of information on Facebook user profiles.

1.11 Thesis Organization

This whole document is divided into 6 different chapters. In the chapter one, background knowledge and domain introduction are discussed along with the problem statement and the brief introduction to the methodology.

Chapter two of this document contains the literature review. After the literature review is done the conclusion from the literature review and the research gaps are highlighted.

In the chapter three of this document, research and methodology is discussed in detail. The diagrams related to methodology and the architecture of the proposed system is added and their explanation is given.

The chapter four is written in accordance with the proposed system, where the complete experimental setup and results are explained. The whole explanation of how the results are obtained and the comparisons are provided in this chapter.

Chapter five contains the description and explanation of the implementation of the proposed system. How the implementation is done, which technologies are used, the suitable platform, everything related to implementation point of view is discussed in this chapter.

The chapter six is about the conclusion and future work. The directions of work in future and how the proposed system has performed is discussed in the chapter.

Chapter 2

Literature Review

To identify the research gaps and the work that is previously done a comprehensive literature is done. After the literature review the research gaps are identified and the limitations of previous studies are highlighted .

2.1 Survey of Existing Techniques

To understand the working of social engineering in social networks. It is necessary to understand the factors and properties that influence the attackers to attack a specific person on social network such as Facebook. These factors are also important to measure the user's openness to phishing attacks. The study proposed by [1] in 2018 proposes a framework by which a user's openness to such attacks can be understood more easily.

Another research in 2017 stated that even if people don't want to provide the personal information on their profiles. It can be extracted or judged by their public behavior on that network. They presented a technique by using which undeclared information of a person can be inferred from the data present on their public profile [2].

A study done in 2020 on social engineering and phishing attacks suggests and demonstrate, how an attacker approaches his victim. With the help of survey

this study summarizes, how a user is persuaded in disclosing his/her personal and sensitive information. The survey also discussed some preventive measures to avoid and detect a phishing attack [3].

To land a phishing attack on social media platforms, the attacker needs information. Once the attacker has sufficient information the attack becomes easy. For extracting the information from social networks, one could go manually and extract the required information or simply use a mining tool. Many such tools that can be used to mine the data and analyze them are compared and described in the survey presented by Nadeem Akhtar in 2014 in his study [4]

In 2018, a research based on analyzing the entertainment apps data collection and privacy vulnerabilities was done. This study stated the issue about how the apps use personal data of their users that is collected during registration and joining process. This study also identified the risks involved in data collection and usage process. And how the apps require more data than they actually need [5].

In a research done by Tadas Limba in 2018, it was stated that the user of Facebook decides about the quantity of information he/she wants to be public. Also, when registering and authorizing for a third-party application, the user must allow the app to view and use the personal data in order to use the app's services. The study also stated that users with publicly available data on Facebook should decide about which type of data they want to share with the third-party app. As a result, they proposed a model for the interaction between user and third-party applications for risk analysis and security of personal data [6].

Another research done in 2018 stated that Facebook uses personal potential data such as religious beliefs, sexual preferences etc. to label the user and shows them ads of their interests. According to EU GDPR this type of personal data cannot be processed because it can be used in malicious wok. A web browser extension was also proposed and implemented to inform the users of Facebook about the interests they have been assigned [7]

An article published in 2017 analyzed how personal data of public is misused by social platforms such as Google and Facebook for the purpose of advertising.

Privacy issues regarding the use of personal data were examined. It also identified, how these platforms provide confusing and incomplete information regarding the use of personal data of their users [8]

In 2016, another study on social engineering using Facebook as a social media platform was done. In that study, source credibility of social engineering attacks was measured by using four factors or dimensions. It was identified that there is a high chance of people accepting a message if the source of incoming message looks appealing and credible. In the study, the authors validated the presented four dimensions and presented a measurement scale [9].

In 2011, the Turkish department of information system security did an analysis by doing social engineering test on public agencies. With the help of phone calling, they tried to gain the trust of victim employees and persuaded them to disclose their personal and sensitive information. The purpose of this research was to figure out about the awareness of employees about the social engineering attacks [10].

Another study done by Jeremiah Onaolapo, showed that social media accounts are more user-centric because the properties that these accounts exhibit, reflect the actual personality. Due to these reasons such types of accounts are more likely to be stolen. After stealing the accounts, the hackers abuse these accounts according to the previously given information. For example, posts and messages are sent as the original user used to do [11].

A study proposed in 2020 performed risk analysis on personal data security. This study states that according to EU GDPR personal data should be secured and proper measures should be there to secure the data. A risk analysis methodology is also proposed [12].

Another study done in 2018 Abid Jamil proposed a model to prevent and mitigate the social engineering attack: phishing attack. They used four realistic scenarios to test the model. They proposed model also figures out the threats related to phishing attack [13].

In 2012, a study done by Jamie L. Pinchot investigated personal data privacy

concerns and consequences of data breach from Facebook. Their results suggested that students share a lot of confidential information on Facebook, and that type of data can be useful to answer personal security questions if captured [14].

In 2013, to assess the severity of personal data breaches, levels were designed. These levels were named as breach level index. Depending upon the type of personal data that was breached, a breach level index was defined. So, each time a breach is detected these indices can be used to detect and calculate the severity of the breach [15].

In 2016, a literature survey on social engineering attack type phishing attack is done. The study also proposed the types of phishing attack, there preventive and detecting measures. The study also described the advantages and disadvantages of phishing attacks [16].

In 2011, a study on reverse social engineering attack using the social networks was done. In that study authors explained how an attacker can exploit the find-friend feature of these networks. And they also discussed the effectiveness and feasibility of these attacks [17].

Study done in 2018 states that there is a great variance in the awareness of privacy and security control settings of Facebook among its users. Some on the users who know about these settings, use them for better security but there way of usage of this platform still reveals everything, and makes this effort useless. The study also reveals that the adult users of this platform take the precaution in comparison to the young users [18].

Frank McCown proposed a study in 2009. In his research he proposed a tool that could be used to extract activities of users of Facebook. That information can be used to perform a social engineering attack in these networks [19].

In 2019 a study states that there has been a massive increase in textual information on social networks such as posts, messages, reviews etc. and with this much increase in the textual information many privacy related problems arise. The study conducted a literature review to describe and discuss main issues that are

related to these online social media platforms. This study also identified the major gaps in available privacy models and their limitations [20].

In 2013, a study was done about the attributes that are considered important and sensitive by the users and are not disclosed by the users. Almost half a million of random Facebook accounts are crawled to see the number of attributes that are revealed publicly by the users on Facebook. Then they quantitatively classified the results on 3 cases. Age distribution, gender based and according to cities [21].

In 2018, a study states that, where online social networks provide such great facility, they also collect the personal and private data of their users. This data can be misused by either the data miners, or unauthorized person to perform some type of cyber-attack. In the study, some of the security and privacy flaws are discussed along with the prevention measures to protect the users from social media privacy problems [22].

A study in 2010 describes the design and security flaws in online social network. The study found out the privacy and security challenges in the design of these social media platforms. In the end this study points out some measures to avoid these design conflicts [23].

A study proposed in 2017, proposed a survey on online social network's privacy and security issue. It described the issues regarding security and privacy that have been reported so far in these networks. On the other hand, it also described the solutions that are available regarding the issue [24].

In 2009, a research describes how people and organization share a lot of personal information of social media some of this information is public but some information is kept private. It states that the private information can be guessed by using some learning algorithm on the publicly available information. They described how an inference attack can be launched on social networking data to guess and predict the private data. Then it states the possible solution to prevent and counter such attacks [25].

A study published in 2015 states the privacy risks that are linked with online social

media platforms. Most importantly when people share sensitive information on social media. They could become the victim of several types of cyber-crimes and also physical stalking. It describes how most of the people either don't configure their privacy settings on these social media platforms or have no idea if the settings exist. This study describes the risks and cyber-attacks that could take place on social media platforms user's privacy. And then provide some measures as a solution [26].

In 2017, a study presented and explained threats related to privacy and security of social media platforms that target users. They also describe the threats that can be caused by sharing of different content on these sites. In addition, this study also states the preventive solutions that are available to avoid these threats [27].

In a research done in 2019, according to the GDPR rule a person has the right to demand and view the data that was required and processed by a specific organization. And it is important to verify, is the person requesting the data is actually authorized to have it or not. To test this, they tried social engineering techniques on some 55 organizations, out of which 15 organization fell in the trap and leaked the data of their users [28].

Another study done in 2016, states that some users of Facebook don't share their personal information because of privacy concerns but their social circle such as friends and family on that platform can unintentionally leak that information. That information can be used in social engineering and phishing attacks. The researchers proposed an inference method to find information like date of birth and education based on interaction with friends and groups. A strategy to avoid information leakage was also proposed [29].

A study in 2015 states the vulnerabilities, that can exist in an organization and cause identity theft and cyber intrusion. The study also explains the working of social engineering and the effects that it can cause by doing identity theft. They also discussed the vulnerabilities and risks involved in social engineering attacks. In the end they also proposed some preventive measures to prevent these attacks from happening [30].

A study in 2020 states the issue of companies getting attack and personal data being breached. They examined different strategies that should be adopted by the company in case of data breach. They state that the customer satisfaction depends upon the severity of data, that is breached and how the company reacts to it. There results show that in case of severe data, it is difficult to regain the customers faith and trust [31].

In 2011, a conceptual study states that online social media platforms are the most important factors of information leakage. It also states that these social networks are a very important vector if attackers want to land an attack. In the end this research presents some security and prevention education to counter this type of scenarios [32].

Another research in 2014, describes how Facebook can be a big cause of information leakage. This research states that many people and organizations can unintentionally leak this confidential information from this platform. It also states that sometimes organizations try to hide their identity by using alternate names, but that can also be compromised [33].

In a study proposed in 2008, it was discussed that social platforms such as Facebook make the user's profile information open to developers. And that anyone can extract user's information without them knowing. To address the issue regarding privacy, a privacy management system was also introduced to protect the profile of users [34].

A study proposed by "ENISA" proposed an equation for the calculation of data breaches, that include some sort of personal information. Different recommendations were provided to calculate the severity of the breached data. The equation uses 3 parameters, each parameter provides an individual score and in the end a simple calculation is performed to calculate the complete severity score for the breached data. [35].

For scrapping the information from Facebook user profiles, there are several legal concerns, it is better to know the type of data that can be scrapped. Automated

scrapping is considered illegal and the only way to scrap is by using the screen scrapping technique [36]

social engineering attacks become successful if there exists a human vulnerability. a study in 2021 presented such vulnerabilities that can make a social engineering attacks successful along with the examples of some phishing attacks [37].

The primary way of data collection for surveys is the questionnaire. while designing a questionnaire some guidelines should be considered. And there are some ethical issues that need to be understood before asking the questions from public [38].

A study done on Facebook profile information disclosure, discussed how different information types are sensitive and how with the increase of age the percentage of available information decreases, a scoring tool was designed to detect threats because of information disclosure [39].

Similar study proposed how the information that is present of several platforms is key to stealing the private information. By joining the information found from several sources how an attack can be performed is explained in the study [40].

2.2 Conclusions from Literature Review

After performing the in-detail literature review, it can be concluded that a big emphasize has been given to the privacy and security issues of social media platforms. It can also be concluded that the information present on the profiles of these social media platforms plays an important role in making the user a victim of cyber-attacks. Such as phishing attacks. Many recent studies such as [3] in 2020, [12] in 2020 or [18] in 2018 are also done in the direction of data breach and privacy risks, and how data can be used to perform social engineering attacks. These recent studies have targeted the privacy concerns, data breach and the possibility of attacks that can be launched in several ways by using the information present on various social media platforms.

2.3 Comparative Analysis and Survey of Existing Techniques

From the comprehensive literature review that is provided in the previous section. Three similar studies done by Pinchot [14], Baatarjav [34] and farahbaksh et al. [21] are analyzed and their comparison is provided below. All these studies work on the idea of extracting publicly available information on Facebook profiles and then perform quantitative analyses on them. However, the objectives and aim of each study is different. The reason for choosing the studies is the extraction of publicly available information present on Facebook. A complete comparative analysis of these studies is performed below.

2.3.1 Methodology and Dataset

The first study did analysis on college students, 146 results were received, out of them 121 were the active user of Facebook. a questionnaire was used to conduct the survey. Based on age, three groups were created from the samples collected. Groups were created as following:

- Age from 18 – 33 as Millennial
- Age from 34 – 45 as Generation X
- Age from 46 – 64 as Baby Boomers

Similarly, the second study performed the survey on university of north Texas. They performed analyses of 4,919 profiles and used Facebook API to extract the information. The third study, however, used an HTML based crawler and performed the survey on 479,000 profiles. The profiles were completely random.

Comparison between the methodology and dataset is provided in Table 2.1. The table displays the comparison of the methodologies used in the relevant studies, it also shows how the data is collected and what was the objective of each study.

The no of records collected and the technique used to srap information from the social media platform is also dislayed in the table.

TABLE 2.1: Methodology and Dataset of previous researches

Study No.	Objective/Aim	Audience	No. of Records	Technique
Study 1	whether the information present on student's profile is helpful in answering security questions. Do these students have knowledge of privacy control mechanism	Students/College Undergraduates	146	Questionnaire
Study 2	Using Facebook Weak privacy to extract information from profiles	Facebook users from University of north Texas	4,919	Facebook API
Study 3	What type of personal attributes are publicly available on Facebook profiles.	Random Facebook users	479,000	HTML Crawler

2.3.2 Information Type

All techniques extracted personal information available on Facebook's profile. Comparison between the type of information that was considered while crawling by these three studies is provided in Table 2.2. The table displays all the possible information that is present on a specific profile and if it is extracted in the specific study or not. The 'Y' in the table means that the information is considered and collected in the study. Whereas, 'N' in the table represents no for the specific type of information against each study. Similarly all the possible information types and the study result is shown in the table.

TABLE 2.2: Information type

Type of Information	**Pinchot [14]**	**Baatarjav [34]**	**farahbaksh et al. [21]**
Date of Birth	Y	Y	Y
Gender	Y	N	Y
Current city	Y	Y	Y
Hometown	Y	Y	Y
Employer	Y	N	Y
Occupation	Y	N	N
Education	N	Y	N
College/University	Y	N	Y
Activities	N	Y	Y
Major	Y	N	N
Relationship	N	Y	N
Friend list	N	N	Y
Graduation Date	Y	N	N
High School	Y	Y	Y
Team	N	N	Y
Sports	N	N	Y
Athlete	N	N	Y
Interest	N	Y	Y
Inspire	N	N	Y
Religion	Y	N	N
Political Views	Y	Y	N
Sexual Orientation	Y	N	N
Music	Y	Y	Y
Note	N	Y	N
Wall	N	Y	N
Books	Y	Y	Y
Movies	Y	Y	Y
TV Shows	Y	Y	Y
Games	Y	N	Y

2.3.3 Results

The results of Pinchot [14] are provided in Table 2.3. In the first column of the table information type is shown. And in the second column, the percentage of people/profiles that were found with that specific type of information is shown. For example, the gender information is found on 81% of the profiles, the hometown is found to be present in 76 % of profiles and games information is found on 34% profiles only. Just like this, each information type with the percentage of profiles on which the information is found is written in the table. In the end

based on the results the Pinchot [14] states some preventive measures to avoid the sensitive information from getting leaked and to educate the users about privacy configurations.

TABLE 2.3: experiment results of Pinchot [14]

Type of information shared	**No.of people who shared the information**
Date of Birth	63.6%
Gender	81.0%
Current City	75.2%
Hometown	76.0%
Employer	45.5%
Occupation	43.0%
College/University	79.3%
Major	49.6%
Graduation Date	38.8%
High School	85.1%
Religion	33.9%
Political Views	29.8%
Sexual Orientation	47.9%
Music	51.2%
Books	41.3%
Movies	50.4%
TV Shows	44.6%
Games	34.7%

The results of Baatarjav [34] are displayed according to 4 groups: age, sex, relationship and Political preferences. The results of Baatarjav [34] are provided in Table 2.4 and Table 2.5. It can be seen in the tables, that there are 35% males and 65% females present on the social media for their selected audience. And for all these groups, age, relationship status, political preference, male, female and age group information is extracted. For each, they calculated the percentage of profiles, on which the specific information was found. Based on these results the study provided a privacy protection Mechanism as a counter measure to prevent the information leakage.

A similar study 2013 was also done, the objective of the study was to find out the attributes that are publicly available on Facebook profiles and then classify them on different categories. Same like previous results, this study also collected the

TABLE 2.4: Percentage of people who revealed the Information

Category	Group	Percentage who revealed the info
sex	Male	35
	Female	65
Age	15-19	4
	20-24	82
	25-29	14
	30+	0.5
Relationship	Single	47
	In relationship	35
	Engaged	6
	Married	12
	Complicated	0
	Open Relationship	0.4
Political Preferences	Very liberal	6
	Liberal	28
	Moderate	34
	Conservative	24
	Very conservative	2
	Apathetic	4
	Libertarian	3

TABLE 2.5: Results of Baatarjav [34]

Type of information	number of profiles the information was found
Age	62%
Relationship status	64%
Political preferences	48%
Male	65%
Female	35%
20-24 age	82%
15-19, 25-29 and 30+ age	18.5%

information in the first step. Then, after the collection of the information. They calculated the profile percentage on which a specific information was found. It can be seen in the results, that the current city information is found on more that 30% of the profiles, also gender is found on more than 50% profiles. Same like this, all type of information that is collected from the profiles are listed and the percentage of profiles, is listed in front of each information. The complete results of the Farahbakhsh et al. [21] are provided in Table 2.6. As stated in Pinchot [14] and Baatarjav [34], Farahbakhsh et al. [21] did not provide any preventive and

counter measures about information leakage and privacy.

TABLE 2.6: results of Farahbakhsh et al. [21]

Information type	**number of profiles the information was found**
Friend-list	62.7 %
Current City	36.1%
Hometown	34.6%
Gender	53.5%
Birthday	2.9%
Employers	22.5%
College	16.8%
High School	13.2%
Aggregate-Interest	48.4%
Music	41.0%
Movie	28.3%
Book	16.7%
Television	31.8%
Games	9.4%
Team	8.5%
Sports	8.5%
Athletes	10.7%
Activities	20.5%
Interests	10.9%
Inspire	1.9%

2.3.4 Limitations

Following are the limitations that are observed and found in the existing solutions.

- Limitation of Technique in Pinchot [14] is the smaller dataset
- Pinchot [14] also targeted only students.
- Pinchot [14] also doesn't calculate severity levels of information found on these profiles.
- Farahbakhsh et al. [21] doesn't provide any counter measures for protection of privacy.
- Baatarjav [34] and Farahbakhsh et al. [21] also don't provide any severity levels of information

2.4 Identified Research Gaps

After doing a comprehensive literature review regarding privacy and security concerns of social media platforms. And performing a comparative analysis of researches that stated the issue of publicly available and accessible information present on Facebook profiles. The research gap that was found can be described as follows:

Firstly, the main deficiency that is found in the researches is that the severity levels of publicly available information on Facebook are not defined.

As the information that is available on Facebook profile can be used to perform several cyber-attacks such as, password recovery and identity theft, it can also be collected and analyzed by a hacker to land a phishing attack on the users.

Awareness of general public about the social engineering and phishing attack on Facebook need to be studied. Along with that the severity levels of information that most people make public on Facebook should be defined by using an authentic scale.

Chapter 3

Proposed System

As described in the literature review section, previous studies only focused on the information extraction and getting to know about how many profiles are present on the social media that possesses a certain information. None of the studies focused on severity rating of the profiles and how a certain information can be used and tailored in making a social engineering attack successful. Moreover, how a specific information can be a cause to start a social engineering attack and making the owner victim of the social engineering attack, mainly phishing attack. For this purpose, this research focuses on providing a quantitative scale for the severity of the publicly available information.

3.1 Introduction to the System

After critically analyzing the literature and the problem discussed, a solution is proposed that can help to measure the severity of publicly available information present on social media profiles. The solution uses the equation proposed in [35]. overall proposed solution consist of several steps which are discussed in the section below. This chapter provides the explanation of the proposed solution and the methodology to calculate the severity of publicly available information on the

social media profiles. The whole working and methodology of the proposed system is starting from heading 3.3 on wards.

3.2 ENISA Methodology to Calculate Personal Data Breach Severity

The "European Union Agency for Network and information security" also known as ENISA, in 2013 provided some recommendations and methodology to assess the severity of data breaches if they contain any sort of personal data. A working document was published, in which a detailed working and calculation formula was presented to calculate the severity of data breaches with personal data. following the Idea and methodology proposed in the document, the "EU General Data Protection Regulation Academy" published a white paper [1] in which they implemented the proposed equation and offered a methodology so that severity of personal data breaches can be determined and to determine and adopt mitigation steps as well as notification to the concerned department according to the requirements of GDPR. The equation proposed is as follows:

SE = DPC x EI + CB

Where SE stands for "Severity", DPC stands for "Data Processing Context" and CB stands for "circumstances of breach".

Each attribute has its predefined score and it can be adjusted to produce the most appropriate results. The discussed equation has been proposed to assess the severity of the personal data breaches and is not applied on the publicly available information that is present on the social media profile especially from the aspect of social engineering attack.

In the equation above, there are three different parameters, each type of parameter has its own score range. Each parameter is scored by looking at the recommended levels and the circumstances and then a final severity is calculated by performing the calculation on these platforms.

[1] https://info.advisera.com/eugdpracademy/free-download/assessing-the-severity-of-personal-data-breaches-according-to-gdpr

3.2.1 Recommendations for Scoring the Equation Parameters

Complete recommendations for scoring of equation's parameters are provided in detail in [35]. The scoring mechanism according to the recommendations for each parameter of is provided in detail in the next section.

3.2.2 Data Processing Context (DPC)

The Data processing context refers to the nature of data that is breached, along with some factors linked to overall context.
According to the technique, this parameter is the core as it tells about how critical the breached information is.
There are four different categories of the breached data that are as follows.

- Simple Data: Eg. Biographical data, contact details, education, family etc.
- Behavioral Data: Eg. Location, Traffic data, personal preferences etc.
- Financial data: Eg. income, Bank statements, invoices etc.
- Sensitive Data: Eg. health, sexual life, political preferences/affiliation etc.

The scores for each category are 1,2,3 and 4 respectively.

3.2.3 Ease of Identification (EI)

Ease of identification means the easiness of identification, of the individual whose data is breached. the score is assigned after looking at data and the scenario. If the breached data can help to identify the individual, for example, if the picture and full name is present in the data, then it is easy to identify the individual. In this case the score of "EI" is maximum, which is 1. otherwise it is considered 0 if the individual cannot be identified.

3.2.4 Circumstances of Breach (CB)

This parameter is concerned with the circumstances that are related to the breach data with respect to the security measures such as:

- Loss of Confidentiality
- Loss of Availability
- Loss of Integrity
- Malicious intent

For scoring the circumstances 3 different scores are provided for loss of confidentiality, integrity and availability. A single score is given for the malicious intent. If the data breach causes the loss of confidentiality and their is no evidence of illegal processing then the score should be 0. If the data is disposed to a number of known recipients, then the score should be 0.25. If the data is disposed to a unknown number of recipients, then the score should be 0.5.

For scoring the loss of integrity, the score should be:
0: if data altered but without any illegal use 0.25: data altered and possibly used illegally but with a possibility to recover. 0.5: data altered and used illegally and there is no chance of recovery

similarly, for scoring the loss of availability the score should be:
0: if data is recoverable 0.25: data remain unavailable temporarily 0.5: data cannot be recovered.
For scoring the malicious intent, where the breach of data occurs due to intentional actions. The score should be 0.5.

The scores of this category is adjusted and instead of the actual values, adjusted values are used. The adjusted value are just a mapping of actual number with another number. The revised adjusted scores are as follows:

- 0 is considered as 0
- 0.25 is considered as 1
- 0.5 is considered as 2

3.3 Research Methodology

To perform the research, experimental research methodology will be used. In the initial stage the literature review is performed from the related research papers and articles. Then from the conclusion of the literature review, Research gap is identified and a problem statement is described. The problem statement raised some research questions that are described . To answer these questions an experimental methodology will be adopted.

First of all, to perform the exploration phase, according to the problem statement, profiles of social media platforms should be explored and required data or information type and presence will be checked. Once the information types are finalized, severity levels will be defined so that the experiment can be performed on the data and results can be recorded. Once the results are generated from the experiments, these results will then be compared with the results collected from the field experts and a conclusion is drwan.

3.3.1 Experimental Methodology

For performing the proposed research, the experimental research methodology will be used. The Experimental methodology can be divided into five phases[2]. Each of the phase of the methodology is explained briefly below.

1. **Identifying a research Problem**: Finding the problem for research purpose by doing literature review.

[2]https://writing.colostate.edu/guides/page.cfm?pageid=1363guideid=64

2. **Planning an experimental research study**: Plan and prepare an experiment to conduct regarding the research problem.

3. **Conducting the experiment**: Perform the experiment and gather the data.

4. **Analyzing the data**: Perform detailed analysis on the data collected through experiment.

5. **Present the results**: Evaluate and then present the results generated after the analysis.

The proposed system uses the equation provided in [35] to calculate the severity of publicly available information on FACEBOOK profiles. The severity is calculated from the aspect of social engineering attacks and other possible cyber-attacks as well as how the information can be utilized in performing such attacks.

3.4 Information Collection from Facebook Profiles and Legal Concerns

As scrapping large amount of data from Facebook by using any automated means is considered illegal and is not allowed, Screen scrapping is the only valid way to collect the publicly available information present on the Facebook profiles [36]. The technique of screen scrapping is basically based on automated browsing, where a user behaviour is simulated to collect the data present on the screen.

In order to avoid any kind of legal issues related to scrapping of data from Facebook profiles, the proposed system does not use scrapping of any kind at all. Instead of scrapping the information from Facebook profiles. What basically happens is that the presence of information is checked on someone's profile. It means that the proposed system is not concerned with the information or what the actual information is, instead it checks if a specific type of information is present on a profile or not.

3.5 Architecture Diagram

Figure 3.1 shows the architecture diagram for the proposed solution

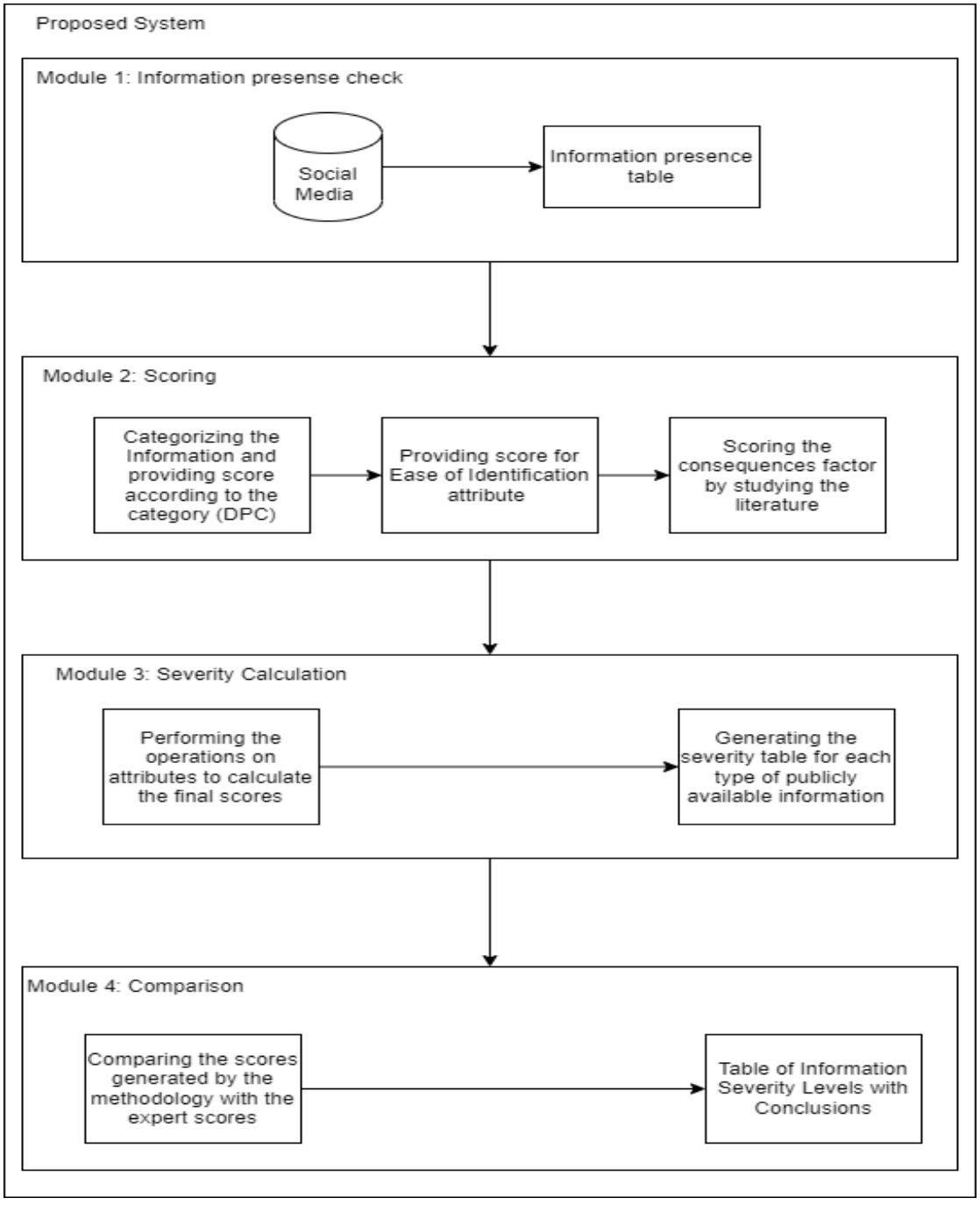


FIGURE 3.1: Architecture diagram of proposed system

The whole system consist of four different modules. In the first module possible categories of publicly available information is checked from a profile of Facebook

and an information presence table is constructed. This table is then passed to the next module.

During the second module, also known as the scoring module, each information is categorised and assigned a score according to type of data/information. Similarly, for each type of information the ease of identification parameter of the equation is scored according to the recommendations. After assigning the scores for first two parameters, the last parameter is scored by keeping in mind the consequences that can occur related to the social engineering attack. The individual scores are then passed to the third module as input.

In the third module, the severity calculation module, the operations are performed on the individual scores to generate a collective score also called severity. once the severity scores are generated, a severity table is constructed, that contains the information and their severity scores. The severity table is passed to the next module.

In the fourth and the last module, the Comparison phase, The calculated severity scores are compared and with the scores obtained from the field experts and then percentage difference is calculated in both the proposed system results and the experts results. To find the agreement between the experts result for different information types, the inter rater agreement will be calculated for each type of given information.

3.6 Assigning Information Severity Scores by Field Experts

For comparing the scores generated by proposed system, a questionnaire is designed and distributed among some field experts. Each field expert assigns a score against each information type and in the end an average score is calculated for the specific information type. Figure 3.2 shows the methodology diagram for expert scoring.

Firstly, the questionnaire is prepared, then it is distributed among the experts,

once the experts have submitted the response, an average for each of the information type is calculated and a severity table is designed.

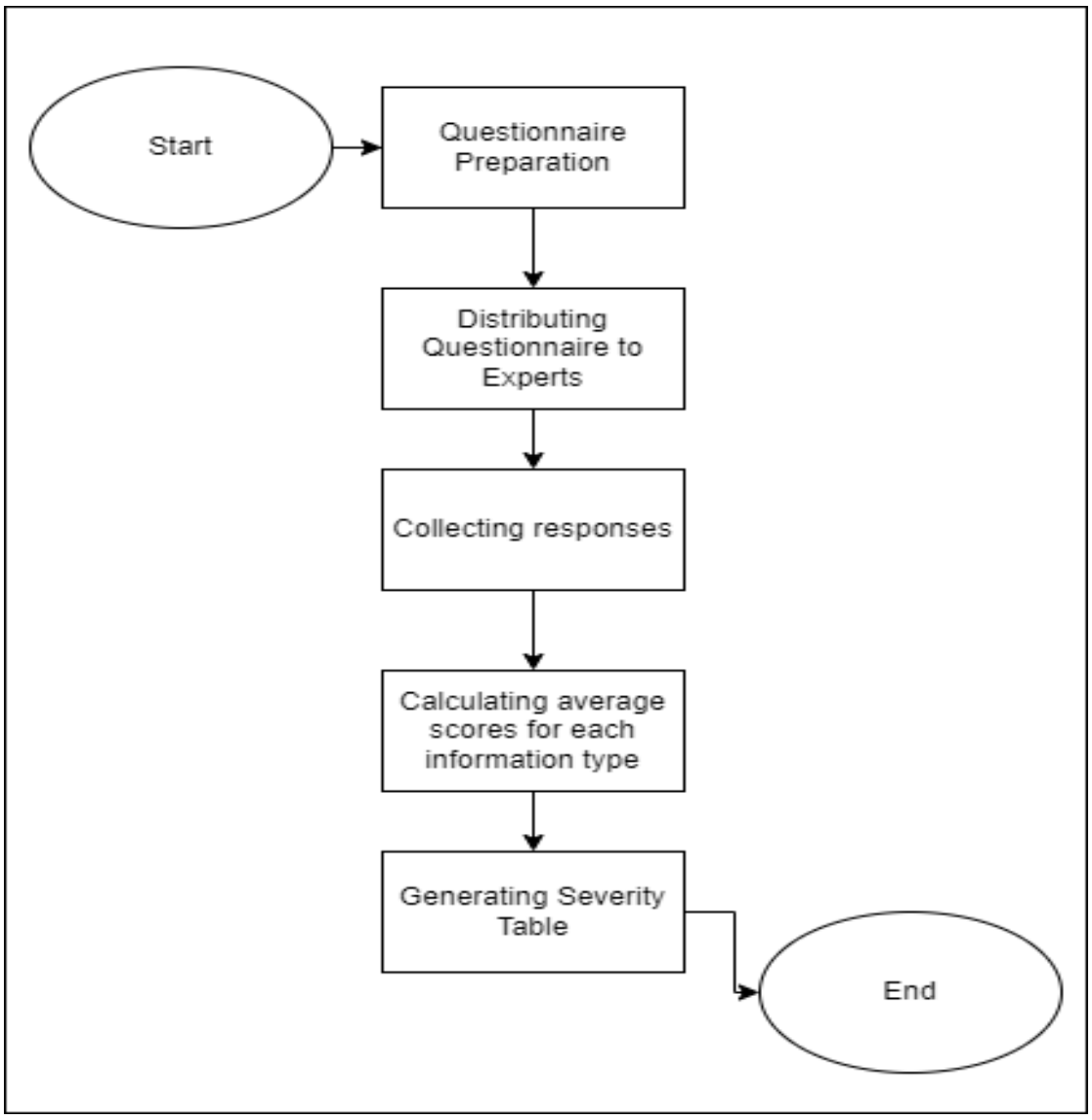


FIGURE 3.2: Methodology Diagram for Expert's Scoring

3.7 Methodology Diagram

Figure 3.3 shows the methodology diagram of the proposed system. The whole methodology of the proposed system depends on several steps.

First of all the profiles of Facebook are explored and the publicly available information is checked. Once the presence of information is checked, the different

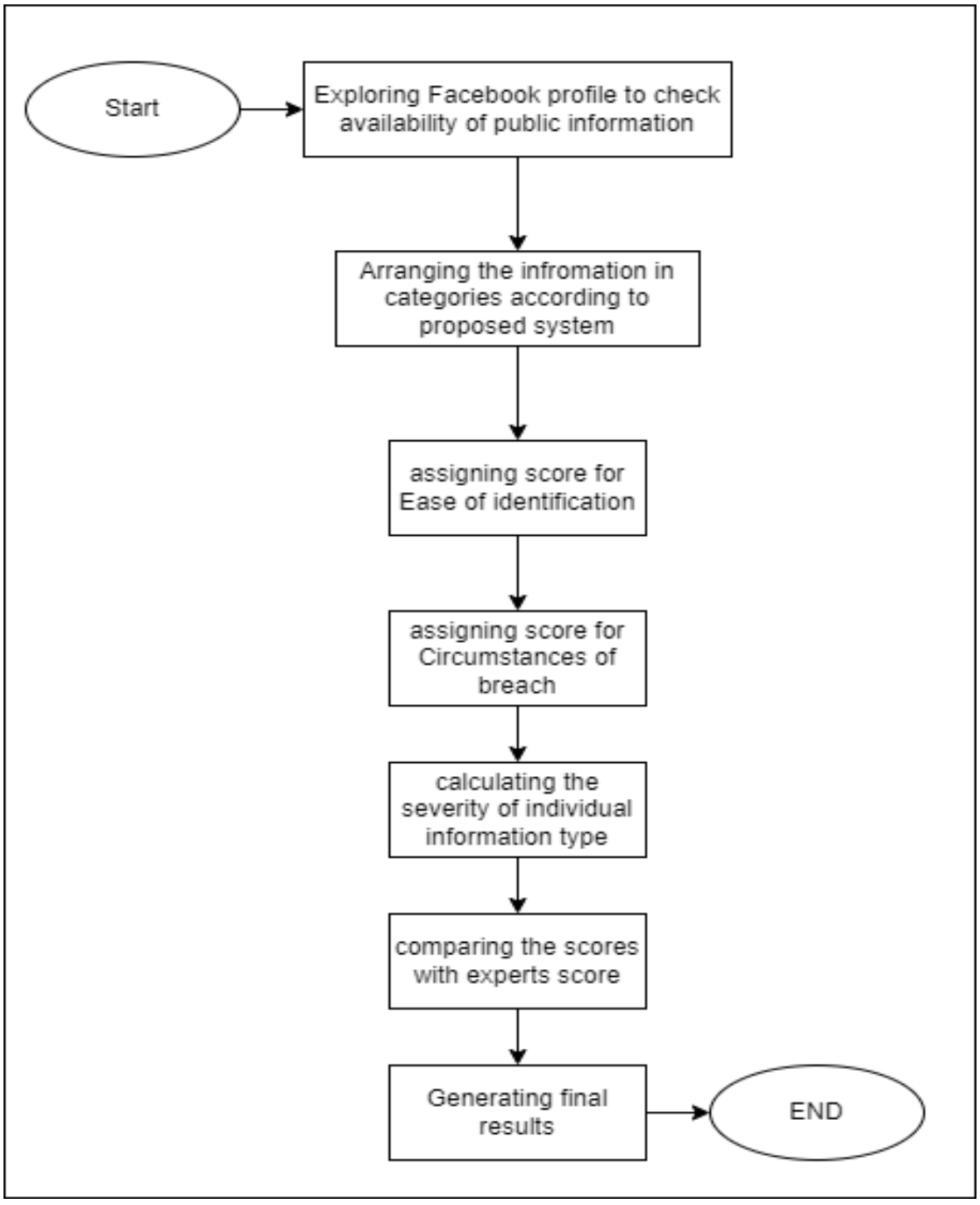


FIGURE 3.3: Methodology diagram of proposed system

types of information that can be extracted are then scored in case of availability. The scoring is done using the recommendations of the previously discussed equation. Firstly all the information types are arranged in categories and their score is assigned, in the next step for each information type, the EI(Ease of identification) parameter is scored by checking the recommendations.The "circumstances of breach" parameter also known as the CB is scored by checking the circumstances

related to the security parameters. In the proposed solution, this attribute works by keeping the consequences that can occur if a specific information is tailored in performing a social engineering attack. The score is given by carefully finding the examples of social engineering attacks that could use a certain type of information, that is publicly available on Facebook profile. once a suitable example is found it is then mapped with the examples present in the recommendations and a score is assigned.

Chapter 4

Experiment and Results

This chapter provides the details about the experiment that was performed for the proposed system and the results that were generated. As the research methodology that is being used is the Experimental research methodology, an experiment is performed to get to know the results of the proposed system As described in the previous chapter the objective is to define the severity levels for information that are publicly available on social media profiles. Information from the profiles will be collected and analyses will be performed to produce the results. This whole procedure involves exploration, experiments and evaluation. So, the research methodology that will be used to carry out the research will be Experimental research methodology.

4.1 Experimental Setup

This section explains the whole experiment process. The experiment will include the selection of social media platform, selection of information type and then scoring from experts and the proposed solution, and the comparison between them. The steps and the preparation that was involved in the experiment of the proposed system is described in detail in this section. All the steps are explained in detail. If there is any extra step involved, that is also explained.

4.1.1 Choosing the Appropriate Social Media Platform

The social media platform that is used to perform the experiment and collect information is Facebook. As it provides a comprehensive list of information that are available on a specific profile as compared to other social media platforms such as Instagram, Twitter and LinkedIn. Moreover, attributes that are available are mostly personal.

4.1.2 Proxy Settings of Profile Information on Facebook User Profile

When a new profile is created on Facebook, it is created with default proxy settings. The proxy settings on Facebook profiles basically decides the group of people than can see a certain information on that profile. The proxy settings, an individual can apply to a specific information on his/her profile are as follows:

- Public
- Friends
- Friends Except
- Specific Friends
- Only me

4.1.3 Public

The public proxy sets the information to be seen by anyone who has a profile on Facebook. Any information that is provided and has its proxy set to public, will be displayed to everyone with a profile on Facebook. There are many information types, for which the privacy settings are set to public by default. A complete information list with default list of privacy setting for that information, is provided later in this section.

4.1.4 Friends

The friends proxy sets the information to be seen by only those who are added as friend in the profile with the information.

4.1.5 Friends Except

This type of proxy works almost same as the friends but with a little change, that, you can exclude a specific group of friends who cannot see that type of information.

4.1.6 Specific Friends

The "Specific friends" proxy works opposite to the "Friends Except" as it sets the information to be seen by only a specific group of friends.

4.1.7 Only Me

This setting of proxy restricts the information to be seen by only the person with the profile.

4.2 Information Types and Presence on Facebook User Profiles

A profile with default proxy settings on Facebook contains the following types of information that can been seen publicly.

1. Work/Job
2. Residence
3. School/college

4. Relationship status
5. Hobbies
6. Family members
7. Details about you
8. Life event
9. Contacts(Shown to friends on default settings)
10. Questions/answered
11. Birthday
12. Gender

4.3 Severity Scores of Information by Field Experts

Once the information types and their presence is checked from the profiles of Facebook, their scoring process starts. As described in the methodology section, the information types are scored by the proposed methodology as well as the field experts and the scores are then compared for the evaluation purpose.

To get the scores of severity of publicly available information on Facebook profiles, from experts, a questionnaire was prepared by using the "Google Forms". As this questionnaire is related to research, so some guidelines were adopted from the literature [38] and the questionnaire was prepare accordingly.

Once designed, this questionnaire was then distributed to some field experts that answered the questions asked in the questionnaire. Each expert was asked to fill the questionnaire by carefully reading the question statement. A total of twelve responses were received from the experts. The designed questionnaire is attached under Appendix A.

4.4 Severity Scores of Information by Public

A similar questionnaire was also prepared for scoring of severity from public. The purpose of this questionnaire is to get an understanding of, how the general public understands the importance of information on their Facebook profiles with respect to cyber-attacks. See Appendix B for questionnaire.

4.5 Questionnaire Contents

Both the questionnaire consisted of similar questions, except the section asking for basic field related or personal information. The questions asked for severity scoring of publicly available information on Facebook profile, in the questionnaire from experts are as follows:

1. How critical a profile should be if it contains the information about job organization and job position of the user? (Work/Job place information)
2. What should be the severity of a profile that contains the living place or residence information of the user?(Residence)
3. How critical can it be on a scale of 5, if a profile contains the educational information like School/college/university, ?
4. How would you rate a profile with Relationship status information?
5. How, a profile that contains information about hobbies of the user can be rated on the given scale?
6. What should be the severity level of a profile that tells about family members of the user of that profile?
7. How a profile, that contains extra details about person with the profile such as nickname, can be rated?

8. How would you rate a profile that contains answers to most popular questions such as, Favorite writer, favorite sports?

9. What do you think about criticalness of a profile that contains life event information?

10. According to you how a profile containing several type of contact information such as, email and phone number of the user can be rated?

11. What should be the severity level of a profile that contains birthday information of the user of that profile?

12. What should be the severity level of a profile that contains Gender information of the user of that profile?

Each expert answers all of these questions and assigns a score from 0-4 where:

- 0 = No criticalness
- 1 = less critical
- 2 = moderately critical
- 3 = critical
- 4 = highly critical

In the end a final average score will be calculated for each type of information.

4.6 Scoring the Information Using the Proposed System

For scoring the severity of the publicly available information on Facebook profiles by using the proposed system, there are several steps that are followed. Each of the step and the process is explained in detail in this section.

4.6.1 Information Presence Check

First of all, to calculate the scores for the information found on a specific profile of Facebook, the type of information and their presence must be checked.
Once the information type and presence is checked, the information presence matrix or an information presence table is created that tells us about the important personal information that can be found easily on a profile of Facebook.

4.6.2 Information Categorization

In this section, according to the recommendations of "GDPR methodology of assessing severity of a data breach" each type of information is categorized in their respective categories. A total of twelve different types of information was found on a profile. These information types lie in 2 different categorize according to the recommendations as shown in table 4.1. From the available information

TABLE 4.1: Categories of Information type

Category	Information type	Score
Simple Data	Work/job Education Contacts Residence Family Members Birthday gender Life events relationship Status Hobbies	1
Behavioural Data	Residence/Location Popular Questions Details about you	2

the information type "Residence/Location", "Question/Answered" (tells about the liking and disliking of a person) and the "Details about you" (tells about the nickname/maiden name, favourite quotes, blood donations etc) are categorized under the Behavioral data category with basic score as 2.

For the rest of the information types that are "work/Job information, Education information, contacts, Residence, Family members, date of birth, gender, life events, relationship status, and hobbies" are categorized under the Simple/Biographical data with basic score as 1.

4.6.3 Ease of Identification Scoring

As described earlier that this parameter is basically scored on the easiness of the identification of a specific person based on the breached data. Also how easily the available information can be matched with a specific person.

When we talk about a social media profile, every information that is found there, belongs to the person with the profile. So, identification factor becomes very easy. Moreover, presence of a profile picture, also makes it easy to match the information to the individual. On the basis of these factors, the score of this parameter is set to maximum, which is 1.

So the Score for "EI" parameter for every information type is considered **1**.

4.6.4 Scoring Circumstances of Breach

The final parameter that needs to be scored depends upon the circumstances that can occur due to the breach of data such as loss confidentiality, integrity, availability and malicious intent.
As the proposed study is done for the information present on Facebook profile and the importance of that information in context of social engineering attacks. Or simply, what role an information can play in making the person a victim of social engineering attack.
This parameter can also be considered as the consequences of information leakage in context of social engineering attack.
For scoring this parameter, the recommendation examples and the examples in literature related to social engineering attacks is considered and then the scores

TABLE 4.2: Consequences of data breach

Information	Consequences	Score	recommendation	reference
Work/Job	Shoulder surfing	2	Malicious intent	[37]
School/College/Uni	Baiting	2	Malicious intent	[37]
Contacts	Phishing attack	2	Malicious intent	[37]
Residence	Location leakage	2	Loss of confidentiality	[6]
Family Members	Personal information leakage	2	Loss of confidentiality	[6]
Details about you	Nick/maiden Name leakage	2	Loss of confidentiality	[6]
Birth Date	Age prediction	2	Loss of confidentiality	[29], [39]
Life events	Educational bgrnd prediction	2	Loss of confidentiality	[29]
Relationship status	Marital status/Family life	2	Loss of confidentiality	[2]
Gender	personal info/Identity Theft	2	Loss of confidentiality	[2], [39]
Popular Questions	personal preferences	2	Loss of confidentiality	[35]
Hobbies	personal preferences	2	Loss of confidentiality	[35]

are assigned to each type of information.

The scores for each type of information after carefully consulting the literature and the recommendations is provided in table 4.2.

First information is the "Work/Job" information. If a person has revealed the job position and the organization he/she works at then a shoulder surfing attack can be performed and even a dumpster diving type of social engineering attack can also be performed. So, This type is scored to 2 on the basis of "malicious intent" recommendation from [35].

Just like the work and job place information, if a person has revealed the education and the institute where he studies, then an attacker can approach and perform a

baiting attack on the victim. on this base, the score of this parameter is also set to 2.

In the next row, the contact information is mentioned, if we talk about the phishing attacks, then contact information plays an important role in such attacks where an attacker can send phishing emails and messages to victim and lure the victim in a trap. This sets the score of this information type to 2.

If a person has revealed his Family members and best friends on his profile. The attacker can perform profile cloning or identity theft attack by creating a fake profile with the same information as one of the victim's relative or friend and maybe succeed in making the victim to disclose some important function. This and the reason that this type of information is considered personal results the score to be set to 2.

Revealing the gender information can help in identity theft, The Birthday tells about age, from the life event information, educational background can be predicted, similarly popular questions and hobbies tell about the personal preferences of a user. just like this, against each type of information, the possible consequence is written and the score after considering the recommendation and reference is assigned.

4.6.5 Calculating the Final Score for Each Information Type

After the calculation of scores for each parameter, the required operations are performed on the parameters to calculate the final severity score for each type of information. To calculate the final score, the value of first parameter is multiplied with the value of second parameter and then the value of consequences is added to get the final score.
The multiplication provides an initial score and then depending upon the consequences with respect to cyber-attacks or information leakage, a score is added in the severity to compute the final score.

4.6.6 Results of Proposed solution

The results of proposed solution are generated after assigning the values of each parameter of the equation and then performing the required operations.
The complete details of the scoring of information are provided in the table 4.3.

TABLE 4.3: Scores of proposed solution

Information	DPC	EI	CB	Final severity
Work/Job	1	1	2	3
Residence	2	1	2	4
School/College	1	1	2	3
Relationship Status	1	1	2	3
hobbies	1	1	2	3
Family Members	1	1	2	3
Details about you	2	1	2	4
Popular questions	2	1	2	4
Life event	1	1	2	3
Contact Information	1	1	2	3
Birthdate	1	1	2	3
Gender	1	1	2	3

In the first column of the table, information types are written. The second column shows the scores assigned after the categorization of each type of information also known as the "Data processing context". The third column displays the "Ease of identification" score and the fourth column shows the score for the consequences of breach.

The first two values are multiplied together to generate an initial value and then, depending on the consequences that can occur with respect to cyber-attack such as social engineering attack, a value is assigned and added to the score to generate a final score. Same like this, severity scores for each type of information are calculated and written in the table.

4.6.7 Comparison of the Scores with Expert Scores

As discussed earlier, that a questionnaire is designed to get a severity rating for each type of available information on a Facebook profile. Once the scores from

TABLE 4.4: Professions of Field Experts

Profession	**Percentage of experts in the profession**
Self-Employed	16.7
Professor/Teacher	58.3
Developer	8.3
IT-Specialist	8.3
Info-Security Specialist	8.3

experts are gathered, they are compared with the scores calculated by the proposed system. By doing the comparison the proposed system is evaluated and a final verdict and conclusion is drawn.

4.7 Results of Questionnaire

The results obtained from the questionnaire, that was submitted by the field experts are discussed in table below:

Out of all the experts that submitted the questionnaire:

- 58.3% are Professors in a well-reputed university
- 16.7% are self-employed
- 8.3% are developers
- 8.3% are IT specialist
- 8.3% are Information security specialist

The second question was asked about the field of work. Each expert was asked about the specific field in which he/she works. And the results of this question are as follows:

- 25% are penetration tester
- 8.3% work in cryptography

TABLE 4.5: Field of Work of Experts

Field of Work	**Percentage of experts in the Field**
Penetration Tester	25
Cryptographer	8.3
Security Analyst	16.7
Security Consultant	33.3
Security Administrator	16.7

- 16.7% are security analysts
- 33.3% are security consultants
- 16.7% work as a security administrator

Third question was regarding the experience:

- 91.7% have one to five years of experience
- 8.3% have six to ten years of experience

The remaining questions were asked regarding to the information present on the Facebook profile and how critical it can be with respect to social engineering attacks. On the next page, The scoring done by the experts is explained.

The statistics of scores provided by the experts to the information types are shown in table 4.6. In the table, The first column shows the information type that can be found on a specific profile. The remaining columns are labeled as the possible score. Each cell in the table tells the percentage of experts who selected a specific value against any information type.

For each type of information each field expert assigned a score and on the basis of total responses, as shown in the table, 0% experts scored work/job as 0 (no criticalness). 16.7% scored it as less critical. 33.3% scored this information as moderately critical. again 33.3% scored it as critical and finally 16.7% scored the information as highly critical. Just like this every type of information is assigned a score from experts and the statistics are displayed in the table.

TABLE 4.6: Scores of experts

Information	**0**	**1**	**2**	**3**	**4**
Work/Job	0	16.7	33.3	33.3	16.7
Residence	0	16.7	25	50	8.3
School/College	0	33.3	41.7	25	0
Relationship Status	0	33.3	41.7	25	0
hobbies	0	50	33.3	16.7	0
Family Members	0	8.3	33.3	25	33.3
Details about you	8.3	33.3	50	0	8.3
Popular questions	8.3	41.7	33.3	16.7	0
Life event	8.3	8.3	41.7	33.3	8.3
Contact Information	0	0	8.3	41.7	50
Birthdate	8.3	16.7	50	16.7	8.3
Gender	75	8.3	16.7	0	0

The Pie-charts of each question that is answered are provided in the next section. Each pie chart displays the percentage of experts, who selected a specific answer to each of the question.

The description of some of the pie charts of experts is as follows:

1. **Work/Job**: In Figure 4.1 16.7% think that it is less critical 33.3% think, it is moderately critical. 33.3% think it is critical and 16.7% think that it is highly critical.

2. **Residence**: In Figure 4.2 16.7% think that it is less critical 25% think, it is moderately critical. 50% think it is critical and 8.3% think that it is highly critical.

3. **Relationship**: In Figure 4.4 33.3% think that it is less critical 41.7% think, it is moderately critical. 25% think it is critical.

4. **Contact**: In Figure 4.10 8.3% think, it is moderately critical. 41.7% think it is critical and 50% think that it is highly critical.

5. **Gender**: In Figure 4.12 75% think that it has no criticalness. 8.3% think that it is less critical 16.7% think, it is moderately critical.
   Just like this all the scores are represented in the form of pie charts in the figures displayed.

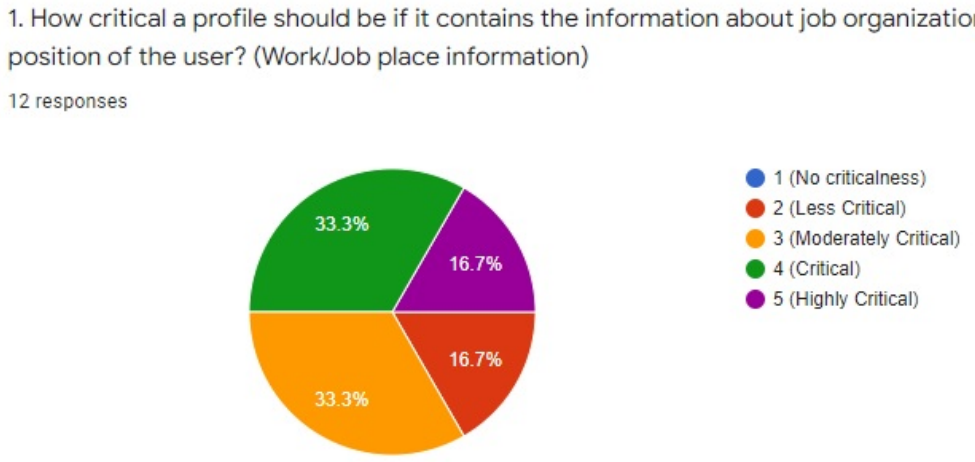


FIGURE 4.1: Q1: for Expert

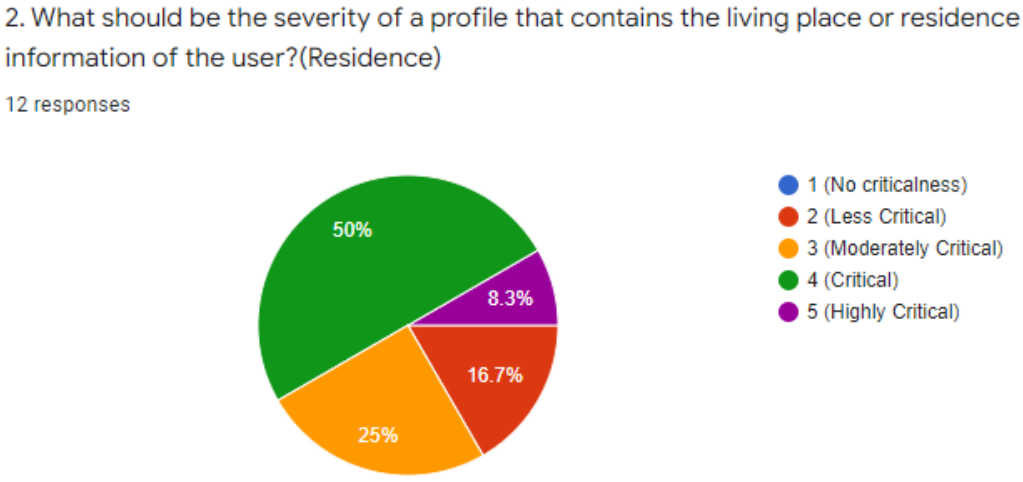


FIGURE 4.2: Q2: for Expert

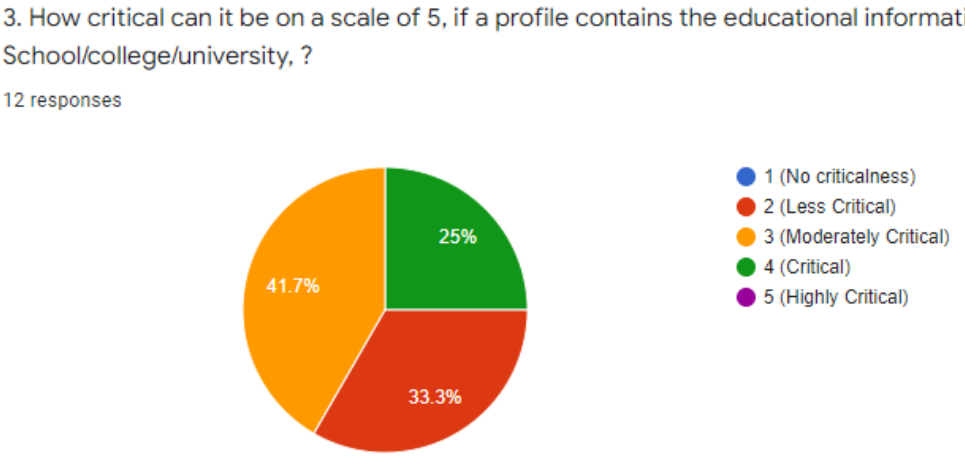


FIGURE 4.3: Q3: for Expert

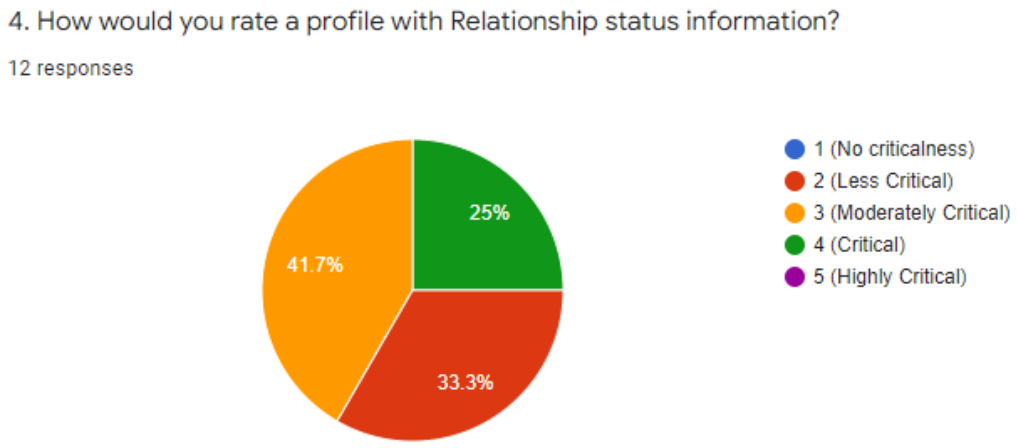


FIGURE 4.4: Q4: for Expert

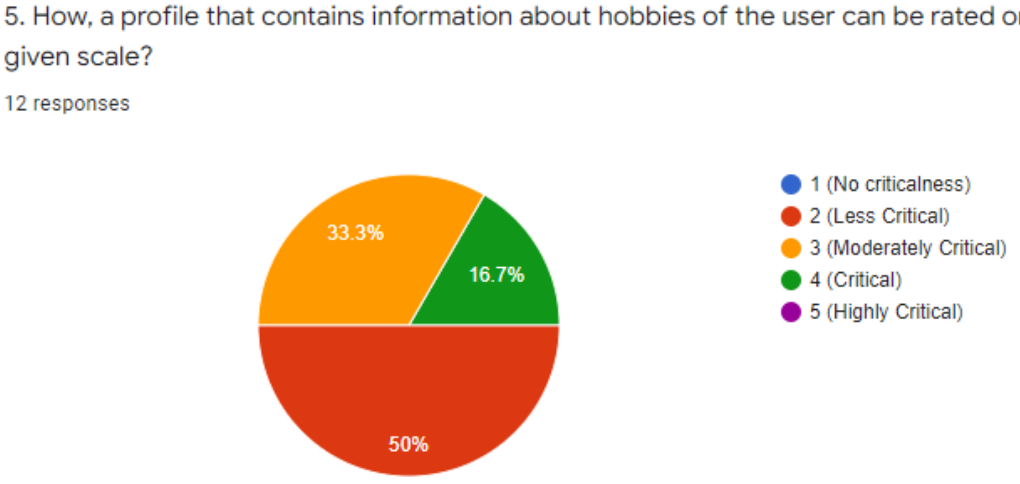


FIGURE 4.5: Q5: for Expert

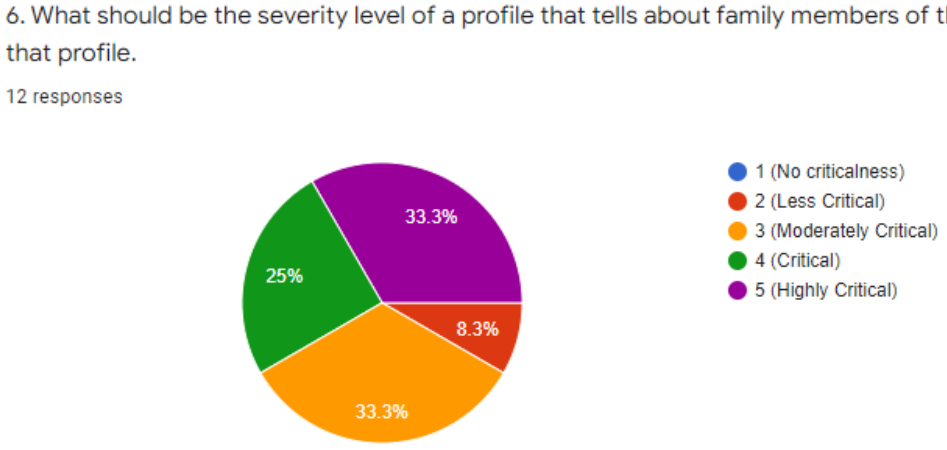


FIGURE 4.6: Q6: for Expert

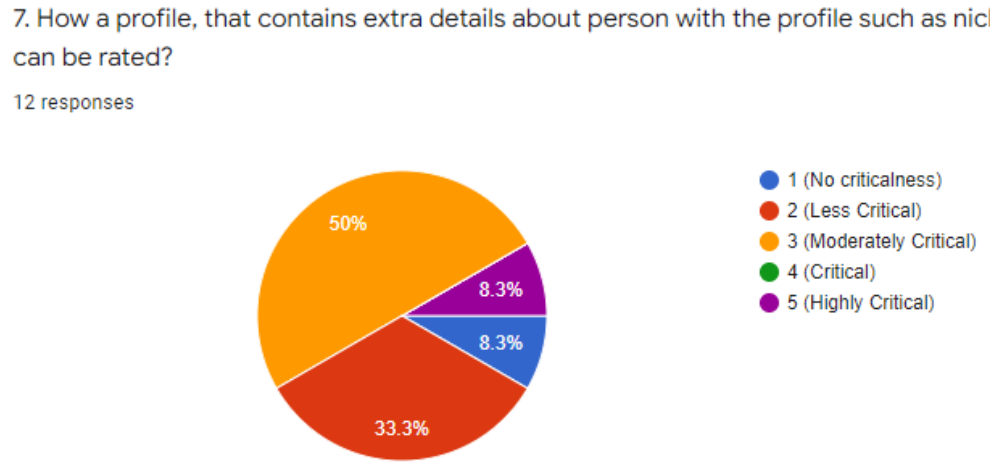


FIGURE 4.7: Q7: for Expert

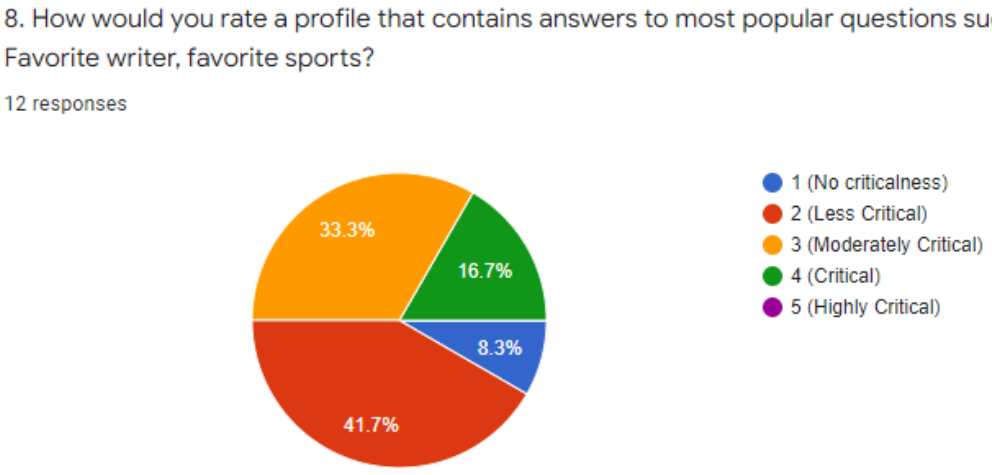


FIGURE 4.8: Q8: for Expert

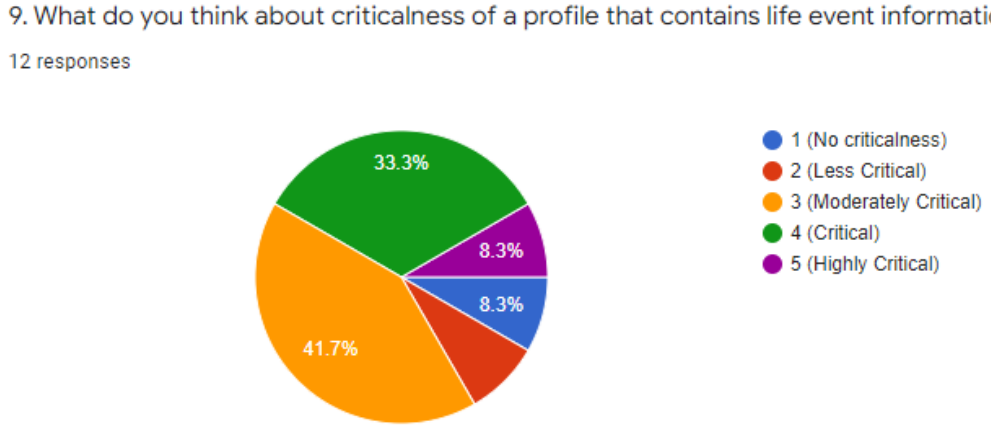


FIGURE 4.9: Q9: for Expert

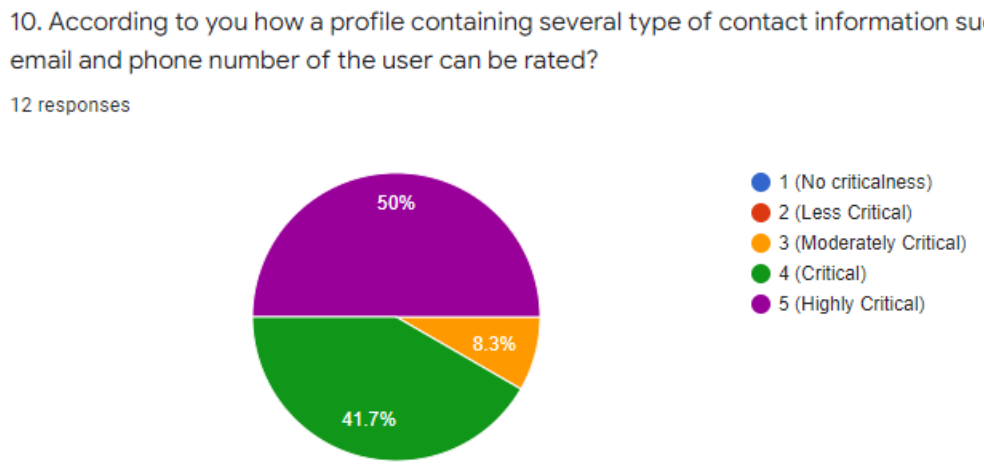


FIGURE 4.10: Q10: for Expert

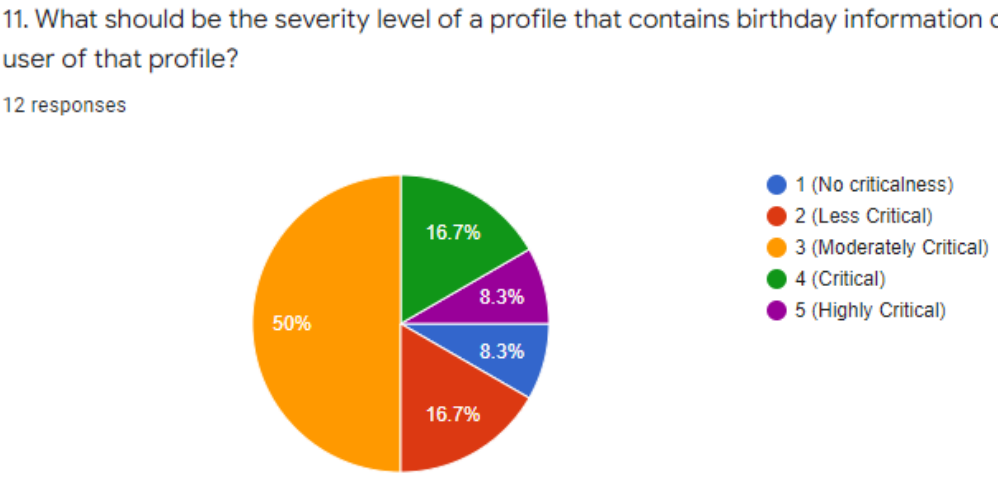


FIGURE 4.11: Q11: for Expert

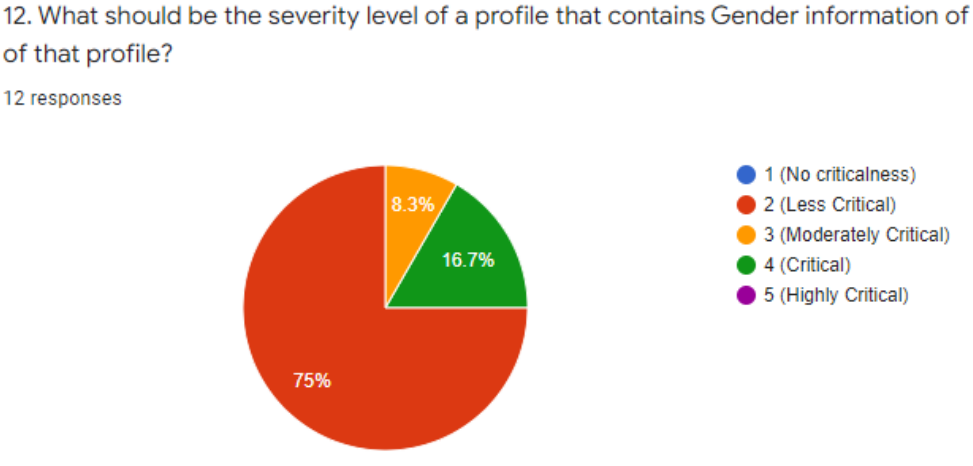


FIGURE 4.12: Q12: for Expert

4.7.1 Average of Severity Scores from Experts

Total of twelve field experts responded to the questionnaire. For the twelve of the experts who filled the questionnaire, each person assigned a severity rating to a specific information type.

The score assigned by each expert is summed up and then divided by 12 to calculate an average severity rating for a specific type of information. The detailed average scores are shown in table 4.7

TABLE 4.7: Average of scores of experts

Information Type	**Average Score**
Work/Job	2.5
Residence	2.5
School/College	1.9
Relationship Status	1.9
hobbies	1.6
Family Members	2.8
Details about you	1.6
Popular questions	1.5
Life event	2.25
Contact Information	3.4
Birthdate	2
Gender	1.4

In the table, the first column displays the type of information and the second column displays the calculated average score for that information type. The average is calculated by adding the assigned score of all experts for each information, and then the sum of all scores is divided by twelve to get an average score. This same formula is applied for calculating the average of all information types. After calculating the average of expert's assigned scores, the results after the computation of average are as follows.

The severity score for Work/job information becomes 2.5, the score of residence information is 2.5. school/college type information score is 1.9. Similarly, the score for contact information is 3.4, the score for gender type information is 1.4. Just like this calculated average score for each type of information is displayed against the information type.

4.8 Scoring of the Information Types by General Public

Just like the method of getting scores from experts, where a questionnaire was sent to experts and each one of them provided a score to the information type. A similar questionnaire was designed to get an understanding of public.

How the general public understands information on social media. and what is the importance of a specific type of information that is found on the profile of Facebook. To get an insight of this concept, a similar questionnaire with almost the same number and type of questions were asked from the public. Except that the target audience of this research is the student and the employers of any organization. The overall statistics of the responses received from public are as follows.

From the overall participants who responded to the questionnaire:

- 61.1% were Students
- 38.9% were employee of some organization

The major audience who solved the questionnaire consists of students. Rest of the questions in the questionnaire, sent to public were same as of the questionnaire provided to the experts.

The overall statistics of the results of public questionnaire is displayed in table 4.8.

Unlike the scores obtained from the questionnaire of experts, here it can be seen that the information type work/Job is scored as zero or non critical by 9.5% of the public. 21.4% scored it as less critical. 31% scored the information as moderately critical. 24.6% assigned critical score that is 3 to this information and 13.5% think that this information is highly critical. A difference between the scores of public and the expert can be seen from the results. There are some information types,

TABLE 4.8: Scores of public

Information Type	0	1	2	3	4
Work/Job	9.5	21.4	31	24.6	13.5
Residence	12.7	20.6	19.8	24.6	22.2
School/College	15.9	27	27	18.3	11.9
Relationship Status	18.3	24.6	32.5	17.5	7.1
hobbies	24.6	27.8	27	17.5	3.2
Family Members	7.9	20.6	25.4	21.4	24.6
Details about you	27.8	23.8	23.8	12.7	11.9
Popular questions	24.6	30.2	23.8	16.7	4.8
Life event	24.6	23.8	23.8	17.5	10.3
Contact Information	7.9	10.3	20.6	20.6	40.5
Birthdate	15.9	33.3	26.2	12.7	11.9
Gender	23.8	31	20.6	19	5.6

that the public thinks is not important with respect to the social engineering attack and information leakage.

Similarly, the table contains all the available information types in the first column and possible score in the rest of the columns. Complete statistics regarding the scoring of the information is provided in the table.

4.8.1 Average of Scores Assigned by Public

Total of 126 public members filled the questionnaire and assigned a rating to the questions asked. The scores that were assigned by the public against each information type is summed up and divided by 126 to calculate the average severity score of the information type. The detailed scores are shown by using the pie charts and tables.

After observing the responses and calculating the average scores of the information types, the average of work/job information becomes 2.11. residence information's average severity is 2.23 and just like this, average severity score of each information type can be seen in the table 4.9. The table displays the average score calculated for each type of information, the work and job information has average score 2.11, where as the score for residence is 2.23. Just like this, each information type has its average score written in front of it in the table given. The pie-charts of the

TABLE 4.9: Average of scores of public

Information Type	Average Score
Work/Job	2.11
Residence	2.23
School/College	1.83
Relationship Status	1.70
hobbies	1.46
Family Members	2.34
Details about you	1.57
Popular questions	1.38
Life event	2.13
Contact Information	2.75
Birthdate	1.71
Gender	1.51

public scores are provided and just like the previous charts, these also show the percentage of public that selected a specific answer for an information type.

As can be seen in the pie charts. For the following information types:

1. **Work/Job**: In Figure 4.13 9.5% think that it has no criticalness. 21.4% think that it is less critical 31% think, it is moderately critical. 24.6% think it is critical and 13.5% think that it is highly critical.

2. **Residence**: In Figure 4.14 12.7% think that it has no criticalness. 20.6% think that it is less critical 19.8% think, it is moderately critical. 24.6% think it is critical and 22.2% think that it is highly critical.

3. **Relationship**: In Figure 4.16 18.3% think that it has no criticalness. 24.6% think that it is less critical 32.5% think, it is moderately critical. 17.5% think it is critical and 7.1% think that it is highly critical.

4. **Contact**: In Figure 4.22 7.9% think that it has no criticalness. 10.3% think that it is less critical 20.6% think, it is moderately critical. 20.6% think it is critical and 40.5% think that it is highly critical.

5. **Gender**: In Figure 4.24 23.8% think that it has no criticalness.31% think that it is less critical 20.6% think, it is moderately critical. 21.9% think it is critical and 5.6% think that it is highly critical.

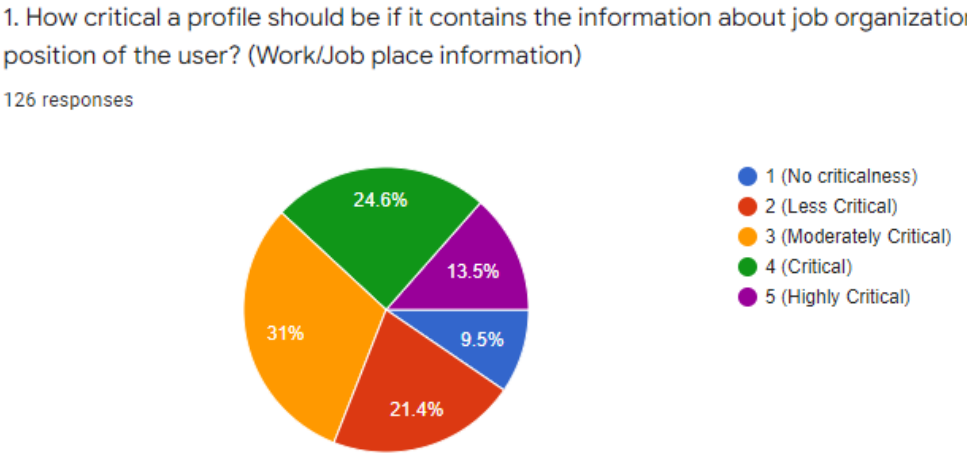


FIGURE 4.13: Q1: for Public

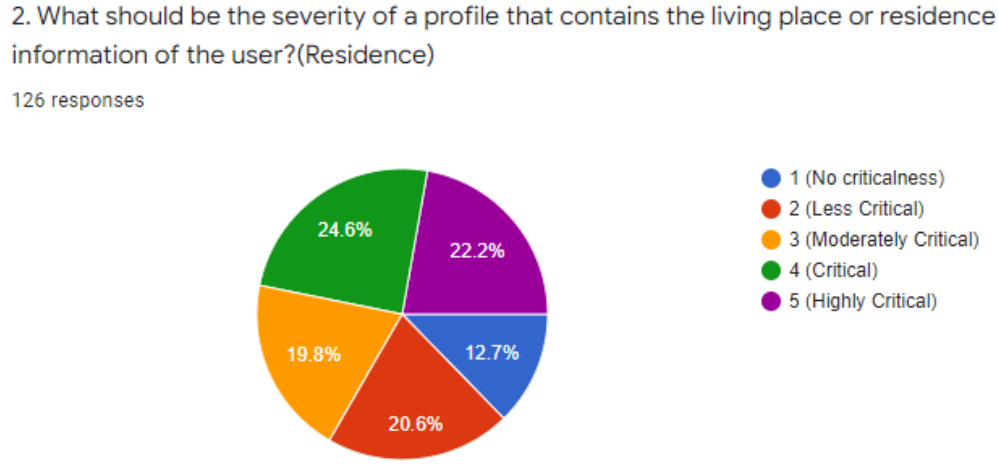


FIGURE 4.14: Q2: for Public

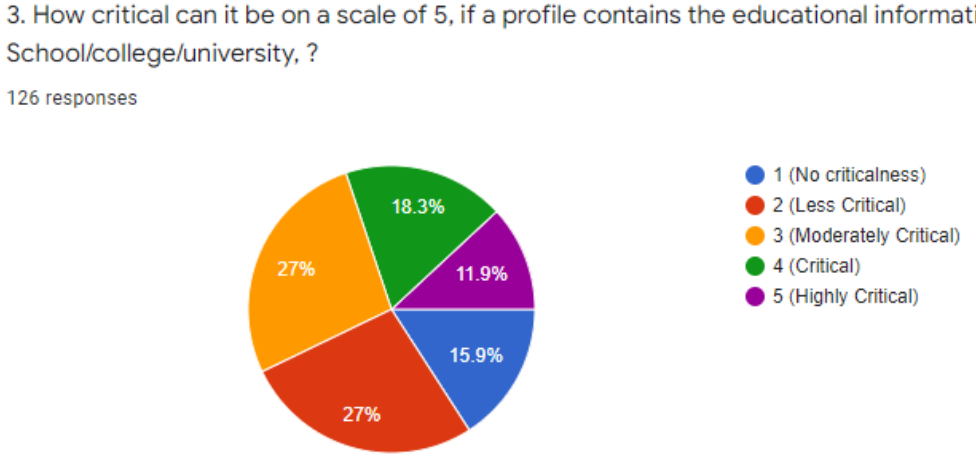


FIGURE 4.15: Q3: for Public

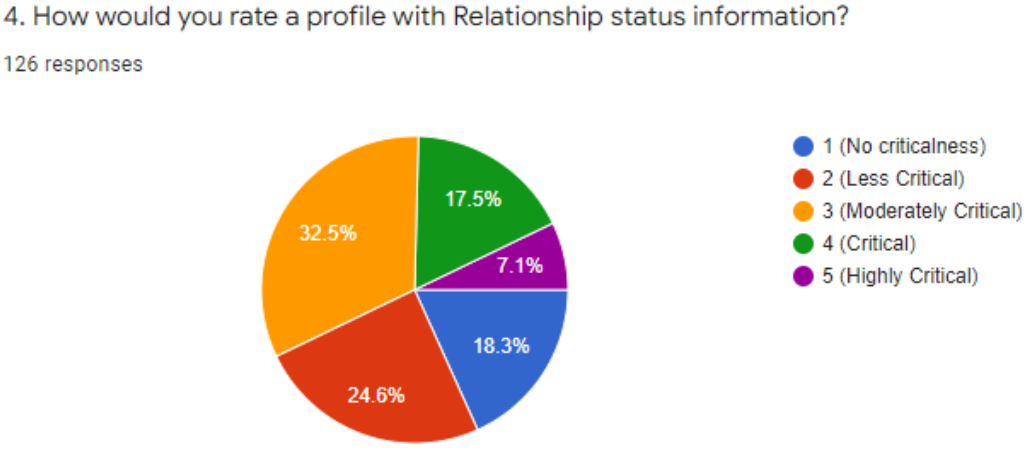


FIGURE 4.16: Q4: for Public

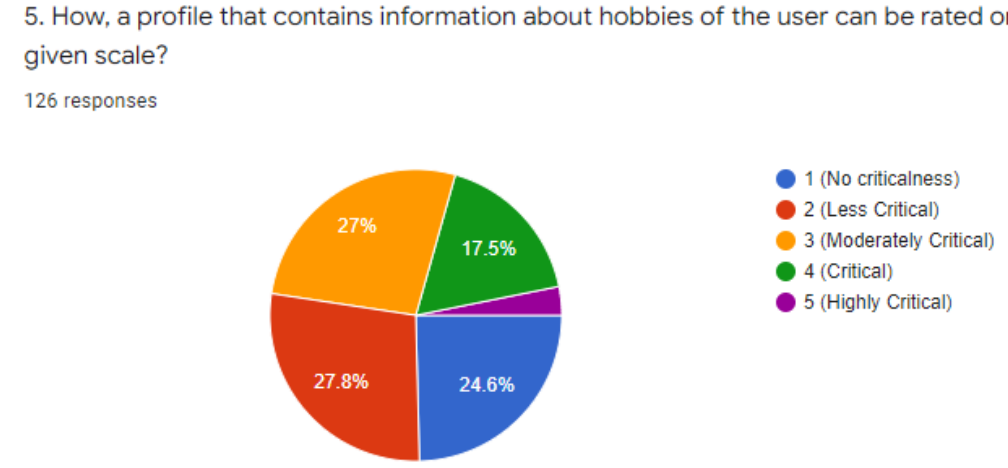


FIGURE 4.17: Q5: for Public

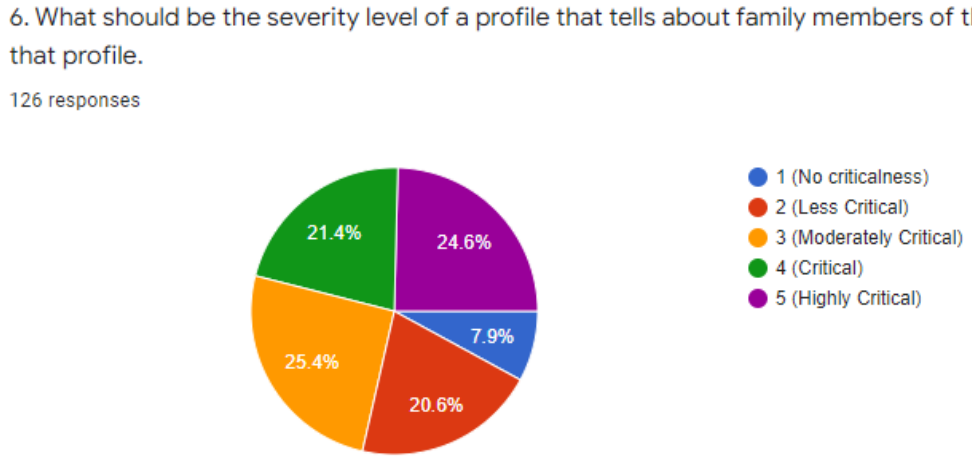


FIGURE 4.18: Q6: for Public

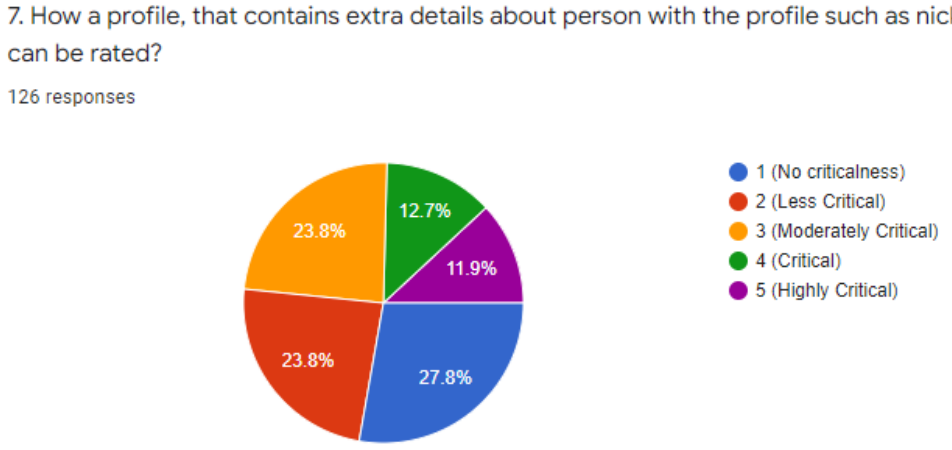


FIGURE 4.19: Q7: for Public

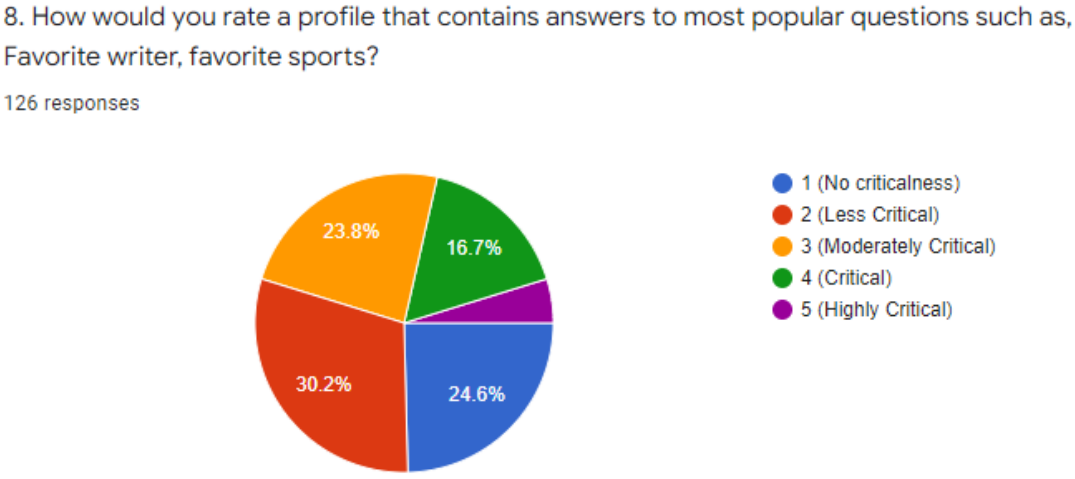


FIGURE 4.20: Q8: for Public

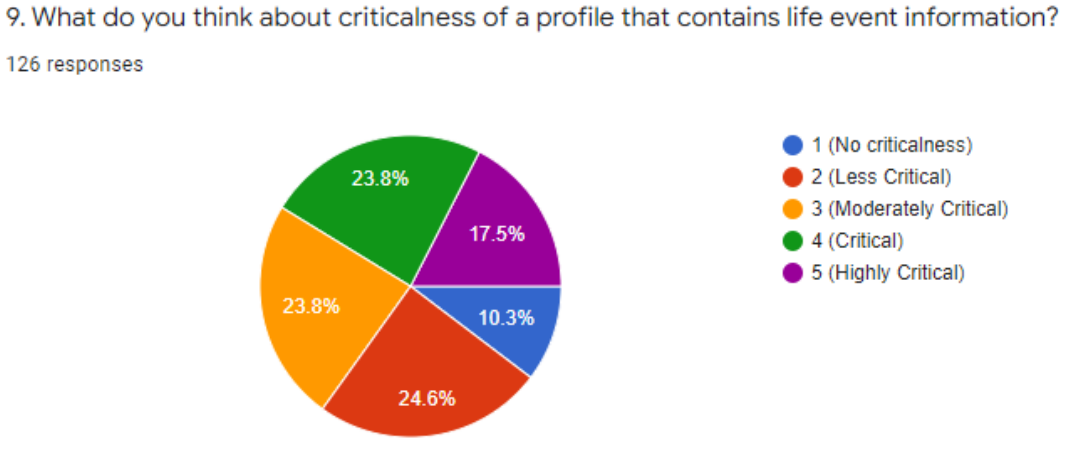


FIGURE 4.21: Q9: for Public

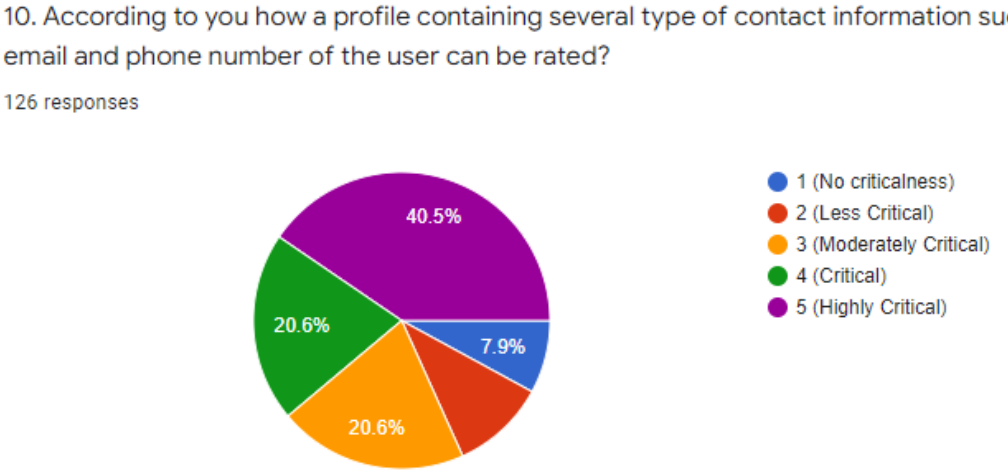


FIGURE 4.22: Q10: for Public

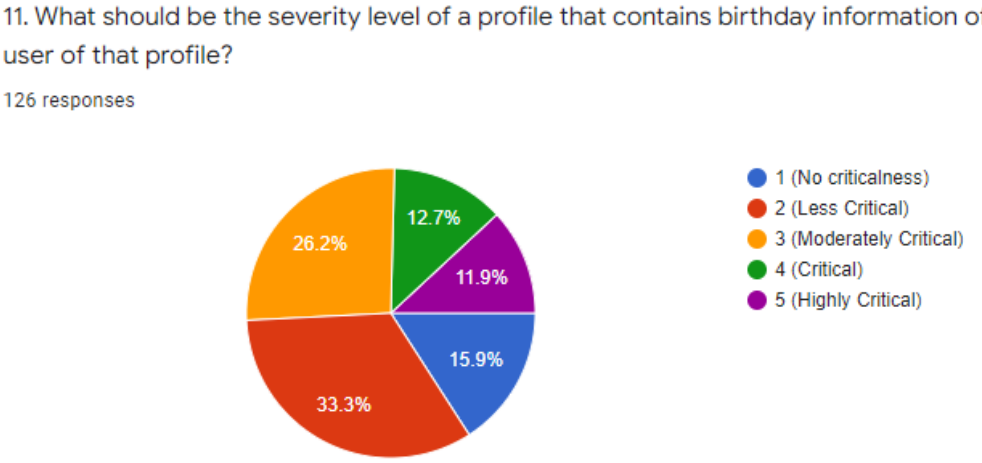


FIGURE 4.23: Q11: for Public

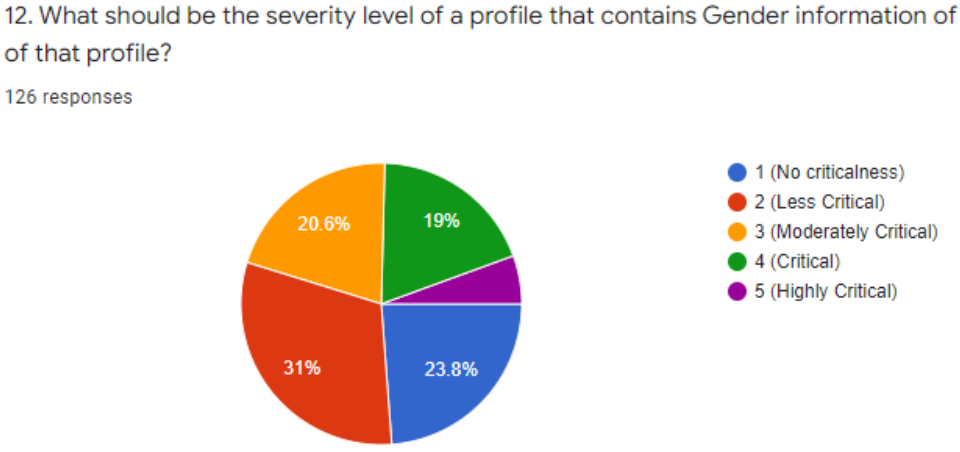


FIGURE 4.24: Q12: for Public

4.9 Comparison of Proposed System Results with Experts' Results

After the completion of result generation from both the proposed system and the expert questionnaire. The next step is to perform the comparison and check the difference between the scores.

For this purpose the percent difference formula will be used.

4.9.1 Percent Difference

The percent Difference is referred to as the relative difference between two values [1]. It is calculated by multiplying the ratio of their difference and their average with 100.

For comparing the two results, this percent formula is used and the difference between the values is expressed in percentage in the table below:

TABLE 4.10: Average of scores of public

Information Type	Proposed results	Expert's results	Percent Difference
Work/Job	3	2.5	18.18
Residence	4	2.5	46.15
School/College	3	1.91	44.06
Relationship Status	3	1.91	44.06
hobbies	3	1.66	57.14
Family Members	3	2.83	5.71
Details about you	4	1.66	82.35
Popular questions	4	1.58	86.56
Life event	3	2.25	28.57
Contact Information	3	3.14	12.77
Birthdate	3	2	40
Gender	3	1.41	71.69

Table 4.10 shows the comparison of the two results and calculates the percent difference.

[1] https://byjus.com/percent-difference-formula/

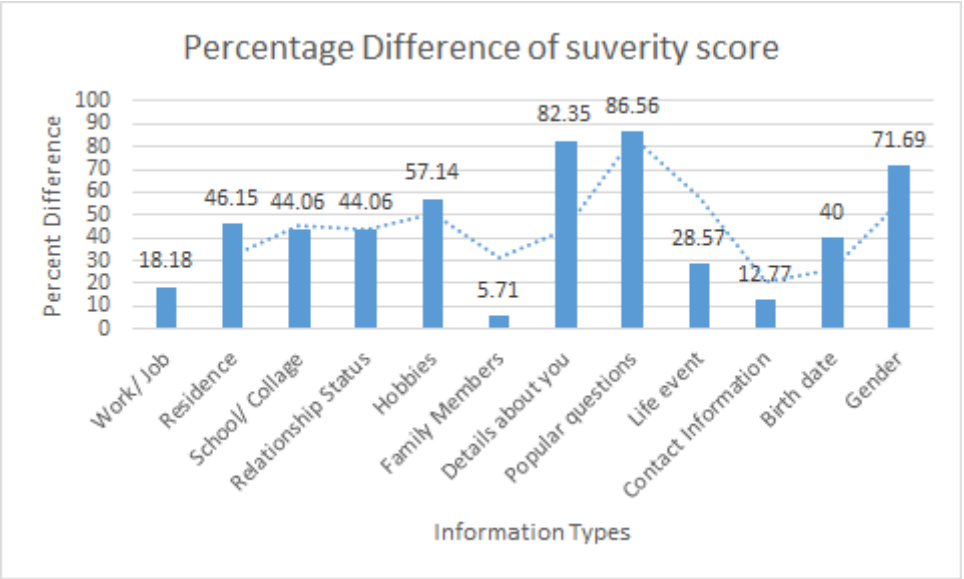


FIGURE 4.25: Percentage difference of the two results

To calculate the percent difference of Work/Job information type, the expert's score is subtracted from the score of proposed system. Then the average is calculated by adding both the values and dividing by two. once the average is calculated, it divides the subtraction result and a multiplication with 100 is performed to generate the percent result. Hence, the work/job information's percent difference is calculated as 18.18.

The operations for calculating the percent difference of the work/job information are repeated for every type of information and the relative difference is found between the two scores.

In Figure 4.25 percentage difference can be seen. The information types with relative difference, less than 50% are as follows:

1. **Work/Job** with difference = 18.18%
2. **Residence** with difference = 46.15%
3. **School/College/university** with difference = 44.06%
4. **Relationship Status** with difference = 44.06%
5. **Family Members** with difference = 5.71%

6. **Life events** with difference = 28.57%
7. **Contact** with difference = 12.77%
8. **Birthday** with difference = 40%

After analysing the scores and difference it can be seen that the family member, Contact, Work/job scores are calculated with a very less difference.

4.10 Inter-rater Agreement

For a better understanding of the scoring of information severity and to know the agreement of the experts upon a specific information type.

TABLE 4.11: Inter-rater agreement of experts over each information type

Information Type	Inter-rater Agreement
Work/Job	21%
Residence	29%
School/College	29%
Relationship Status	29%
hobbies	33%
Family Members	23%
Details about you	30%
Popular questions	26%
Life event	24%
Contact Information	38%
Birth date	26%
Gender	56%

Table 4.11 shows the agreement of experts over the scores of a specific type of information. As discussed earlier each expert has provided a score against each type of information and has given a severity level. For a better understanding and to know about how much experts agree with each other. The inter-rater agreement is calculated for each type of information within the twelve experts that provided the score.

The results show that their is 21% agreement between the scores of work/job information. Similarly for information type Residence, Educational info,Relationship

status 29% agreement can be seen. between all these information the highest agreement is for the Gender information, where 56% of the experts agree. The results can also be seen in the chart below.

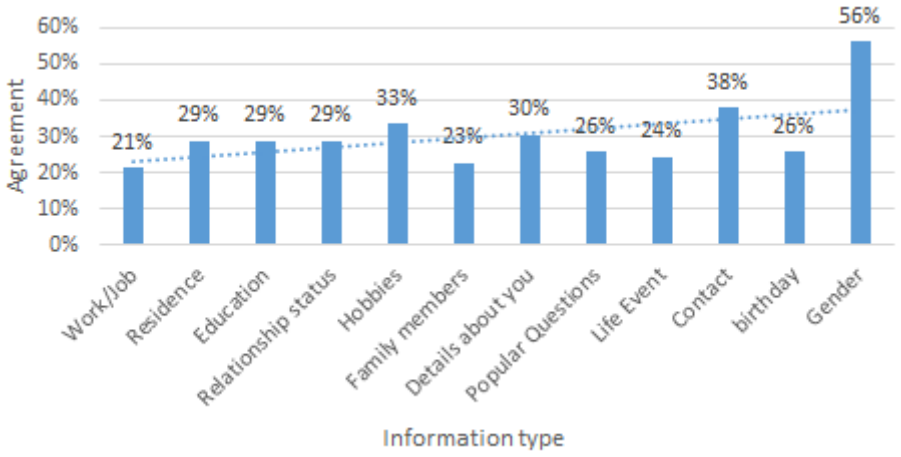


FIGURE 4.26: Inter-Rater Agreement of the experts

4.11 Recommendations

Upon critically analysing the publicly available information on Facebook with respect to Cyber attacks, such as Social Engineering attack. It is found that there are several types of attacks or ways that can be adopted by any hacker or attacker to perform an attack on the user. Such as phishing attack by use of phishing emails on a user, who has provided the contact information on his/her Facebook profile.

A hacker can use the publicly available contact information from a user's Facebook profile and send him phishing links via his email or contact number and lure him in a trap. Just like this example there can be many types of ways, a user can be targeted and damaged. This section provides a list of recommendations for the users of social media platforms. By adopting and following these recommendations, one can avoid and minimize the possibility of being attacked on any of the social media platform. A list of recommended steps to avoid any attacks are provided in the next section. All the recommendations, that are provided, are based on the findings of this research.

- **Information Revelation:** While a user is creating a Facebook account, it requires some personal information to complete the profile creation process. Such as, a user's first and last name, date of birth, contact information like email or contact number and gender etc. is required at the time of profile Creation. Once the profile is created, to connect with the rest of the world and to find the people with similar interest and field, Facebook needs some additional information such as your Job information, your educational background, hobbies, favorite artist/movies etc. But providing these information is always optional. A user can decide whether he/she wants to provide an information or not. So, it is recommended that at the time of profile creation or even while setting your profile, a user should carefully observe and check, which information the platform is asking and if it is really necessary to provide it or not.

- **Privacy Settings:** First and foremost recommended step for avoiding the information leakage is by setting the proper privacy configuration on the provided information. Facebook provides several privacy settings for the information and data provided on a user's profile. These privacy settings include several options like public, friends only and only me etc. These privacy settings are already explained earlier in detail in this chapter. A user should carefully set the privacy settings on each of the provided information on his/her profile. As an information leakage can be a cause of confidentiality breach and can even cause some potential damage in worst case.

- **Friend Requests:** Once the profile completion process is complete, if the user has not set up the privacy configurations on the information provided on the profile, the Facebook sets the settings to default. On default settings some of the information is only shown to the friends. Adding friends on Facebook is one the main feature of all the social media platforms. This feature allows users to send and accept friend requests of people from all over the world. A user may receive many requests on daily basis, it is hereby recommended to verify and review the profile of the request sender. A hacker can also approach a user by stealing his family/friends account.

- **Unknown/Phishing Messages:** Many of the phishing attacks are launched by phishing emails or phishing messages. A user can be lured in an attack by the use of phishing links. Usually phishing attacks start by the sending a message to the victim that contains an interesting context and a link. For example, an attacker can send a message regarding a party's picture gallery and have link attached with the message or email. Upon clicking the link a script can be executed and user login credentials can be captured. So, upon receiving any such message from some unknown user or even a friend, it is recommended to not click the links until unless it is verified that the link is not malicious.

  Also, to avoid such attacks, a user should keep the contact information private and only share the information with others, when necessary

- **Educational and Work information:** Some users provide educational information on their profiles, such as current school or university on their profiles and make it public. An attacker can approach the user and perform the baiting attack on the victim. Similarly, some users reveal the work and job information, such as job position and the organization that they work in. Such users can become the victim of the shoulder surfing attack. In such cases, it is recommended that such information should be kept private, because in worst cases, they can be a cause of damage at personal or even organization level.

  The findings of the study suggest that each and every type of information, that is provided on these platforms has its own importance and they should not be made public.

Chapter 5

Implementation of the Proposed System

5.1 Introduction

After the completion of the scoring phase and comparing the result with scores of experts, the proposed solution can be implemented using any of the current platforms. A demonstration of the basic implementation is provided in this section.

5.2 Implementation Technology

For the implementation of the system, an android application is built using JAVA and the XML interfaces.

Currently the app is used to provide login interface, where a user can login in the application and check the publicly accessible information present on the profile of that individual.

Once logged in the app shows another screen where it shows the publicly accessible information. Now as the information is gathered, the proposed solution can be applied to it to calculate the final severity scores of each type of accessible information.

5.2.1 Android Studio

Android studio is an IDE(Integrated Development Environment). It is used by the developers to develop android OS based applications. For developing the android application of the proposed system, this IDE is used and the programming language used for writing the back-end logic is JAVA.

5.2.2 JAVA

JAVA is a programming language, that is classified in the High-level Category of the programming languages. This language is used by the developers to create different types of applications such as, android applications, desktop application, web application and Enterprise applications.

This language is used to develop the android application for the proposed system. Mainly, it will be used write the back-end code of the application.

5.2.3 XML

"Extensible Markup Language" also known as XML is a language that is mostly used to create the interfaces of different types of application. The android platform also uses XML to design and modify the interfaces of the application. This language is also used for storing the data in a specific format.

5.3 FACEBOOK Graph API

The Facebook Graph API is the HTTP-based API that is mainly used for the purpose of linking third party applications to Facebook social media platform. Also this API helps to query a specific type of data from Facebook or sending data to Facebook.
For the application of the proposed system this API is used to provide users the

Facebook login functionality and then the desired information is gathered by using the API's ME method.

The Graph API is a free tool to be used by the developers and it provides a vast range of functionalities.

5.4 Interfaces of the Application

This section provides the interfaces to the developed application and their working.

5.4.1 Login Screen

Figure 5.1 shows the Main screen of the android application. The screen is developed using android studio and the XML language. The XML is used to write the front end code and JAVA programming language is used to write the back-end logic. This app allows the user to easily login the Facebook profile upon pressing of a single button. The button connects the user to the Facebook login activity.

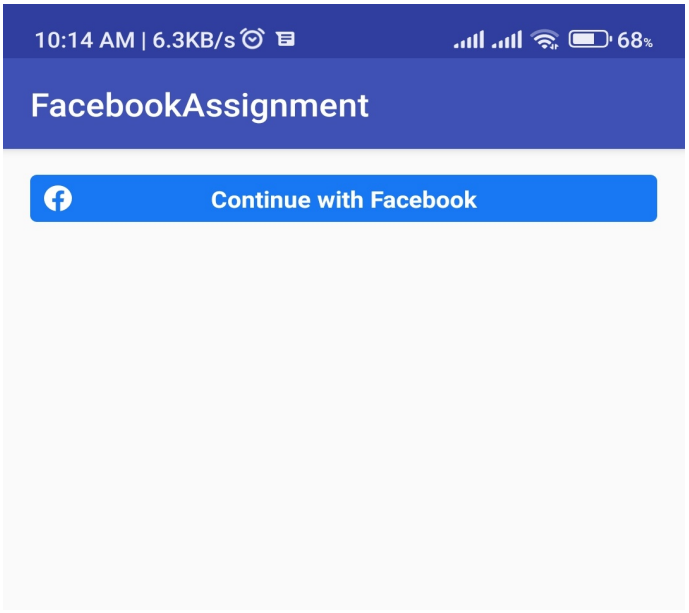


FIGURE 5.1: Screen 1: Login Screen

As shown in the figure 5.1 the android application first provides a button to the user that displays the text "Continue with Facebook". Upon pressing the button

the app makes a call to the Facebook application and prompts the login functionality. The user is automatically logged in if he/she is logged in, in the Facebook application. Otherwise, the app shows a login screen sent by Facebook API and then the user gives the credential for his/her profile.

5.4.2 Information Screen

The figure 5.2 shows the interface for the second screen of the android application. For the development of the interface, markup language used is XML and the the formatting of the data to be displayed on the screen is done by using the same language.

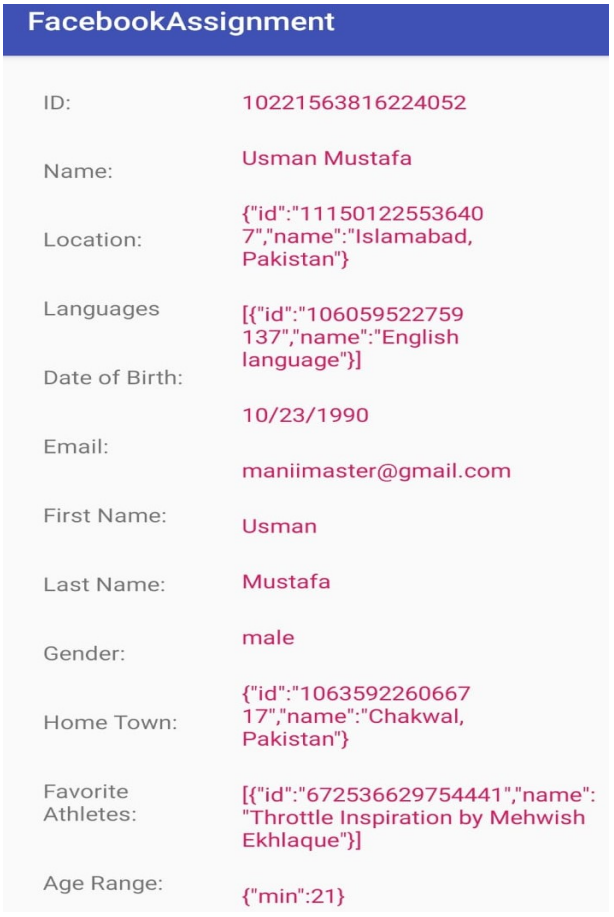


FIGURE 5.2: Screen 2: Information Screen

Once the user provides the login credential the app gets the access to the profile information. This is done by using the Facebook Graph API. The app then, Makes

a call to the ME function of the Graph API and also sends the type of information that is required. The Graph API returns the information in the JSON object format. That object is then parsed and the required information is filtered out.

5.5 Further Working of the Application

The previous sections provided the in-depth working of each activity and interface and their working. It can be seen that the app is successful in gathering and storing the available information that is publicly accessible from a profile of Facebook. The next step is to apply the proposed technique on the extracted information types and calculate the severity ratings according to the proposed scale 5.3. It can be done by calculating the value of each type of parameter for the equation and then performing operations to calculate the actual score of the severity.

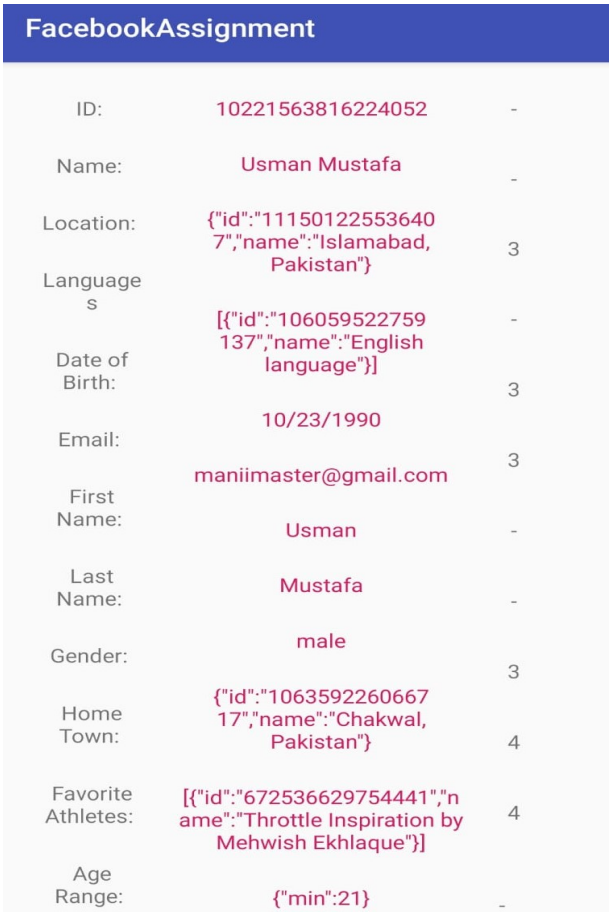


FIGURE 5.3: Screen 3: Information with scores

Chapter 6

Conclusion and Future Work

A system is proposed to calculate the severity of publicly available information on a Facebook user profiles. The scores are calculated through different steps. Public understanding of social network based cyber-attacks and information privacy is understood by preparing a questionnaire. Moreover, for comparison of scores of proposed system, the severity of information type is assigned from the field experts. After the comparison the correlation is computed by calculating the percentage difference. The results show that the family member, Contact, Work/job scores have very less difference as compared to the scores of experts, which is 5.71, 18.18, 12.77 respectively. An android based implementation is also done and it is demonstrated that an application can be built using the idea. From the comprehensive Literature review, it was identified that no work has been done in the past in this direction. for the future work:

- This idea can be improved by introducing more correlation coefficients to increase the credibility of the solution.
- Training of general public as well as students and employees can be done to make them aware of the threats and criticalness of the information that they make public on their social media profile.
- For the implementation point of view, the app can be made better by extracting more information and performing the calculations on the data.

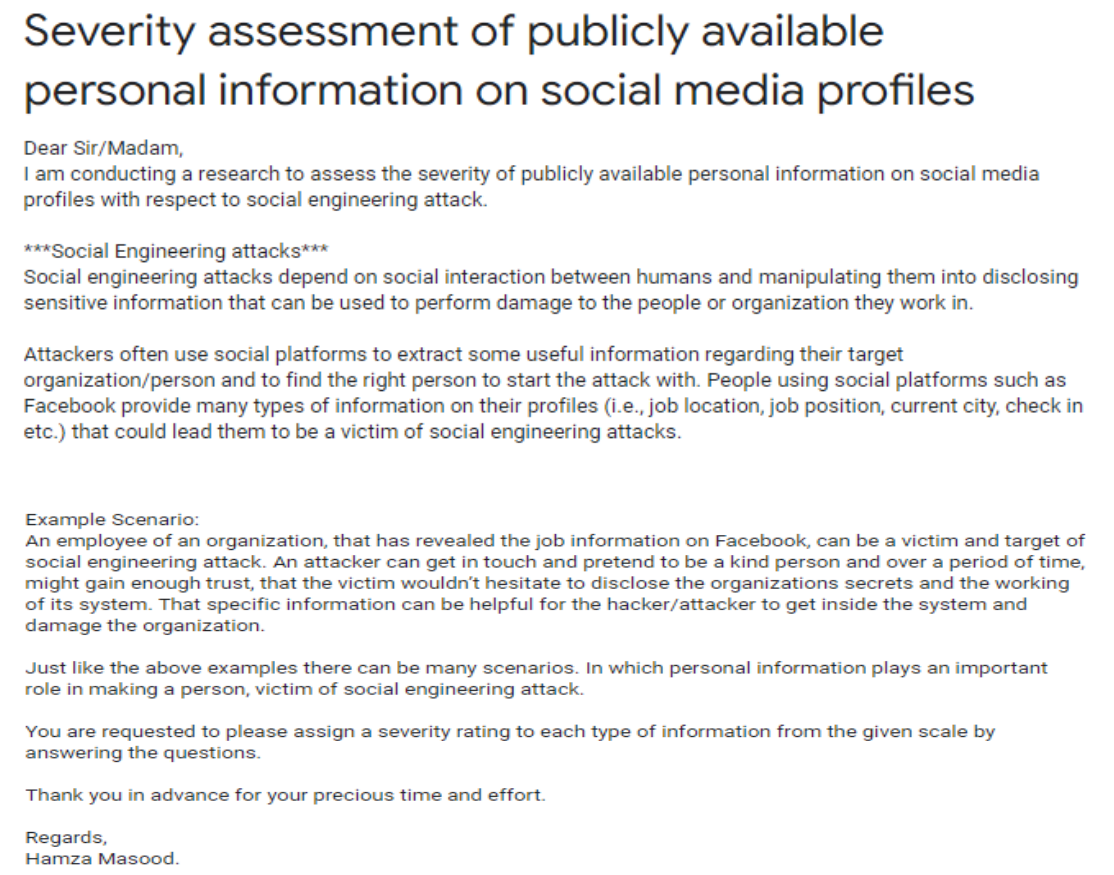
- An Auditing tool can be developed by using this idea, for different organizations, where the social media profiles of employees can be fed to the tool and checked for the public information. The tool can check the profiles of employees and notify about the information that is present on the profiles, that can be cause damage or can be used in performing social engineering attack.

- The android application will be uploaded to the Google Play Store and the reviews of general public will be analyzed to improve the idea.

Appendix A

Questionnaire Design for Experts

This section contains the Questionnaire, that was designed to get the scores of information types from Experts. The questionnaire is available online https://docs.google.com/forms/d/1GYROumVC7EfKXq6NCS-eHVf6rAuaWOZOWvvp_AKFE2Q



Severity assessment of publicly available personal information on social media profiles

Dear Sir/Madam,
I am conducting a research to assess the severity of publicly available personal information on social media profiles with respect to social engineering attack.

Social Engineering attacks
Social engineering attacks depend on social interaction between humans and manipulating them into disclosing sensitive information that can be used to perform damage to the people or organization they work in.

Attackers often use social platforms to extract some useful information regarding their target organization/person and to find the right person to start the attack with. People using social platforms such as Facebook provide many types of information on their profiles (i.e., job location, job position, current city, check in etc.) that could lead them to be a victim of social engineering attacks.

Example Scenario:
An employee of an organization, that has revealed the job information on Facebook, can be a victim and target of social engineering attack. An attacker can get in touch and pretend to be a kind person and over a period of time, might gain enough trust, that the victim wouldn't hesitate to disclose the organizations secrets and the working of its system. That specific information can be helpful for the hacker/attacker to get inside the system and damage the organization.

Just like the above examples there can be many scenarios. In which personal information plays an important role in making a person, victim of social engineering attack.

You are requested to please assign a severity rating to each type of information from the given scale by answering the questions.

Thank you in advance for your precious time and effort.

Regards,
Hamza Masood.

What is your profession? *

- Self-Employed
- Professor/Teacher
- Developer
- IT Specialist/Consultant
- Information security specialist/Consultant

What is your field of work? *

- Penetration Testing
- Cryptographer
- Security Analyst
- Security Consultant
- Cryptanalyst
- Security Administrator

How much experience do you have in Information Security field? *

- 1-5 years
- 6-10 years
- 11-15 years
- more than 15 years

You are requested to answer the questions by selecting only one most appropriate option from the following scale.

1 = No criticalness
(An information with almost no help in social engineering attack.)

2 = Less Critical
(An information that is not directly involved but helps in the social engineering attack i.e. information that helps to develop friendship/trust with the victim)

3 = Moderately Critical
(An information that leads to effect or cause damage to a single person i.e. information that helps in landing an attack on a single person)

4 = Critical
(An information that leads to cause damage to a number of people i.e. if an account gets hacked then, the hacker can target the people in the friend list of that account)

5 = Highly Critical
(An information that leads to cause damage on an organizational level i.e. information that lures the attacker who wants to target a specific company/organization)

Please note that the questions are asked in the context of Social engineering attacks that can be performed by using each type of information. So the severity levels should be provided accordingly.

1. How critical a profile should be if it contains the information about job organization and job position of the user? (Work/Job place information) *

- 1 (No criticalness)
- 2 (Less Critical)
- 3 (Moderately Critical)
- 4 (Critical)
- 5 (Highly Critical)

2. What should be the severity of a profile that contains the living place or residence information of the user?(Residence) *

- 1 (No criticalness)
- 2 (Less Critical)
- 3 (Moderately Critical)
- 4 (Critical)
- 5 (Highly Critical)

3. How critical can it be on a scale of 5, if a profile contains the educational information like School/college/university, ? *

- 1 (No criticalness)
- 2 (Less Critical)
- 3 (Moderately Critical)
- 4 (Critical)
- 5 (Highly Critical)

4. How would you rate a profile with Relationship status information? *

- 1 (No criticalness)
- 2 (Less Critical)
- 3 (Moderately Critical)
- 4 (Critical)
- 5 (Highly Critical)

5. How, a profile that contains information about hobbies of the user can be rated on the given scale? *

- 1 (No criticalness)
- 2 (Less Critical)
- 3 (Moderately Critical)
- 4 (Critical)
- 5 (Highly Critical)

6. What should be the severity level of a profile that tells about family members of the user of that profile. *

- 1 (No criticalness)
- 2 (Less Critical)
- 3 (Moderately Critical)
- 4 (Critical)
- 5 (Highly Critical)

7. How a profile, that contains extra details about person with the profile such as nickname, can be rated? *

- 1 (No criticalness)
- 2 (Less Critical)
- 3 (Moderately Critical)
- 4 (Critical)
- 5 (Highly Critical)

8. How would you rate a profile that contains answers to most popular questions such as, Favorite writer, favorite sports? *

- 1 (No criticalness)
- 2 (Less Critical)
- 3 (Moderately Critical)
- 4 (Critical)
- 5 (Highly Critical)

9. What do you think about criticalness of a profile that contains life event information? *

- 1 (No criticalness)
- 2 (Less Critical)
- 3 (Moderately Critical)
- 4 (Critical)
- 5 (Highly Critical)

10. According to you how a profile containing several type of contact information such as, email and phone number of the user can be rated? *

- 1 (No criticalness)
- 2 (Less Critical)
- 3 (Moderately Critical)
- 4 (Critical)
- 5 (Highly Critical)

11. What should be the severity level of a profile that contains birthday information of the user of that profile? *

- 1 (No criticalness)
- 2 (Less Critical)
- 3 (Moderately Critical)
- 4 (Critical)
- 5 (Highly Critical)

12. What should be the severity level of a profile that contains Gender information of the user of that profile? *

- 1 (No criticalness)
- 2 (Less Critical)
- 3 (Moderately Critical)
- 4 (Critical)
- 5 (Highly Critical)

Appendix B

Questionnaire Design for Public

This section contains the Questionnaire, that was designed to get the scores of information types from General public. The questions for severity collection are same. The questionnaire is available online at https://docs.google.com/forms/d/1h6m3YqbznrNcLjtwXN_wyNDNgNKlqeeQfCerzDQ6UNc/. The only difference is the question asking for the profession, that is shown below:

Bibliography

[1] S. M. Albladi and G. R. Weir, "User characteristics that influence judgment of social engineering attacks in social networks," *Human-centric Computing and Information Sciences*, vol. 8, no. 1, pp. 1–24, 2018.

[2] D. Choi, Y. Lee, S. Kim, and P. Kang, "Private attribute inference from facebook's public text metadata: a case study of korean users," *Industrial Management & Data Systems*, 2017.

[3] A. F. AL-Otaibi and E. S. Alsuwat, "A study on social engineering attacks: Phishing attack," 2020.

[4] N. Akhtar, "Social network analysis tools," in *2014 fourth international conference on communication systems and network technologies*, pp. 388–392, IEEE, 2014.

[5] M. Nuzhat, K. C. Soo, L. N. Yong, and Y. Jinhong, "Entertaining apps: A gateway to personal data breach,"

[6] T. Limba and A. Šidlauskas, "Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the facebook," *Entrepreneurship and Sustainability Issues*, vol. 5, no. 3, pp. 528–541, 2018.

[7] J. G. Cabañas, Á. Cuevas, and R. Cuevas, "Unveiling and quantifying facebook exploitation of sensitive personal data for advertising purposes," in *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pp. 479–495, 2018.

[8] A. Esteve, "The business of personal data: Google, facebook, and privacy issues in the eu and the usa," *International Data Privacy Law*, vol. 7, no. 1, pp. 36–47, 2017.

[9] A. Algarni, Y. Xu, and T. Chan, "Measuring source credibility of social engineering attackers on facebook," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 3686–3695, IEEE, 2016.

[10] T. Mataracioglu and S. Ozkan, "User awareness measurement through social engineering," *arXiv preprint arXiv:1108.2149*, 2011.

[11] J. Onaolapo, N. Leontiadis, D. Magka, and G. Stringhini, "Socialheisting: Understanding stolen facebook accounts," in *30th {USENIX} Security Symposium ({USENIX} Security 21)*, 2021.

[12] S. Kosznik-Biernacka *et al.*, "The analysis of risks to personal data security," *Security Dimensions. International and National Studies*, no. 34, pp. 256–267, 2020.

[13] A. Jamil, K. Asif, Z. Ghulam, M. K. Nazir, S. M. Alam, and R. Ashraf, "Mpmpa: A mitigation and prevention model for social engineering based phishing attacks on facebook," in *2018 IEEE International Conference on Big Data (Big Data)*, pp. 5040–5048, IEEE, 2018.

[14] J. L. Pinchot and K. L. Paullet, "What's in your profile? mapping facebook profile data to personal security questions," *Issues in Information Systems*, vol. 13, no. 1, pp. 284–293, 2012.

[15] R. Stiennon, "Categorizing data breach severity with a breach level index," *URL: https://breachlevelindex. com/pdf/Breach-Level-Index-WP. pdf*, 2013.

[16] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," in *2016 international conference on computing, communication and automation (ICCCA)*, pp. 537–540, IEEE, 2016.

[17] D. Irani, S. Webb, K. Li, and C. Pu, "Modeling unintended personal-information leakage from multiple online social networks," *IEEE Internet Computing*, vol. 15, no. 3, pp. 13–19, 2011.

[18] J. P. Calbalhin, "Facebook user's data security and awareness: A literature review," *Journal of Academic Research*, vol. 3, no. 2, pp. 1–13, 2018.

[19] F. McCown and M. L. Nelson, "What happens when facebook is gone?," in *Proceedings of the 9th ACM/IEEE-CS joint conference on Digital libraries*, pp. 251–254, 2009.

[20] A. Nahi, "Social network privacy models: A systematic literature review and directions for further research," in *3rd International Conference on Communication Engineering and Computer Science (CIC-COCOS'19)*, 2019.

[21] R. Farahbakhsh, X. Han, A. Cuevas, and N. Crespi, "Analysis of publicly disclosed information in facebook profiles," in *2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2013)*, pp. 699–705, IEEE, 2013.

[22] S. Ali, N. Islam, A. Rauf, I. U. Din, M. Guizani, and J. J. Rodrigues, "Privacy and security issues in online social networks," *Future Internet*, vol. 10, no. 12, p. 114, 2018.

[23] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," *IEEE network*, vol. 24, no. 4, pp. 13–18, 2010.

[24] I. Kayes and A. Iamnitchi, "Privacy and security in online social networks: A survey," *Online Social Networks and Media*, vol. 3, pp. 1–21, 2017.

[25] J. Lindamood, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "Inferring private information using social network data," in *Proceedings of the 18th international conference on World wide web*, pp. 1145–1146, 2009.

[26] I. Casas, J. Hurtado, and X. Zhu, "Social network privacy: Issues and measurement," in *International Conference on Web Information Systems Engineering*, pp. 488–502, Springer, 2015.

[27] S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, "Social network security: Issues, challenges, threats, and solutions," *Information sciences*, vol. 421, pp. 43–69, 2017.

[28] M. Di Martino, P. Robyns, W. Weyts, P. Quax, W. Lamotte, and K. Andries, "Personal information leakage by abusing the {GDPR}'right of access'," in *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, pp. 371–385, 2019.

[29] P.-C. Lin and P.-Y. Lin, "Unintentional and involuntary personal information leakage on facebook from user interactions," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 10, no. 7, pp. 3301–3318, 2016.

[30] N. Y. Conteh and P. J. Schmick, "Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks," *International Journal of Advanced Computer Research*, vol. 6, no. 23, p. 31, 2016.

[31] M. Greve, K. Masuch, and S. Trang, "The more, the better? compensation and remorse as data breach recovery actions-an experimental scenario-based investigation.," in *Wirtschaftsinformatik (Zentrale Tracks)*, pp. 1278–1293, 2020.

[32] N. N. A. Molok, A. Ahmad, and S. Chang, "Information leakage through online social networking: Opening the doorway for advanced persistence threats," *Journal of the Australian Institute of Professional Intelligence Officers*, vol. 19, no. 2, pp. 38–55, 2011.

[33] I. Yahav, D. G. Schwartz, and G. Silverman, "Detecting unintentional information leakage in social media news comments," in *Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014)*, pp. 74–79, IEEE, 2014.

[34] E.-A. Baatarjav, R. Dantu, and S. Phithakkitnukoon, "Privacy management for facebook," in *International conference on information systems security*, pp. 273–286, Springer, 2008.

[35] C. Manson and S. Gorniak, "Recommendations for a methodology of the assessment of severity of personal data breaches," *ENISA (European Union Agency for Network and Inform. Security) Working Document, v1. 0*, 2013.

[36] M. Mancosu and F. Vegetti, "What you can scrape and what is right to scrape: A proposal for a tool to collect public facebook data," *Social Media+ Society*, vol. 6, no. 3, p. 2056305120940703, 2020.

[37] Z. Wang, H. Zhu, and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods," *IEEE Access*, vol. 9, pp. 11895–11910, 2021.

[38] H. D. Dewi, "A research paper questionnaire based on library research," *Paradigma: Jurnal Kajian Budaya*, vol. 6, no. 1, pp. 91–101, 2016.

[39] A. Nosko, E. Wood, and S. Molema, "All about me: Disclosure in online social networking profiles: The case of facebook," *Computers in human behavior*, vol. 26, no. 3, pp. 406–418, 2010.

[40] P. Gantela and M. M. Shareef, "International journal of engineering sciences & research technology public data and private information-the threat and attack by cyber world,"